ARTICLE 29 Data Protection Working Party

02107/07/EN
WP 142

Opinion 9/2007 on the level of protection of personal data in the Faroe Islands

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 the Faroe Islands

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 THE FAROE ISLANDS

1.1. The situation of the Faroe Islands

The Faroe Islands are located in the North Atlantic. They are comprised of 18 islands, separated by narrow sounds or fjords. The islands are administratively divided into seven counties, which are divided into 120 communities. Together with Denmark and Greenland, the Faroe Islands constitute the Kingdom of Denmark, which is a constitutional monarchy.

Under the 1948 Home Rule Act the islands became a self-governing community within the Kingdom of Denmark. The Home Rule Act divides all policy areas into two main groups, whereas Common affairs are under Kingdom authority and Special (Faroese) Affairs are under Faroese Home Rule administration and legislation.

The Home Rule Act recognises a competence for the Faroese authorities, consisting of the parliament and the government to legislate and administer Special Affairs[3]. Areas not transferred as 'Special Affairs' remain as 'Common Affairs' under the Kingdom legislate and administrative 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.
[3] Home Rule Act, Section 1.

However, even in those areas, specific competences, such as the administration or adoption of specific rules within the framework of the royal orders, can be delegated. Once a policy area is taken over from the Kingdom Authorities, the Faroese are assumed to have full economic, legislative, and administrative responsibility for a specific area.

The regulation of personal data in the Faroe Islands is based on laws passed by the Faroese Parliament and on laws regulating Common Affairs. The Data Protection Act ("DP Act") was passed by the Faroese Parliament in 2001, and is administered by the Faroese Data Protection Agency ("DPA").

The Danish Data Protection ("DP") Act applies only to the data processing of Kingdom authorities (i.e. the Police, and the prosecution, the county jail and the Prison and Probation Service, the High Commissioner of The Faroe Islands, processing of cases in the area of family law, church authorities). Since the Danish DP Act[4] is based on the Directive, it is assumed that it provides at least adequate protection with regard to the processing of personal data, and accordingly those areas are not considered herein.

1.2. Existing data protection legal framework:

Commentary on the preparatory work for a Faroese data protection law suggests that the DP legislation of both Denmark and Norway have been taken into consideration. Pursuant to a number of declarations made by Denmark between 1994 and 2003, protocols 7, 9 and 13 of the European Convention for the Protection of Human Rights of 1950 were implemented in the Faroe Islands. Pursuant to a declaration made by Denmark at the time of ratification, Convention 108 does not apply to the Faroe Islands.

The data protection regime encompasses a number of different rules protecting the individual about whom data are processed. Those rules are based upon principles and values which are similar to those established under EU law. The Act on Processing of Personal Data ("the Act")[5] represents the primary piece of the DP legislation in the Faroe Islands. This Act clearly reflects the content of the Directive.

Pursuant to Article 299 of the Treaty establishing the European Community, the Directive does not apply to the Faroe Islands, and accordingly, they are considered a third country for the purposes of Articles 25 and 26 of the Directive.

[4] Act No. 429 of 31 May 2000 on Processing of Personal Data. This Act implements Directive 95/46/EC 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.

[5] Act No. 73 of 8 May 2001.

2. ASSESSMENT OF THE DATA PROTECTION LAW OF THE FAROE ISLANDS 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 the Faroe Islands by reference to the Act.

Methodological criteria

The methodological criteria for assessing the DP regime of the Faroe Islands 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).[6] These can be set out as follows:

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

The Act applies to the processing of the personal data of natural persons in the private and public sector.[7] However, it will only apply *"if: 1) the processing of personal data is wholly or partly by automatic means, 2) personal data which form part of a filing system or are intended to form part of a filing system and this is a non-automatic systematic processing of data*".[8] The Act does not apply to the processing of personal data undertaken by a natural person with the view of exercising activities of a purely private nature.[9]

According to the Act, 'Personal data' shall mean "*any information relating to an identified or identifiable natural person ("data subject")*".[10] This definition corresponds to the first part of the definition on 'personal data' stated in the Directive, Article 2 (a).

[6]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).

[7]Articles 1 and 3(1)of the Act.

[8]Article 3(1) of the Act. This rule is in line with Article 3(1) of Directive 95/46/EC.

