01446/12/EN
WP 198

Opinion 07/2012 on the level of protection of personal data in the Principality of Monaco

Adopted on 19/07/ 2012

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 the free movement of such data, and in particular Articles 29 and 30 paragraph 1 (b) thereof,

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

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION AND BACKROUND

On 11 November 2009 the Principality of Monaco requested the Commission to handle the procedure for the declaration of Monaco as a country that offers an adequate level of protection within the meaning of Article 25(6) of Directive 95/46/CE, on Personal Data Protection.

In order to proceed with the study of the adequacy of Monaco, the Commission requested the Working Party to produce an opinion, which analyzes the extent to which the Monaco regulatory system fulfills the requirements for the application of the personal data protection regulations set out in the Working Document "Transfers of Personal Data to Third Countries : Applying Articles 25 and 26 of the EU data protection directive", adopted by the Working Party created by Article 29 of the Directive on 24 July 1998 (document WP12).

The WP29, during the plenary session of 4th and 5th April 2011 appointed the CNIL, due to its historical relationship with Monaco, as rapporteur on this adequacy study.

The CNIL has met several times with the Data Protection Authority of Monaco, the "Commission de Contrôle des Informations Nominatives" (hereinafter, CCIN). In order to study the data protection legislation of Monaco and its practical implementation. As regards some concerns regarding the effective independence of the CCIN, the CNIL Chairman called upon a mediation meeting between the CCIN and the Monaco Government on 28 May 2012. This meeting has led up to the conclusion of an Agreement clarifying the competences and the relationships between both parties in terms of human resources and budget management.

As decided during its meeting held on 6 June 2012 the Working Party circulated the draft opinion to the "Adequacy Subgroup" for review. It also decided to adopt this opinion via written procedure.

After a conference call, the draft opinion has been sent on 4 July 2012 to the "Adequacy Subgroup" for review. The proposal was approved by the Working Party by written procedure.

2. DATA PROTECTION LEGISLATION IN THE PRINCIPALITY OF MONACO

Monaco is the second smallest and the most densely populated country in the world. Monaco is a principality governed under a form of a hereditary constitutional monarchy according to the Constitution of 17 December 1962, reformed on 2 April 2002. It is a sovereign city State bordered by France on three sides, with one side bordering the Mediterranean Sea. Its population is around 32 800 inhabitants. Its economic activity is concentrated in commercial transactions and, in particular, tourism. Monaco and France are bound with a strong political, customs and monetary union. The largest part of its population is French nationals (28.4%), followed by Monegasque (21.6%).

According to historical links between France and Monaco, the Monaco data protection legislation is close to the French data protection law.

Article 20 of the Monaco Constitution confirms the protection of the right to privacy and declares that "*Everyone has the right to respect for his private and family life and the secret of his correspondence*".

The protection of personal data is regulated by the Act n° 1.165 of 23 December 1993 on the protection of personal data and by the Sovereign Ordinance N°2.230 of 29 June 2009 setting out the implementing conditions of the Act n° 1.165. The Act has been amended by Act n° 1.353 of 4th December 2008 and by the Act n° 1.353 of 1st April 2009 (hereinafter "Act" or "Act 1.165").

The Act establishes the CCIN as an independent authority. During its few years of functioning under new rules and status (since 2009), the CCIN has issued various guidelines, deliberations, two annual reports and other information on various subjects *(*ex. biometrics, GPS chips, video surveillance etc.) to set out rights and duties for individuals, businesses and the State and to provide guidance on the practical application of privacy principles.

In the international sphere, Monaco has signed and ratified the European Convention on Human Rights in 2005, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and its Additional Protocol (in force since 01/04/2009) as well as the International Covenant on Civil and Political Rights on 28/08/1997.

3. ASSESSMENT OF THE DATA PROTECTION LAW OF THE PRINCIPALITY OF MONACO AS PROVIDING ADEQUATE PROTECTION OF PERSONAL DATA

The Working Party points out that its assessment of the adequacy of the data protection legislation into force in Monaco refers essentially to the Act n° 1.165 on the protection of personal data of 23 December 1993 as it has been amended in 2008 and in 2009.

The provisions of this Act have been compared with the main provisions of the Directive, taking into account the Working Party's opinion WP12. This opinion lists a number of principles which constitute "*a "core" of data protection "content" principles and "procedural/enforcement" requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate"*.

3.1. Definitions

The Act provides for definitions of "personal data", "processing", "data controller", "recipient" and "data subject" (art.1).

Although certain definitions are not provided ("filing system", "processor", "third party" and "the data subject consent"), all these concepts are used or deduced from several Articles of the Act[1].

