ARTICLE 29 Data Protection Working Party

02072/07/EN
WP 141

Opinion 8/2007 on the level of protection of personal data in Jersey

Adopted on 9 October 2007

OPINION OF THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA
set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995

On the level of protection of personal data in Jersey

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1], ("the Directive") and in particular Articles 29 and 30 paragraph 1 (b) thereof,

Having regard to the Rules of Procedure of the Working Party[2], and in particular Articles 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION: LAW ON DATA PROTECTION IN JERSEY

1.1. The situation of the Channel Islands and Jersey

The Channel Islands consist of five main islands: Jersey, Guernsey, Alderney, Herm and Sark, located in the English Channel within the Gulf of St Malo off the north-west coast of France. They are not part of the United Kingdom and have no representation in Parliament at Westminster. Constitutionally, they are divided into the Bailiwicks of Guernsey and Jersey.

The Bailiwick of Jersey is a dependency of the United Kingdom. The United Kingdom is responsible for the Jersey's international affairs and for its defence. Jersey itself has autonomy in relation to its domestic affairs, including data protection. Although the United Kingdom authorities are responsible for all international treaty negotiations, the effect of ratification by the United Kingdom will not extend to Jersey unless so requested by the Bailiwick's authorities.

[1]OJ L 281, 23.11.1995, p. 31, available at:
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm
[2]Adopted by the Working Party at its third meeting held on 11.9.1996.

Jersey is part of the customs territory of the Community. The common customs tariff, levies and other agricultural import measures apply to trade between the Jersey and non-Member countries, and there is free movement of goods in trade between the Jersey and the Community. However, other Community Rules, including those relating to data protection, do not apply. At the time the United Kingdom transposed the Directive, Jersey authorities indicated that such legislation would not apply to Jersey. Since then, it has introduced its own data protection legislation.

Pursuant to Article 299 of the Treaty establishing the European Community the Directive does not apply to Jersey and so it is a third country within the meaning of Articles 25 and 26 of the Directive.

1.2. Existing data protection legal framework:

The following Conventions have been ratified on behalf of the Bailiwick:
European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR);
International Covenant on Civil and Political Rights;
International Covenant on Economic, Social and Cultural Rights;
UN Convention on the Elimination of Racial Discrimination.
Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108).

The Data Protection (Jersey) Law 1987, which came into force on 11th November 1987, was based on the United Kingdom's Data Protection Act 1984, although the supervisory agency, the office of Data Protection Registrar, was not an independent agency, but was under the control of the Government.

Fundamental reform was introduced by the Data Protection (Jersey) Law 2005, which is modelled both on the United Kingdom's Data Protection Act 1998 and on secondary legislation adopted pursuant thereto. Its purpose is to reflect the requirements of the Directive.

2. ASSESSMENT OF THE DATA PROTECTION LAW OF JERSEY AS PROVIDING ADEQUATE PROTECTION OF PERSONAL DATA

The Article 29 Data Protection Working Party ("Working Party") assesses the adequacy of the law on data protection in Jersey by reference to the Data Protection (Jersey) Law, 2005, ("the Jersey law").

Methodological criteria

The methodological criteria for assessing the DP regime of Jersey are set out by the Working Party in its document, *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (WP 12 5025/98).[3] These can be set out as follows:

[3]See also European Commission, *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data* (Luxembourg: Office for Official Publications of the EC, 1998).

1. Content Principles
    - Purpose limitation
    - Data quality and proportionality
    - Transparency
    - Security
    - Rights of access, rectification and opposition
    - Restrictions on onward transfers
    - Additional principles are to be applied to specific types of processing, such as those concerning (i) sensitive data, (ii) direct marketing and (iii) automated decisions

2. Procedural/enforcement mechanisms
    - Delivery of a good level of compliance
    - Support to individual data subjects
    - Provision of appropriate redress to the injured parties

Definition and scope of the law

The Preamble to the Law states that it is a measure '*to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information and for purposes incidental thereto and connected therewith'*.

The Data Protection (Jersey) Law adopts the following definitions of the main data protection concepts:

Personal data

Personal data is *data that relate to a living individual who can be identified –*

(a) from those data; or

(b) from those data and other information that is in the possession of, or is likely to come into the possession of, the relevant data controller,

and includes any expression of opinion about an individual who can be so identified and any indication of the intentions of the data controller or any other person in respect of an individual who can be so identified; [4]

This definition differs in from that adopted in the Directive. In particular, the Jersey Law requires that an individual be identified from information in, or likely to come into the possession of the relevant data controller. Contrary to that, the Directive provides in Article 2 that *an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity* and specifies in recital 26 that *to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.* This means that where information relates to an individual who can be identified not by the controller but by

[4] Article 1.

other persons, such information would be protected under the Directive, whereas it would only be granted protection by the Jersey Law where the identifying information is likely to come into the possession of the data controller.

