DATA PROTECTION LAWS OF THE WORLD

Monaco

MONACO

Last modified 10 January 2023

LAW

Within the Principality of Monaco (Monaco) data protection is regulated by Data Protection Law n° 1.165 of December 23, 1993, modified from time to time and notably by Law n° 1.353 of December 4, 2008 and most recently by Law n°1.462 of June 28, 2018 (the "**DPL**"). Furthermore, article 22 of the Monegasque Constitution protects the right to privacy and the secrecy of correspondence of every citizen.

Further, Monaco is part of the Council of Europe and entered into Convention n° 108 of the European Council of January 28, 1981 for the protection of individuals in the context of automatic processing of personal data, and into its protocol addendum regarding the controlling authorities and cross-border flows of data, effective from April, 1st 2009.

Monaco is not part of the EU and did not adopt Data Protection Directive 95/46/EC (hereinafter referred to as the "**European Directive**") or its successor the General Data Protection Regulation (Regulation EU 2015/679) of April 27, 2016 (hereinafter referred to as "**the GDRP**").

As a consequence, the European Commission does not consider Monaco as ensuring an adequate and sufficient level of protection in conformity to the Article 25 of the European Directive.

To address this issue, some of the European standards, and notably the European definition of "**personal data**", have already been transposed into Monegasque law by legislations dealing with the automated processing of personal data, in particular:

- Law n°1483 of December 17, 2019, regarding the creation of a digital identity (and thus, of a digital identification number) for citizens and residents of Monaco and, within this context, of a Monegasque National Register of Digital Identity, and
- Law n°1482 of December 17, 2019, regarding the digital economy in general.

A new draft law incorporating some of the European standards is also expected shortly.

It is also important to note that, pursuant to article 3.2. of the GDPR, the GDPR is already applicable to companies established in Monaco that process personal data of persons (or "**data subjects**") residing in the EU where such processing is related to (i) the supply of goods or services to such persons (irrespective of a payment for such supply) and (ii) the monitoring of their behavior taking place within the Union. It shall be noted that in such a case, the company established in Monaco may be required to designate in writing a representative in the European Union (article 27 of GDPR).

DEFINITIONS

Definition of personal data

Under the DPL, personal data is defined as data enabling identification of a determined or determinable person. Any individual who can be identified, directly or indirectly, notably by reference to an identification number or to one or more factors specific to their physical, psychological, psychological, economic, cultural, or social identity is deemed to be determinable.

Definition of sensitive personal data

While not expressly defined under the DPL, sensitive personal data is considered to be personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health / genetic data, sex life, data concerning morals or social matters.

Definition of data processing

Under the DPL, data processing is defined widely as any operation or set of operations performed on such data, whatever the process used (including collection, recording, organization, modification, storage, extraction, consultation, destruction, as well as exploitation, interconnection or reconciliation, transmission, broadcasting).

Definition of the data processor/controller

Under the DPL, the person in charge of the processing or "**Data controller**" shall be considered as any person (natural or legal entity governed by private or public law) who alone or jointly with others, determines the purpose and means of the processing and who decides of its implementation.

Definition of the data subject

Any person whose personal data are processed.

NATIONAL DATA PROTECTION AUTHORITY

The Monegasque regulator is the Commission for Control of Personal Data (*Commission de Contrôle des Informations Nominatives* or "**CCIN**") whose composition was recently amended by Sovereign Ordinance n°8.575

The CCIN has different missions and powers, which mainly include (i) a mission of registration and examination of cases (e.g. it receives declarations of processing, expresses advices and opinions, issues authorizations when needed), (ii) a mission of council and proposal (e.g. it makes proposals to the competent authorities and recommendations, informs the data subjects of their rights and obligations, publishes reports) and (iii) a mission of control and investigation.

REGISTRATION

Data controllers, who process personal data must notify the CCIN and request approval so that their processing of personal data may be registered. Any changes to the processing of personal data will require the registration to be amended. Concerning data controllers who are legal persons governed by public law, public authorities and bodies governed by private law with a mission of general interest, the decision shall be taken by the competent authorities or bodies following a reasoned opinion from the CCIN. A recent Ministerial Order of 18 March 2021 has brought some changes to this procedure.

Any natural or legal entities governed by private law who intend to implement automated data processing including personal information must first complete the required procedure with the CCIN.

There are four possible procedures to follow:

- Ordinary declaration (all nature or legal persons governed by private law usually fall under the ordinary declaration procedure);
- Simplified declaration (all processing compliant to a referenced Ministerial Order and only when it is clearly established that the processing operations do not adversely affect the rights and freedoms of the data subjects);
- Authorization request (only for automated processing of personal data relating to suspected unlawful activities, offences or security measures or including biometric data required to check persons' identities, or for the purpose of surveillance);
- Legal advisory request (only processing relating to research in the field of health - excluding biomedical research and for

processing implemented by natural or legal persons governed by public law, public authorities, organizations governed by private law entrusted with a mission of general interest or a concessionaire of public utility).

The data controller must decide which procedure is the most adapted to the processing he wants to implement. To do so, he needs to analyze the purpose of the processing, and depending on this purpose, complete one of the aforementioned procedures (ordinary request, simplified request, authorization request, or legal advisory request).