[9]Article 3(2) of the Act.

[10]Article 2(1) of the Act.

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 Faroese law complies with this requirement. Section 8 (2) of the Act provides that personal data shall be collected only for specified and legitimate purposes in accordance with the profession of the processor, and shall not be further processed in any manner incompatible with those purposes. There are exceptions only in the case of explicit consent, and for data for historical, statistical and scientific purposes, fewer than provided for in Article 13 of the Directive.

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.

Section 8 (3) of the Act provides that the data shall be relevant and not excessive in relation to the purposes for which the data are collected and the purposes for which they are subsequently processed, and Section 8 (6) states that the processing of data shall be accurate and organized in a way which ensures the required up-dating of the data. Furthermore, necessary checks should be made to ensure that data, which turns out to be inaccurate or misleading shall be erased or rectified without delay. The Working Party considers, therefore, that this requirement is met by Faroese 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 Section 21 of the Act, which provides that where the data have been obtained from someone other than the data subject, the controller collecting the data shall inform the data subject which personal data have been collected and, also provide the name and address of the controller and the purposes of the processing, advise if the personal data is forwarded, and if so, to whom, and any other information necessary to enable the data subject to safeguard his interests in accordance with the law. These rules do not apply where the data subject already has the information referred to, where recording or disclosure is laid down by law, or where providing such information either is impossible or requires a disproportionate effort.

The derogations - when disclosure can endanger national security or foreign policy, when related to crime prevention, when disclosure is not in the interests of the data subject for health or personal reasons, for reasons of confidentiality imposed by law, for internal use within an office, and when there are overriding public or private interests - are contained in Article 22, and are generally consistent with the exemptions permitted by 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.

Article 31 (2) to (5) of the Act relates to security. Individuals and companies performing work for a controller or a processor, having access to data may only process such data on the instructions of the controller. Processing shall then be conducted pursuant to a written agreement between the parties, which itself must contain this proviso. Applying appropriate technical and organisational security measures, the controller and the processor shall ensure that the processing of personal data satisfies the provisions of the Act concerning reliability, and personal freedom and access and shall implement appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction, loss or alteration, unauthorised disclosure, abuse or other processing in violation of the provisions laid down in the Act. Documentary proof of organisational security measures shall be available to employers of the controller and processor and to the Data Protection Agency. A controller's instructions may not restrict journalistic freedom or impede the production of an artistic or literary work.

The requirements in Faroese law regarding technical and organisational security measures satisfy this principle.

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, according to Article 19 of the Act, if the data subject demands, the controller must inform of the name and address of the controller and his representatives, the controller's subordinates, the manner and purpose of any processing, the nature of the data being processed, the source of the data, whether the data has been disclosed to anybody and if so, to whom, and what security measures are involved, as long as this itself does not compromise security. In that regard, Faroese law appears to comply with the requirements of WP12.

The exemptions, contained in Articles 22 (1), (3) and (4), appear to be consistent with those authorised by Article 13 of the Directive. It may be questioned whether the exemption on data which are only used in the office and not disclosed to others is in line with this Article. The rules on provision of information apparently do not apply in this situation thus eliminating the right to be informed at the moment where data is only used in the office and not disclosed to others.

The Faroe Islands has informed the Article 29 Working Party that the original translation of Article 22, part 1, no. 5, in the Faroese Act is inaccurate. The translation should have been as follows: "which are solely to be found in texts drawn up for internal preparatory purposes and which have not been disclosed to other persons."

The Faroe Islands has further informed the Article 29 Working Party that the exemption has to be assessed in connexion with the Faroese Act concerning Access to Documents in Administrative Files to which the Faroese Act on Processing of Personal Data has references. The Act concerning Access to Documents in Administrative Files, among other things, states that internal documents are an exemption from the rules of access but it is still possible to access the actual information in these documents. This rule is similar to the rules about internal documents in the Danish Act concerning Access to Public Records.

The Faroe Islands has finally informed the Article 29 Working Party that the exemption in Article 22, part 1, no. 5, is copied directly from the Norwegian Act concerning the processing of personal data.

Taking into account the additional information given by the Faroe Islands about the wording and its interpretation, the exemption regarding the right to be informed about internal documents does not appear to constitute a serious restriction on the right to be informed.