However, in order to avoid interpretations, that can be harmful to personal data protection, it would be better, if Monaco legislator defines the above mentioned terms This is especially important with regard to the definition of "consent" and that of "processor". In this connection, the WP would like to refer to the clarification input given via its Opinions on the concepts of "controller" , "processor", and "consent" (in particular as to its being "explicit" and "informed") as well as on the very concept of "personal data".

3.2. Scope of application of the legislation

The scope of application of the Act is mainly defined under chapter V of the Monaco Act and is very similar to the Articles 3, 4, 13 of the Directive.

As regards the material scope of the Act, it covers all forms of processing of personal data (automated or non-automated, Art.24-1) in whatever shape or form (Art.1 first paragraph), protects natural as well as legal persons (deduced from Art.3, Art.13 etc.) and covers processing carried out by the entire public and private sector.

There might be some interrogation as regards the introduction in Article 13 of the Act n°1.165 of provisions allowing legal persons to oppose to their personal data being processed. The WP considers that the scope of application of the Act should be clarified in order to avoid textual inconsistencies with the initial scope of application as provided in Article 1 referring only to the protection of natural persons.

As provided by the Directive, the Monaco Act shall not apply to the processing of personal data carried out held by a natural person solely as part of their personal or domestic activities. Moreover, the Act shall not apply to the processing pursuant to Article 15 of the Constitution (related to the right of reprieve, amnesty and naturalization) or carried out by the judicial authorities for the purposes of proceedings initiated before the Courts and international mutual assistance procedures (Art.24-2 of the Act).

Besides, Article 25 of the Act provides for exceptions on processing for purposes of literary and artistic expression, in the same way as Article 9 of the Directive.

As regards the territorial scope, Article 24 provides, in similar terms to the Directive, that the Act applies to the automated processing:

- carried out by a data controller established in Monaco;
- carried out in Monaco, even if such processing is destined only for use abroad;

[1] Filing systems is mentioned in art. 23-1, 24-1, 24-2, 25, processor in Article 1 (definition of recipient), Article 17 (related to security requirements), third party in Articles 8 (6°), 12, 14, 20-1, data subject consent in Articles 10-2, 12.

- where the data controller is established abroad, but makes use of processing facilities located in Monaco; in such case, the data controller must appoint a representative established in Monaco, who is to make the declaration, request for an opinion or application for authorization and upon whom the obligations laid down by the law are incumbent, without prejudice to legal action that might be lodged against the data controller themselves.

Therefore, the Working Party considers the scope of application of the Monaco data protection Act to be similar to the one provided by the Directive although some adjustments of the current wording would appear to better clarify how its provisions are applicable to legal persons.

3.3. Content principles

a) Basic principles

1) The purpose limitation principle: 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 exceptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the Directive.

The Working Party considers that the legislation of Monaco implements this principle through its Article 10-1, which provides that "*Personal data must be: collected and processed fairly and lawfully; collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes ;(...)*"

Furthermore, Article 22 of the Act provides that "*The following shall be punished by imprisonment for three months to one year and by a fine as described in item 4 of Article 26 of the Criminal Code or only one of those two penalties: (...) 9° persons knowingly use or cause to be used personal data for other purposes than those described in the declaration, request for an opinion or application for authorization.*"

Therefore, the Working Party considers that Monaco legislation complies with the purpose limitation principle.

In addition, it is interesting to note that Article 10-2 of the Act also provides for conditions for a lawful processing, in the following terms: *"Processing of personal data must be justified:*

- by consent from the data subject(s), or;

- by compliance with a legal obligation to which the data controller or their representative is subject, or;

- by it being in the public interest, or;

- by the performance of a contract or pre-contractual measures with the data subject, or;

- by the fulfilment of a legitimate motive on the part of the data controller or their representative or by the recipient, on condition that the interests or fundamental rights and freedoms of the data subject are not infringed."

2) The data quality and proportionality principle: 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.

The Working Party considers that the quality principle is expressly included in Article 10-1 of the Act n°1165.

According to Article 10-1 "*Personal data must be: - collected and processed fairly and lawfully; (...) - adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed; (…)*". In addition, the last sentence of this Article foresees that "*The data controller or their representative must ensure compliance with these provisions*".

Likewise, according to Article 9 of the Act, the retention period cannot exceed the period set out in the request for an opinion, declaration or application for authorization, except where it is to be processed for historical, statistical or scientific purposes or where the CCIN has given its authorization.

According to Article 21(4°) of the Act, persons who retain personal data beyond the period indicated in the declaration, request for an opinion or application for authorization or beyond the period fixed by the Personal Data Protection Supervisory Commission (i.e. the CCIN) shall be punished by imprisonment for one to six months and by a fine as described in item 3 of Article 26 of the Criminal Code.