As regard the term "relate" in the definition, it is relevant to mention the importance of the UK case law established by the Durant case. In that ruling, the UK Court of Appeal has laid down two notions to assist where it is not clear whether data "relate to" a person and hence constitute "personal data" within the meaning of the UK Data Protection Act. These are whether the data are "*biographical in a significant sense*", and whether "*the focus of the information*" is the data subject. These notions are themselves part of a more general consideration, in cases of doubt, as to whether the data are information *affecting the data subject's privacy*.

Given the strong links between the Jersey legal system and its English counterpart with the Jersey Court of Appeal being staffed by English lawyers it may be that the case will be followed. In so far as such interpretation restricts the definition of personal data of the Directive, this may compromise the extent to which the Jersey legislation protects personal data.

Relevant Filing system

The term 'relevant filing system' is defined in the legislation as encompassing:

> *any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible*[5].

The Jersey Law uses the same formulation as applied in the United Kingdom's Data Protection Act 1988, which was applied restrictively by the Case Law derived from the English Court of Appeal's ruling in the case of *Durant v. Financial Services Authority*[6]. The Court of Appeal, concluded that a "a 'relevant filing system' for the purposes of the Act, is limited to a system: 1) *in which the files forming part of it are structured or referenced in such a way as to clearly indicate at the outset of the search whether specific information capable of amounting to personal data of an individual requesting it under section 7 is held within the system and, if so, in which file or files it is held*; and 2) *which has, as part of its own structure or referencing mechanism, a sufficiently sophisticated and detailed means of readily indicating whether and where in an individual file or files specific criteria or information about the applicant can be readily located*". This interpretation is more restrictive than the Directive, which defines filing system as *any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis,* and specifies in Recital 27 that t*he content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data.* Therefore, in those cases where the file is organised according to specific criteria relating to individuals and allowing easy access of data, but where the conditions laid down by the Court are not satisfied

[5] Article 1.
[6] [2003] EWCA Civ 1746

(for instance, where the information about an individual is contained in a file that does not have subfolders indicating what sort of information is kept there), that information would not be subject to the protection of the Act, whereas it should be covered by the data protection rules of the Directive.. Given the strong links between the Jersey legal system and its English counterpart with the Jersey Court of Appeal being staffed by English lawyers it may be that the case will be followed. However the extent to which these types of less structured manual files are likely to be transferred from an EU member state to Jersey is small. This situation does not therefore pose a serious obstacle to consider the Jersey Law as providing adequate protection in respect of its handling of manual record systems.

2.1. Content Principles

Basic principles

The purpose limitation principle requires that data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the Directive. Exemptions are also possible pursuant to Article 9 of the Directive, when necessary to guarantee freedom of expression.

The Working Party is satisfied that Jersey complies with this requirement. The second and fifth data protection principles in Part 1 of the First Schedule to the Jersey Law provide that personal data shall be obtained only for specified and lawful purposes, shall not be further processed in any manner incompatible with that purpose or those purposes, and shall not be kept for longer than is necessary for that purpose or those purposes.

The data quality and proportionality principle requires that data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

In its third and fourth data protection principles, the Jersey Law requires that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed, and that they shall be accurate and, where necessary, kept up to date. The Working Party considers, therefore, that this requirement is met by the Jersey Law.

The transparency principle requires that individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2) and 13 of the Directive**.**

This requirement has been met in Article 7(1) of the Jersey Law, supplemented by paragraphs 2 and 5 of Part 2 of the First Schedule.

The Jersey Law provides for exceptions to the operation of the transparency principle. Generally, these cover the same areas of activity as those described above in the context of the purpose limitation principle, and contain the same criteria relating to the determination whether the application of the exception may be considered necessary for the purpose at issue.

Article 31 of the Jersey Law provides for exemption for regulatory purposes intended to protect against public financial loss or prejudice. Article 32 of the Jersey Law relates to the publication of works of journalism, literature or art in the public interest. Article 34 of the Jersey Law provides that the transparency principle will not apply where the data consist in information that the controller is obliged by law to make available to the public. The first two appear to come within the scope of Article 13 of the Directive. Article 34, however, does not meet the criteria necessary to come within the scope of Article 13 of the Directive. In fact, it contains an exception which cannot be considered as a necessary measure to safeguard any of the important public interests mentioned in Article 13, and has no justification, inasmuch as the data that the controller makes available to the public (for instance data on the legal situation of a house in a real estate public register) is not the same as the information that he has to provide to the data subject about the *processing* (controller, purpose, categories of data, recipients, right of access) and therefore cannot substitute for it. However the assessment of adequacy is concerned with the protection of personal data transferred to Jersey from EU member states not with data collected domestically from data subjects in Jersey. It is hard to envisage the circumstances in which data transferred from the EU to Jersey will then fall to be published in a public register in Jersey. Even if it does the obligations under the transparency principal will largely fall on the EU transferor rather than the Jersey recipient.