As to the right of rectification, Article 27 of the Act places an obligation on the controller to carry out rectification, erasure or blocking of personal data, and notification thereof to a third party to whom personal data has been disclosed, either on his own motion or at the request of the data subject, and thus meets the requirements laid down in WP12 that the data subject be able to obtain the correction of inaccurate data.

The right of opposition is dealt with in Article 26 of the Act, which establishes that the data subject may at any time object to the processing of data relating to him, and if such objection is subsequently upheld, the processing may no longer contain such data. This provision confers upon the data subject greater rights than 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 (that is, 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.

According to Article 16 of the Act, a transfer to foreign countries may take place only if the foreign country in question ensures an adequate level of protection, and permission is granted by the DPA. The adequacy of the level of protection afforded by a foreign country shall be assessed in the light of all the circumstances surrounding a data transfer operation, the purpose and duration of the processing operation, the nature of the data, the rules of law in force in the foreign country in question and the professional rules and security measures which are complied with in that country.

Permission from the DPA is required to transfer personal data to foreign countries.[11] However, the Minister of Justice may – upon the recommendation of the DPA – decide that data may be transferred to some countries without the permission of the DPA.[12] Such provisions are contained in Ministerial Order no. 33 which states that personal data may be transferred to EU-member states, Iceland, Norway, Switzerland, Argentina, Guernsey and Isle of Man without the authorization of the DPA.[13] The transfer of personal data to foreign countries thus appears to require an assessment similar to the assessment conducted under EU law.[14] This assessment is conducted by the DPA.

The provisions of the Act regarding the transfer of personal data appear to meet the criteria of WP 12. The derogations[15] are limited to those sanctioned in Article 26 of the Directive.

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 Act[16] is consistent with Article 8.

The Act 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. Article 10 of the Act lists the conditions which must be met before sensitive personal data can be processed.

[11] Article 16(1) of the Act.

[12] Article 16(2) of the Act.

[13] Ministerial Order no. 33 of 11.4.2005 on Transfer of Personal Data to countries without the permission of the Data protection Agency, Article 1(1).

[14] However, the Faroese Act is slightly different to Article 25 of Directive 95/46/EC.

[15] Article 17 of the Act.

[16] Article 2 (9) of the Act.

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 transfer of data for the purpose of marketing under the Act requires that the data subject opts-in. Disclosure of data concerning a consumer to a third party for the purpose of marketing or the use of such data on behalf of a third party for the purpose of marketing requires the explicit consent of the data subject,[17] which may be withdrawn at any time. [18] The data subject has a right to object to the processing of data relating to him,[19] implying that if the objection is justified[20] the data subject may opt-out from having the data used for marketing purposes. This right of objection may be exercised at any time.[21]

Accordingly, the level of protection under the Act in respect of direct marketing is in conformity with WP12.

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 Faroe Islands has informed the Article 29 Working Party that for now the Faroese Act does not contain a specific provision regarding automated decisions.

The Faroe Islands has found the data subject to be protected pursuant to other provisions in the Act – such as the rights to access, information and to object.

As to decisions from public authorities, the data subjects are further protected by the laws of administration and access. In accordance with unwritten administrative rules, valid in the Faroe Islands, public authorities have to assess each matter on its own, and can therefore not use automated decisions.

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.

[17] Article 9(3) of the Act.

[18] Article 29 of the Act.

[19] Article 26(1)of the Act.

[20] Article 26(2)of the Act.

[21] Article 26(1) of the Act.

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 Faroese law provides a number of elements, including the following, to serve this objective.

(a) Data Protection Commissioner

Faroese law provides for a Data Protection Agency .[22]

The Data Protection Agency, consisting of a Board and a Secretariat, is responsible for the supervision of all processing operations covered by this Act, and shall act with complete independence in executing the functions entrusted to it.
This means that the government is not in the position to give the DPA orders or instructions. The decisions made by the DPA are final and cannot be appealed to either the Ministry of Justice or to any other administrative authority.

The members of the Board are appointed by the Minister of Justice for a term of 4 years. As a general rule, the members of the Board cannot be dismissed. However, in exceptional cases a member may be dismissed by the minister, e.g. in a case of financial fraud. The members also act under the rules of "competence to act" which secure that the decisions made by the Board are independent.