Therefore, the Working party considers that the legislation of Monaco complies with the data quality and proportionality principle.

3) The transparency principle: 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.

The Act provides for transparency requirements in its Articles 14, 14-2 and 10.

Article 14 of the Act requires, in similar terms to those contemplated in Article 10 of the Directive, that the data subject shall be informed by the data controller, regarding:

- the identity of the data controller and, if applicable, the identity of their representative in Monaco;
- the purpose of processing;
- the obligatory or optional nature of replies;
- the consequences for them of failure to reply;
- the identity of recipients or categories of recipients;
- their right to oppose, access and rectify their data;
- their right to oppose the use on behalf of a third party, or the disclosure to a third party of their personal data for the purposes of prospection, particularly commercial prospection.

This Article also provides that : "*Where personal data is not collected directly from the data subject, the data controller or their representative must provide the data subject with the information listed in the previous paragraph, except where the data subject has already been informed, cannot be informed, or where this involves disproportionate measures with regard to the utility of the action or if collection or disclosure of the data has been expressly provided for by legislative or regulatory provisions*."

Moreover, Article 14-2 regarding the use of electronic communications networks, provides that the subscriber or user must be provided with clear and comprehensive information about the purposes of processing, and the means available to refuse such processing.

The exceptions to this Article are those stated above (see, Section 3.2. "Scope of application") and comply with the exceptions provided by the Directive.

Penal sanctions are provided by Article 21 (6°) and (7°) of the Act for the infringement of the above mentioned provisions.

In addition, Article 10 provides for a Data Processing Register which can be consulted by any legal or natural person and which contains details on declarations, requests of opinions and applications for authorization relating to data processing.

As a consequence, the Working Party considers that the transparency principle is fulfilled by the data protection legislation of Monaco.

> **4) The security principle:** Technical and organizational 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 Working Party considers that the legislation of Monaco complies with this principle.

Section III of the Act 1.165 is expressly dedicated to "Secure and confidential processing": Articles 17 contains all the requirements for security measures to be taken by the data controller and service provider and expressly states the following:

"*The data controller or their representative must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss, corruption, unauthorized disclosure or access, in particular where processing involves the transmission of data over a network, and against all other unlawful forms of processing.*

Measures implemented must ensure an adequate level of security with regard to the risks posed by processing and by the nature of the data to be protected.

Where the data controller or their representative makes use of the services of one or more service providers, they must ensure that the latter are able to comply with the obligations laid down in the two previous paragraphs.

Processing carried out by a service provider must be governed by a written agreement between the service provider and the data controller or their representative, stipulating in particular that the service provider and members of their staff are acting solely upon instructions from the data controller or their representative alone and that the obligations described in the two previous paragraphs are also incumbent upon said service provider.

If the service provider wishes to use the services of one or more subcontractors in order to provide all or some of the services set out in the aforementioned agreement, the provisions of the previous paragraph shall apply thereto."

As it has been recommended under Section 3.1, for the sake of clarification and in order to avoid diverged interpretations, the Working party believes that it would be more satisfactory if the legislation of Monaco explicitly defined the concept of "service provider".

Besides, Article 17-1 of the Act provides for specific measures of security for some processing managed by public authorities or presenting particularities (ex. Biometric data).

Article 21 (3°) of the Act provides for imprisonment for one to six months and for a fine as described in item 3 of Article 26 of the Criminal Code in case of infringement of the above provisions.

Therefore, we consider that the legislation of Monaco complies with the security principle.

> **5) The rights of access, rectification and opposition:** 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 in line with Article 13 of the Directive.

Various Articles refer to these rights and Section II of the Act is expressly dedicated to the exercise of rights to access, to oppose and to rectify as well as the duties of controllers regarding these rights.

In particular, according to Article 13 of the Act, natural as well as legal persons have a right to oppose to personal data processing and to have access to their data under the conditions laid down in Section II of the Act, as well as to have such data amended if appropriate (Art.15-16).

Article 15 of the Act provides for a right of access in terms very similar to those provided by Article 12 of the Directive. Indeed, *"All persons justifying their identity may obtain, from the data controller or their representative:*

1° information at least as to the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data is disclosed;

2° confirmation as to whether or not data related to him or her is being processed;

3° such data communicated in written, non-coded form, conforming to the stored data; information of a medical nature shall be communicated to the data subject or the doctor that they have appointed for this purpose. (...);

4° information relating to the automated reasoning process having led to the decision described in Article 14-1."

Moreover, the Act also provides in its Article 15-1 for an indirect right of access in case of processing carried out by judicial or administrative authorities, exclusively within the scope of the duties legally conferred upon them.