Schedule 7 of the Jersey Law provides for exceptions where data relates to the operation of the armed forces and where compliance would prejudice that purpose. Exemption is provided for in respect of certain corporate finance data which constitute an important national economic or financial interest. Other exceptions relate to management forecasts, information to be used in negotiations with the data subject, and data which is covered by a claim to legal professional privilege. These would appear to be justified by Article 13 of the Directive.

Exemptions in the case of judicial appointments and the honours system, which apply in a very narrow field, do not appear to fall within the exceptions in Article 13 of the Directive.

The security principle requires that technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

The provisions of the Jersey Law appear to meet the requirements laid down by WP12 in respect of the security principle. The requirement that a controller adopt an appropriate level of security is explicitly stated, and in the case where processing is carried out for the controller, the requirement that a written contract be established, imposing equivalent obligations on the processor to those pertaining to the controller, meets the WP12 requirements in this respect.

The rights of access, rectification and opposition requires that the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be those in Article 13 of the Directive.

As to the right of access, Article 7 of the Jersey Law appears to comply with the requirements of WP12. The stated exceptions to the access rights appear to be consistent with those in WP 12 as authorised by Article 13.

As to the right of rectification, Article 14 of the Jersey Law seems to meet the requirements laid down in WP12, that the data subject be able to obtain the correction of inaccurate data. The Jersey Law extends further in that, if a Court considers it reasonably practicable, a data controller may be required to notify recipients of data that such data have been rectified.[7]

The right of opposition is dealt with in Article 10 of the Jersey Law, which establishes the right to prevent processing likely to cause damage or distress. This provision reflects the requirement in WP12 that there should be a right of objection 'in certain circumstances'.

Restrictions on onward transfers requires that further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should conform to Article 26(1) of the Directive.

In its eighth data protection principle, the Jersey Law provides that personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures a level of protection which is adequate according to the listed criteria.[8]

In the application of this principle, European Community decisions regarding the adequacy or otherwise of processing in a third country are said to be binding upon the Jersey authorities in the course of any proceedings under the Data Protection (Jersey) Law.[9]

Jersey Law contains no requirement that specific transfers outside the EEA are to be notified to the Data Protection Commissioner either in advance or subsequent to the transfer. It is, however, required that, at the time of notification, the controller must supply information as to the range of countries outside the EEA to which transfers may be made. If 10 or fewer countries are involved, the countries must be identified by name; if transfers to more than 10 countries are envisaged, notification must stipulate that transfers may take place on a 'worldwide' basis. Although transfers need not be notified, if the Data Protection Commissioner is satisfied that data has been transferred in circumstances where an adequate level of protection is not

[7] Article 14(5).
[8] Schedule 1, part 2, para. 13.
[9] Schedule 1, part 2, para. 15.

provided, an enforcement notice may be served to the controller pursuant to Article 40. However, the decision as to whether or not this requirement has been fulfilled is left to the data controller, and is not accompanied by any apparent audit or monitoring activities on the part of the Data Protection Authority.

Additional principles to be applied to specific types of processing are:

Sensitive data - where 'sensitive' categories of data are involved (those listed in Article 8 of the Directive), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing. The definition of sensitive data in the Jersey Law is consistent with Article 8.

The Jersey Law prescribes conditions for the processing of sensitive data. WP12 requires that for the processing of sensitive personal data, additional safeguards should be in place making specific mention of explicit subject consent. Schedule 3 of the Jersey Law lists the conditions which must be met before sensitive personal data can be processed.

Direct marketing - where data are transferred for the purposes of direct marketing, the data subject should be able to 'opt-out' from having his/her data used for such purposes at any stage.

The Jersey Law makes provision for such an option, adding the additional safeguard of applying to Court if the data controller does not respond to the request. It thus complies with the WP12 requirement in this field.

Automated individual decision - where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the Directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.

The provisions of the Jersey Law in these respects appear sufficient to justify a finding of adequacy. In providing for a right to object to the application of systems of automated decision making, at least in some specified situations, the Jersey Law exceeds the requirements of the WP12. It is also possible, after a decision is made, to require the data controller to reconsider it. There is also a requirement that the individual should be informed of the logic involved in the system.