The DPA is funded from the Faroese budget, which is decided by the Faroese Parliament. The DPA is attached to the budget which is allowed by the Parliament to the Minister of Justice. Once the Parliament has made a decision, it is the DPA who has disposal of the grant.

Taking into account the above mentioned safe guards, there should be no doubts as to whether the requisite conditions to ensure the DPA complete independence have been met.

Finally, it can be mentioned that the Faroese DPA is organised in exactly the same way as the Danish DPA.

The DPA, either on its own initiative or acting on a complaint from a data subject, ensures that data is processed in compliance with this Act, deals with notifications and applications for authorisation, maintains a public register of all notifications and authorisations, prepares opinions in relation to legislative proposals, monitors the processing of personal data, provides directions to the private and public sector where necessary, and ensures good practice, and monitors developments concerning processing of personal data within this country and in third countries and provides information about such developments.

[22] Article 36 of the Act.

It may order a controller to discontinue a prohibited processing operation, and rectify, erase or block specific data undergoing such processing; prohibit a controller from using a specified procedure if there is a risk that data will be processed in breach of the Act; order a controller to implement specific technical and organizational security measures to protect from processing data which may not be processed, and to protect data against accidental or unlawful destruction or accidental loss, alteration, and disclosure to any unauthorized person, abuse or any other unlawful forms of processing, and in special cases, it may issue an injunction against a data processors.

The members and the staff of the Data Protection Agency shall at any time, without any court order, have access to all premises from which processing operations carried out are administered, or from which there is access to the data subject to processing, and to all premises where data or technical equipment are stored or used.

These powers satisfy the requirements as to adequacy.

The annual reports include all activities of the DPA. The reports are publicly available and can be retrieved from the website of the DPA.[23] So far, the DPA has published 3 reports, covering 2002, 2003 and 2004.[24]

(b) The existence of adequate enforcement means and sanctions

In order to encourage the obligated addressees of the Act to deliver a good level of compliance with the content rules, the Act establishes sanctions and penalties to be imposed in case of non-compliance. However, if more severe punishment is prescribed under other legislation, such other legislation shall be the legal basis for the imposition of sanctions and penalties.[25] Sanctions and penalties can only be imposed by Courts.[26]

All the essential provisions of the Act are supported by sanctions, consisting of fines or detention in case of non-compliance, and compensation for damages in respect of security measures under Article 31. Liability is not limited to natural persons, but can extend to legal persons.

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.

The data subject's rights are listed in Chapter 7 of the Act.[27] The method by which a data subject can enforce his or her rights is set out in Article 30, by means of a complaint to the DPA. As an alternative, a data subject can resort to the general right to file a complaint directly at the county court.

---

[23] Article 41 of the Act.

[24] The reports may be found on the home page of the DPA in Faroese. http://www.datueftirlitid.fo/index.asp?pID={6A552A7B-263D-4D06-B468-F966DDAD0A15}

[25] Article 44(1) of the Act.

[26] The Constitutional Act of Denmark of 5 June.1953, Articles 3 and 63.

[27] Articles 26-30 of the Act.

Once a decision is taken by the DPA, it cannot be appealed either to the Ministry of Justice or any other administrative authority, but must be appealed in the Courts.

One of the tasks of the DPA is to provide assistance for the interpretation of the Act. It is an accessible body, which hears complaints from data subjects, and adjudicates on alleged breaches of the Act. In particular, citizens can demand that the DPA make an assessment, providing to the individual institutional support in the issues to be addressed. The procedure for assessment is described in detail on the DPA's website and it involves no cost.

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 46 of the Act provides that the controller shall compensate any damage caused by the processing of personal data in violation of the provision of this Act, unless it is established that such damage could not have been averted through the diligence and care required in connection with the processing of personal data.

Articles 44 and 45 impose sanctions, consisting of fines or detention, for breaches of the Act. Persons carrying on business can be deprived of that right if convicted of an offence under the Act.

Accordingly, the Working Party considers that that Faroese 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 Faeroese law may not meet every requirement imposed upon the Member States by the Data Protection Directive, the Working Party is aware that adequacy does not mean complete equivalence with the level of protection set by the Directive.
Thus, on the basis of the above mentioned findings, and the additional information given by the Faroe Islands, the Working Party concludes that the Faroe Islands ensure 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