Likewise, data controller or their representatives have the obligation, under Article 15-2 of the Act to take appropriate measures in order to amend incomplete or erroneous personal data, delete data that might have been obtained by unlawful means, delete the named form of data upon expiry of the storage period fixed by the CCIN.

At the same time, the Act recognises in its Article 16, in the same terms as the Directive (Art.12b), the right of a data subjects to demand that their data be rectified, supplemented, clarified, updated or deleted where such data proves to be imprecise, incomplete, equivocal, obsolete or if its collection; likewise, according to Art.16 recording, disclosure or storage is prohibited.

Exceptions close to the Article 13 of the Directive apply (see Section 3.2. "Scope of application"). Furthermore, Article 15 last paragraph of the Act provides for exemption from the duty to reply to requests that are abusive as a result of their number or repeated or systematic nature.

Article 21(2°) of the Act provides for imprisonment for one to six months and for a fine as described in item 3 of Article 26 of the Criminal Code in case of a voluntarily opposition to communicate to a data subject their personal data, or to amend or to delete any of such information which has proved to be imprecise, incomplete, equivocal or collected in violation of the law.

Article 22 (5°) of the Act provides for stricter sanctions in case of infringement of the right to object to the processing of the data relating to a data subject.

Therefore, we consider that Monaco complies with the rights of access, rectification and opposition on the condition that exceptions are interpreted strictly.

> **6) Restrictions on onward transfers:** 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 be in line with Article 26(1) of the Directive.

The third chapter of the Act refers to the regulation of transfers. In particular, Article 20 provides that a transfer of personal data may only be carried out, if the recipient country affords an adequate level of protection. The adequacy of the level of protection afforded by a third country must be appreciated in the light of all the circumstances relating to the transfer

operation or set of transfer operations; the CCIN provides a list of countries assuring a sufficient level on its website.

Article 20-1 of the Act establishes exemptions from this above provision in certain circumstances:
- where the data subject has given his consent;
- where the transfer is necessary in relation to a contract or a legal claim;
- where protection of an important public interest so requires;
- where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest;
- where the transfer is necessary for the performance of a contract between the data subject and the controller taken in response to the data subject's request etc.

Moreover, as provided by the Directive (Art. 26) a transfer of personal data to a country or organization, which does not have an adequate level, is permitted under the CCIN authorization, if the data controller or their representatives offer sufficient guarantees, as for example appropriate contractual clauses.

Furthermore, Article 21(5°) of the Act provides for imprisonment for one to six months and for a fine for breaches of restrictions on onward transfers.

The Working Party believes that the rule that have been set out comply with the principle of restriction of further data transfers to third countries.

Moreover, the Working Party would like to recommend that every appreciation made by the CCIN should take into account the interpretation of the concept of "adequate level" provided by the WP12 and by the "Working Party" on the matter as well the one concerning standard contractual clauses.

Therefore, we consider that Monaco legislation complies with the onward transfer principle.

b) Additional principles

Document WP12 refers to certain principles that should be applied to specific types of processing, concentrating on the following:

1) **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 Working Party considers that this principle is fulfilled in Monaco data protection legislation, taking into account especially Article 12 of the Act, which provides for a list of these data, as well as the conditions of their lawful processing that coincides with those contained in Article 8 of the Directive.

Article 12 of the Act provides for an express prohibition on processing of personal data revealing

- political memberships or opinions,
- racial or ethnic origin,

- religious or philosophical beliefs,
- trade-union membership,
- the processing of data concerning health or sex life,
- morals and social measures.

The WP notes that the list of "special categories of data" includes genetic data, which is in line with the suggestions made by the WP in connection with the ongoing revision of the DP legal framework in the EU as well as with the current text of the proposal for an EU data protection regulation put forward by the European Commission; it also includes data relating to "lifestyle" ("*moeurs*") and "social welfare measures", which considerably expands the scope of application of the prohibition in question.

The processing of these data can be lawful only under the application of some enumerated conditions, very close to those provided by the Directive, such as written and express consent, public interest, processing of the members of an ecclesiastical institution or a body with a political, religious, philosophical, humanitarian or trade-union aim, processing required for the purposes of preventive medicine, data processing relates to information that has manifestly been made public by the data subject, processing required in order to record, exercise or in the defense of rights before the Courts or meeting a legal obligation.

Moreover, according to the Article 7-1 of the Act, the processing of personal data for the purpose of medical research shall not be carried out unless a motivated opinion of the CCIN has been obtained.

The WP also notes that the CCIN's "prior authorization" is necessary according to Article 11-1 to allow data controllers other than judicial and administrative authorities to process certain categories of data like information on "suspicions of unlawful activities" or "biometric data required to check persons' identities" or "for the purposes of surveillance".