2.2. Procedural/ Enforcement mechanisms

The WP 12 principles require that the assessment of the adequacy of a third country's legal system should identify the underlying objectives of a data protection procedural system, and on this basis judge the variety of different judicial and non-judicial procedural mechanisms used in that country.

The objectives of a data protection system are to deliver a good level of compliance with the rules; to provide support and help to individual data subjects in the exercise of their rights, and to provide appropriate redress to the injured party where rules are not complied with.

Delivery of a good level of compliance means that the system is characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important role in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.

The Working Party notes that the Jersey Law provides a number of elements, including the following, to serve this objective.

(a) Data Protection Commissioner

The Jersey Law provides for the office of Data Protection Commissioner, appointed by the States Assembly, a single-chamber institution, partially elected, which serves as both the executive and the legislature. It has the legal status of a 'corporation sole', making it an agency which is both independent of government and possesses a legal status which will continue in the event of the person holding the office ceasing to do so. The Commissioner may only be removed by the States' Assembly, and the terms and conditions of the appointment shall not be construed so as to create a contract of employment or agency between the States and the person appointed. The person is paid out of the States' general revenue.
Insofar as the Commissioner is appointed by the States, which is the parliament, and can only be dismissed by the States there is no doubt on the ability of the Commissioner to perform her duties in complete independence.
The Commissioner's duties and powers consist of gathering notifications, assessing certain forms of processing, powers of investigation and powers of enforcement, are specified in the Jersey Law. Additional duties are laid down in Article 51 of the law. The Commissioner's powers appear more limited than those set out in Article 28 of the directive. As regards her investigative powers, and her ability to gain access to premises and gather information, in principle a warrant by the judicial authority is needed, but this may be hampered if the data controller opposes it. This diminishes the effectiveness of this measure and makes this unfit for random checks or to conduct "*sua sponte*" investigations.

The Working Party's concerns about the lack of sufficient powers of the Commission therefore casts some doubt about the suitability of the Commissioner as an instrument to deliver a good level of compliance.

(b) The existence of adequate enforcement means and sanctions

The Jersey Law provides for a number of sanctions against data controllers who fail to comply with its requirements. Article 17 provides that failure to notify when obliged to do so is an offence. Article 20 requires data controller to notify any changes to the nature or purposes of processing.

Support to individual data subjects means that an individual should be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be institutional mechanism allowing independent investigation of complaints.

In this respect the Jersey Law provides an adequate level of protection. Without a formal constitution it is difficult to guarantee the independence of an agency, but there is no evidence of any degree of political interference with the functioning of the Commissioner's office and no indication of any disputes regarding the level of resources provided.

The provisions of Article 42 of the Jersey Law enabling a data subject to request the Commissioner to assess the legitimacy of processing provide an important adjunct to the rights which the subject may enforce through the Courts. In addition, Article 53 provides cases in which data subjects can request the Commissioner's assistance in relation to legal proceedings. In these respects the Jersey Law meets the requirement of support to individual data subjects.

The Jersey Law also continues the establishment of the Data Protection Tribunal which serves as an appellate body from decisions of the Commissioner.

Provision of appropriate redress is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

Article 13 of the Jersey Law provides that an individual who suffers by reason of any contravention by a data controller of any requirement of the law is entitled to redress. It also provides rights relating to the rectification, blocking, erasure and destruction of any inaccurate data. These rights extend beyond the data itself to encompass any expression of opinion which appears to have been founded on the inaccurate data. The rights are supplemented by provisions about committing offences as a result of which individuals might be adversely affected.

Accordingly, the Working Party considers that that the Jersey Law makes sufficient provision for adequate redress where individuals have suffered as a result of breach of the relevant rules.

3. RESULTS OF THE ASSESSMENT

While there may be some doubt that Jersey Law would fully meet the requirements imposed upon the Member States by the Data Protection Directive, the Working Party recalls, though, that adequacy does not mean complete equivalence with the level of protection set by the Directive. Some concerns exist in the areas of definitions of personal data and other concepts; transparency; and powers of the Commissioner but, after taking into account the explanations and assurances given by the Jersey Authorities the Working Party does not consider that these are significant in relation to the protection provided for personal data transferred from EU member states to Jersey.

Thus, on the basis of the above mentioned findings, the Working Party concludes that Jersey ensures an adequate level of protection within the meaning of Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Done at Brussels, on 9th October 2007

For the Working Party
The Chairman
Peter SCHAAR