The WP takes into account the fact that, in practice this article is used by the CCIN to provide a higher level of protection by subjecting specific monitoring or surveillance processing (such as video surveillance, geolocation or control of access) to a prior authorization procedure.

Besides, Article 21 of the Act provide for stricter criminal penalties for illegal processing of sensitive data.

Therefore, the Working Party considers that the Act complies generally with the sensitive data requirements.

2) **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.

Since 2008, the Act provides for the right to object to the processing of personal data or their disclosure to third parties or used on the behalf of the processor commercial prospecting.

Article 13 of the Act offers the right to oppose, for legitimate reasons, their personal data being the subject of processing.

Furthermore, Article 14 states in the following terms:
"Persons from whom personal data is collected must be informed: [...]
- *of their right to oppose, access and rectify their data;*
- *of their right to oppose the use on behalf of a third party, or the disclosure to a third party of their personal data for the purposes of prospection, particularly commercial prospection. [...]".*

Article 21 (6°) and (7°) provide for penalties in case of breach of the above Articles.

Although it would be clearer to have, like in the Article 14 b) of the EU Directive a " *right to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing* (…)", the WP considers that, in the light of the WP 12 requirements, the provisions of Article 14 of the Act n°1.165 on the right of the subscriber or user to be informed, together with Article 13, provide acceptable safeguards with a specific right to oppose in case of direct marketing purposes.

3) 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.

According to the Article 14-1, the Act provides for a right to the data subject not to be subject to a decision which produces legal effects concerning or significantly affecting them and which is based solely on the automated processing of data intended to evaluate their profile or certain aspects of their personality.

It also states that:
"*A person may nevertheless be subject to a decision described in the previous paragraph if such decision:*

-is taken in the course of the entering into or performance of a contract, provided the application for the entering into or performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard their legitimate interests, such as arrangements allowing them to express their point of view and have their application re-examined;

-or is authorized by legal or regulatory provisions which lay down measures to safeguard the data subject's legitimate interests."

Therefore, the Working Party considers that the Act complies with the "automated individual decision principle".

Lastly, it worth noting that, according to Article 7 of the Act, processing carried out by data controllers, legal persons governed by public law, public authorities, entities governed by private law with a duty of general public interest or public service concession holders shall be decided by the authorities following a reasoned opinion issued by CCIN.

Procedural/enforcement mechanisms

The Working Party's opinion WP12 "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" points out that to assess the adequacy of a third country's legal system it is necessary to identify the underlying objectives of a data protection procedural system, and on this basis to judge the variety of different judicial and non-judicial procedural mechanisms used in third countries.

In this respect, the objectives of a data protection system are essentially threefold:

– 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,
– To provide appropriate redress to the injured party where rules are not complied with.

a) To deliver of a good level of compliance with the rules: A good system is generally 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 part in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.

1. Awareness among data controllers and individuals

The Working Party considers that the level of awareness provided by the data protection legislation of Monaco is satisfactory view the recent modification (2009) of the powers and composition of the data protection authority of Monaco as well as the small size of the country.

Article 6 of the Act provides for a prior notification obligation of automated processing of personal data, carried out by data controllers, natural or legal persons governed by private law which shall comprise an undertaking that processing complies with the requirements of the law.

These declarations must contain some elements specified by Art.8 of the Act (e.g. identity of the signatory and that of the data controller, methods, purposes and justification, the identity of the persons responsible for using the data and the measures taken to enable the right of access to data to be exercised, the categories of persons have access to the data, the categories of data, and data, that is being processed, its origin, the duration of retention, categories of persons concerned by processing and the categories of authorized recipients to whom such data may be disclosed, interconnection or other means of relating data, as well as any transfers to third parties, measures taken to ensure security of processing and of data, and to guarantee secrets protected by the law, indication, where appropriate, that processing is intended to communicate data abroad, even where it takes place by means of operations performed beforehand outside Monaco).

Nevertheless, standards may be enacted by Ministerial Order following a proposal or opinion issued by the CCIN, setting out the criteria to which certain processing categories of processing manifestly not infringing fundamental rights and freedoms must adhere. Such

processing may be the subject of a simplified declaration of compliance, or be exempted from any obligation of declaration, under conditions laid down by the aforementioned Ministerial Order (art.6).

Furthermore, the website of the CCIN, is practical and easy to manage and contains useful information clarifying the legislation provisions on rights and duties of natural and legal persons and the implementation of the new law. It also contains all the deliberations of the CCIN as well as the annual reports, explaining the authority's activities.

According to recent statistics, the CCIN has received during 2009 very few requests, something understandable, due to the first year of its new functions. However, 2010 seems an active second year : 28 opinions, 13 decisions on authorization requests, 2 deliberations on investigations, 3 recommendations, 2 propositions for simplified formalities, 1 deliberation on a consultation for a bill of law, 1 deliberation on the CCIN internal organization.

The CCIN has also participated in 86 meetings with controllers from the private sector and 27 with controllers from the public sector and has answered in 159 phone consultations.

Moreover, the existence of a registry of all the personal data files carried out in the Principality of Monaco is provided by Art.10 of the Act. It is available for consultation by any natural or legal person who wants to know the controllers and details related to the processing.

The only point that we could remark in this new development of data protection in Monaco is the lack of a provision about an independent data privacy officer in the private or/and public sector who could be charged with ensuring, in an independent manner, compliance with the obligations provided for in this Act (data protection officer proposed by Article 18 par.2 of the Directive). However, that is not an express requirement of the WP12 and constitutes only a recommendation of the Working Party to Monaco legislator.

2. The "Commission de contrôle des informations nominatives" (CCIN)

Section II (Articles 2 to 5-6 of the Act) creates the CCIN as a supervisory authority having the task of monitoring and checking compliance with legislative and regulatory provisions relating to the protection of personal data and having the fully independent remit, under the conditions defined by the Act.

Its main role consists in the monitoring of personal data processing carried out in the Principality of Monaco by public and private entities as well as by individuals. Article 2 of the Act sets out the jurisdiction of the CCIN, which consists in filing registration, power to conduct inspections, authorization, issuing of opinions, making of recommendations, investigation, issuing warnings and formal notices to data controllers, etc.

Regarding structural independence, the Act provides in its Article 2 that the CCIN has the fully independent remit, under the conditions defined by this Act of being in charge of registration, authorization, inspection and all other tasks required by the Directive. Also, according to Article 5 (second paragraph) of the Act the members of the Commission shall not receive instructions from any authority in the performance of their duties.

The Secretary-General and all the members and officers of its services are subject to the general rules applying to civil servants and State officials, except where there are specific legal or regulatory provisions. Nevertheless, they are bound only by hierarchical and disciplinary powers of the CCIN Chairman (Art.5-3).

Moreover, the CCIN Chairman is by absolute majority elected among its representatives while his appointment as well as of the rest five members is valid for 5 years renewable once (Art.5).

The CCIN is composed of six members proposed by some specific and enumerated authorities, as a result of their expertise (Art.4). Proposals shall be made independently of the authorities, councils and institutions concerned (Art. 4) and shall be remitted to the Prince (Art. 1st of the Sov. Ord.)

As regards incompatibilities, Article 5 of the Sovereign Ordinance n°2.230 provides for incompatibilities between the office of a CCIN member and five other offices listed in this Article (Member of the Monegasque Parliament or Municipal Councilor, Member of the Council of State, that of sitting judge, except for the Member proposed by the Minister of Justice that of civil servant or State official, municipal official or an official of a public institution, who is currently in office; those working on the performance of duties or shareholdings in Monegasque or foreign companies contributing to the manufacturing of equipment used in computers, telecommunications or the provision of IT or telecommunication services.).

Besides, CCIN officials and members are due by the Act to professional secrecy and confidentiality (Art.5-1).

According to Article 5-5 of the Act the Chairman of the Commission shall conclude all contracts and agreements required for the proper functioning of its departments.

However, according to Monaco administrative rules and practices the choice of recruitment of the CCIN Chairman shall always be submitted to the Council of Government (and then to the Prince). Moreover, employment contracts of contractual officials are signed by the Directorate of Civil service and not by the CCIN Chairman. Finally, every promotion proposed by the Chairman must be submitted to the Directorate of Civil Service and be transferred for approval to the Council of Government and then to the Prince for a final decision.

As regards financial independence, Article 5-4 of the Act provides that the funding required for the operation of the CCIN shall be listed in a specific chapter of the State budget.

The Chairman shall prepare and submit to the Ministry of State (*Ministre d'Etat*) propositions indicating anticipated revenue and expenditure. Expenditure shall be prepared by the Secretary General or the Chairman. The Commission accounts must be audited on an annual basis under conditions laid down by Sovereign Ordinance (Art. 5-4 of the Act).

According to the Article 28 of the Sovereign Ordinance n°2.230 the Chairman of the CCIN shall send the Prime Minister the accounts when closed, in order that they may be audited by the Official Auditor.

In practice, the CCIN is submitted to an exhaustive prior expenditure control of the Official Auditor of expenditure (*Contrôleur Général des Dépenses*). This control seems to be based on a Monaco administrative practice applicable to a large majority of public authorities but cannot totally satisfy independence requirements provided by Article 28 of the Directive.

In relation to this issue, it is important to recall that the Grand Chamber of the Court of Justice of the European Union advocated a large interpretation of terms "complete independence" of Article 28 of the Directive (C-518/07 of 9th March 2010):

Thus, as was stated:

- "*It follows that, when carrying out their duties, the supervisory authorities must act objectively and impartially. For that purpose, they must remain free from any external influence, including the direct or indirect influence of the State or the Länder, and not of the influence only of the supervised bodies* "(§25).
- "*That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data*."(§30).
- "*Furthermore, it should be pointed out that the mere risk that the scrutinising authorities could exercise a political influence over the decisions of the supervisory authorities is enough to hinder the latter authorities' independent performance of their tasks*." (§36).

The CNIL, as rapporteur, considered that the above exposed elements concerning influence of the Monaco Government on the recruitment, promotion of the CCIN staff, as well as on the exhaustive prior control of the CCIN expenditures, could possibly undermine the CCIN independence and consequently, can impact the adequacy of the Monaco data protection legislation with European requirements.

In order to resolve those issues that refrain from recognition of adequacy, the CNIL Chairman called upon a mediation meeting between the CCIN and the Monaco Government on 28 May 2012.

This meeting has led to the conclusion of an Agreement between the Monaco Government and the CCIN with the aim to clarify administrative practices and to clarify the competences between both parties in terms of human resources and budget management in order to reinforce the independence principle.

According to this Agreement, the CCIN Chairman will be competent to:
- define the modalities of recruitment without any Government control of opportunity (e.g. drafting recruitment form, defining required skills and conditions of the selection, deciding on the recruitment process and interview);
- when the recruitment concerns a civil servant or a contractual agent, the CCIN should ensure, with the help of the Government that the conditions of the recruitment are in line with the applicable rules on civil servants and contractual agents. In addition, the appointment of the said person is deliberated within the Council of Government. The

CCIN Chairman is the competent authority to sign the employment contracts for contractual agents;

- decide of the internal promotion of the CCIN agents within the framework of the Government's budget;

Moreover, the Agreement prescribes formally that the *a priori* expenditures control must not be a control of opportunity but must remain a pure control of legality.

3. Enforcement means and mechanisms

Chapter III of the Act (Articles 18 and 19) provides for enforcement means and sanctions as regards the legality of files. Articles 13 to 15 of the Sovereign Ordinance n°2.230 provide also details on investigation and investigators.

- According to the Article 18 of the Act, members appointed by the CCIN in accordance with the conditions defined by the last paragraph of Article 13 of the Sovereign Ordinance 2.230, have access, from 6 am to 9 pm, to the places to be controlled. They shall have an official letter of appointment from the CCIN Chairman and they can request to investigate any document or person they consider necessary for the investigation.

- Article 19 of the Act provides for administrative sanctions that CCIN shall pronounce in case of non compliance with the Act (warning or formal notice ordering the ending of irregularities or the elimination of their effects).

In case of irregularities constituting criminal offences, the CCIN shall be passed on without delay to the Prosecutor General by the Chairman of the Commission. Moreover, if the controller has not complied with the letter of formal notice, the Presiding Judge of the Court of First Instance, to whom the matter shall be referred by the Chairman of the Commission, ruling in emergency proceedings, shall order any appropriate measures to end such irregularities or to eliminate the effects thereof, without prejudice to criminal penalties incurred or applications for compensation from data subjects having suffered harm. A fine may also be issued with this decision.

- Articles 21 to 23 of the Act provide for penalties related to infringements of the rights and provisions of the Act. All this penalties shall lead to the ceasing of the effects of the declaration or authorization and removal from the Automated Data Processing Register.

In the light of all this, the Working Party considers that the objective to deliver a good level of compliance with the rules is achieved only in part. In particular, it encourages Monaco authorities to adopt provisions related to a more effective implementation of the structural and financial independence of the CCIN and to enhance the enforcement powers vested in the authority as regards compliance by the public sector and, more generally, the measures to be imposed on data controllers that fail to comply with the law apart and beyond from the imposition of criminal penalties via judicial authorities. The Working Party would like to refer, in this connection, to the interpretation of the concept of "independence" of a data protection authority set out in the judgment C-518/07 of the Court of Justice of the European Union.

b) **To provide support and help to individual data subjects in the exercise of their rights:** The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

Apart from the above considerations as regards the CCIN independence, the Working Party observes that the legislation of Monaco has introduced various mechanisms designed to comply with this objective.

In particular,

- The CCIN is charged to receive complaints (Art.3) related to infringements of their rights or other provisions of the law (security breach, consent transfer etc.). These complaints can initiate an inspection by the CCIN and might lead to the opening of an administrative sanction proceeding.
- The authority has also the duty to inform individuals on their rights, to report to the Prosecutor General facts constituting offences of which it becomes aware in carrying out its duties, to issue warnings or formal notices to data controllers, for the purposes and under the conditions laid down by this Act, to be a party to legal proceedings for the purposes and under the conditions laid down by this Act etc. (Art.2).
- According to the Article 16 of the Act the data subject has a right to obtain a copy of the information collected, rectified etc. on him without any charges.
- As we have seen above the CCIN has the power to control the application of the Act, to investigate (Article18), to be a party to legal proceedings for the purposes and under the conditions laid down by this Act, to pronounce administrative sanctions etc.
- As also seen above, the CCIN has been consulted 159 times during 2010 which is rather satisfying in the view of the size of the country and the only second year of functioning under the new rules.

Therefore, the Working Party considers that the legislation of the Principality of Monaco offers sufficient mechanisms to provide assistance and support to individuals.

c) **To provide appropriate redress to the injured party where rules are not complied with:** This 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.

According to Article 3 of the Act any natural or legal person whose rights have been infringed, or persons having reason to believe that such rights have been infringed, may refer the matter to the Chairman of the CCIN in order, if appropriate, to implement the measures laid down by the Act, as for example a warning or a formal notice.

If those measures remain unheeded upon expiry of the period given, the Presiding Judge of the Court of First Instance, to whom the matter shall be referred by the Chairman of the CCIN, ruling in emergency proceedings, shall order any appropriate measures to end such irregularities or to eliminate the effects thereof, without prejudice to criminal penalties incurred or applications for compensation from data subjects having suffered harm. A fine may also be issued with this decision (Art.19).

It worth noting that the CCIN has no power to impose penal sanctions but it has the power to pass on to the Prosecutor General irregularities constituting criminal offences without delay.

Furthermore, the Court has the power to impose the following penalties provided by Articles 21 and 22 of the Act:

- One to six months of imprisonment and 9 000 up to 18 000 Euros fine (or one of them) for infringements of principles relating to the status of personal data and conditions for the lawful processing, of voluntarily opposition to communicate to a data subject their personal data, or to amend or delete any of such information which has proved to be imprecise, incomplete, equivocal or collected in violation of the law, lacks of attention related to security measures, conservation after provided deadline, illegal transfer etc.

- Three to twelve months of imprisonment and 18 000 up to 90 000 Euros fine (or one of them) for infringements of sensitive data processing provisions, of illegal collect, for deliberately preventing or hindering investigations, for communication of wrong documents to investigators, etc.

Moreover, the Court has the power, according to Article 23 of the Act to order the confiscation and destruction, without compensation, of media containing incriminated personal data and to prohibit re-registration for a period not exceeding three years and of no less than six months. It may also order a legal person governed by private law to be constrained, jointly and severally with their corporate representative, to pay a fine issued against the latter.

Therefore, the Working Party believes that the legislation of Monaco sufficiently guarantees the right of the data subject to be compensated for any damage infringing upon his rights or property as a consequence of the illicit processing of his personal data.

3. RESULT OF THE ASSESSMENT

In conclusion, pursuant to all the above and to compliance with the Agreement, the Working Party considers that the Principality of Monaco guarantees 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.

At the same time, the Working Party encourages the Monaco authorities, to take into account the recommendations contained in this opinion, particularly those regarding:

- The definition of missing concepts provided by the Directive 95/46 (e.g. “filing system”, “third party”, “processor”, “data subject consent”);
- The need to clarify how the provisions of the Act are applicable to legal persons in the light of the initial scope of application of the Act as defined under Article 1.
- The need to clarify the right for data subjects to be informed in a timely manner (especially when data have not been obtained directly from the data subject), and to object without legitimate basis to processing for direct marketing purposes as the current wording of Articles 13 and 14 of the Act does not expressly mention the term “without legitimate basis”.

- The desirability of enhancing the enforcement powers vested in the authority as regards compliance by the public sector and the measures to be imposed on data controllers that fail to comply with the Act apart and beyond from the imposition of warnings, formal notices and criminal penalties via judicial authorities;
- The establishment of the mechanism of independent data privacy officers, in order to assure a better compliance of controllers with the Act.
- The constant consideration of European Commission decisions and Article 29 Working Party documents as regards their assessment about an adequate level of data protection in third countries;

Finally, the Working Party congratulates the CCIN and the Monaco Government for the signature of the Agreement ensuring independence of the Data Protection Authority (CCIN) and invites both parties to strictly respect the commitments resulting from its terms.

Done at Brussels, on 19 July 2012

For the Working Party
The Chairman
Jacob KOHNSTAMM