The notification to the CCIN should include at least the following information:

- What data is being collected
- Why the data will be processed
- The categories of data subject
- Whether the data will be transferred either within or outside the Monaco.

DATA PROTECTION OFFICERS

There is no requirement in Monaco for organizations to appoint a data protection officer.

However, appointing a data protection officer is viewed by the CCIN as evidence of a company's measure taken in order to ensure compliance with the data protection legislation. In practice however, companies in Monaco do not generally appoint data protection officers.

When appointed in these companies, he is usually responsible for informing and advising the members of the entity on the legal obligations regarding data processing and for cooperating with the CCIN.

COLLECTION & PROCESSING

Data processing must be justified by at least one of the following bases:

- The data subject's consent
- A legal duty imposed to the data controller
- A public purpose
- The performance of a contract entered into between the data controller and the data subject
- The data controller's legitimate interests, unless the data subject's fundamental rights and liberties outweigh the controller's legitimate interests

If sensitive personal data is processed, at least one of the above bases must be met plus one from an additional list of more stringent conditions (determined in Article 12 of DPL).

Additionally, the data controller must provide the data subject with fair processing information. This includes information about the identity of the data controller, the purposes of processing, the identity of recipients, the right to oppose, access and amend their data and any other information needed under the circumstances to ensure that the processing is fair.

TRANSFER

Monaco is not part of the EU, so the DPL does not distinguish between EEA jurisdictions and non-EEA jurisdictions.

However, the DPL provides that the transfer of data is authorized for cross-border access, storage and processing of data only to a country which offers equivalent data protection and reciprocity (and in particular circumstances, including for example when the

data subjects gave his consent for such transfer or when the transfer of data is necessary to save his life or a public interest).

The CCIN has established a list of the countries deemed to offer equivalent protection and reciprocity.

Data transfers to countries with an adequate level of protection are not subject to the authorization by the CCIN.

The CCIN has adopted a position of principle and decided that all personal data transfers to a country or an organization which does not ensure an adequate level of protection should, in any event, be submitted to the Commission in the form of a transfer authorization application. Subsequently, the CCIN affirmed that it is necessary to submit a transfer authorization application to the Commission if personal data will be accessed from a country that does not have an adequate level of protection.

GDPR has an impact on data transfers to and from Monaco. Two situations must be distinguished:

- Companies of the European Union that want to send data to Monaco:

  They should no longer have to carry out any specific formalities with their supervisory authority as long as tools to protect the data are put in place between the European data controller and his subcontractor or subsidiary, notably:

  - An approved code of conduct pursuant to Article 40 of the GDPR;
  - An approved certification mechanism pursuant to Article 42 of the GDPR.
  - Standard data protection clauses approved by the European Commission (art.46);
  - Binding corporate rules (art.47);

- Companies that want to send data from Monaco

As described above, they are still subject to the data transfer formalities of the CCIN if they wish to send data to a country which does not have an adequate level of protection.

SECURITY

Data controllers must take appropriate technical and organizational measures designed to protect against unauthorized or unlawful processing, accidental loss or destruction of, or damage to, personal data.

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 engages a service provider to process personal data, they must ensure that the service provider is able to comply with the obligations laid down in the two previous paragraphs.

The implementation of processing by such service provider must be governed by a written agreement between the subcontractor and the data controller that stipulates specifically that the service provider and his employees work under the sole directive of the data controller, and that he is also accountable for the obligations relating to the security of the processing.

BREACH NOTIFICATION

There is no mandatory requirement in the DPL to report security breaches or losses to the CCIN or to data subjects.

ENFORCEMENT

The CCIN and Monegasque Courts are responsible for enforcing the DPL. If the CCIN becomes aware that a data controller is in breach of the DPL, it can serve an enforcement notice requiring the data controller to resolve the non-compliance. Failure to comply with an enforcement notice is a criminal offense and can be punished on conviction with imprisonment of one month to one year or a fine of between €9,000 and €90,000 or both.

Sanctions remain rare. The CCIN website only mentions one decision of sanction dated July 18, 2017, which was a warning and the fixation of an action plan to implement corrective measures, against a Monegasque company which didn't submit to the CCIN a request to conduct automated processing of personal data.

ELECTRONIC MARKETING

Prior to implementing any electronic marketing activity the CCIN must be notified, as electronic marketing activities may use personal data. The DPL does not prohibit the use of personal data for the purpose of electronic marketing *per se*. However, when implementing electronic marketing activities a company must respect the provisions of Articles 1, 10-1, 10-2 and 14 of the DPL.

The automated or non-automated processing of personal data must not infringe the fundamental rights and freedoms enshrined in Title III of the Constitution.

When marketing, 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
- Adequate, relevant and not excessive in relation to the purposes for which it is collected and / or further processed
- Accurate and, if necessary, updated; every reasonable step must be taken to ensure that data which is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further processed, is erased or rectified
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed.

Processing of personal data must be justified by one of the following bases:

- By consent from the data subject(s)
- By compliance with a legal obligation to which the data controller or their representative is subject
- By it being in the public interest
- By the performance of a contract or pre-contractual measures with the data subject
- By the fulfillment 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

Data subjects from whom personal data is collected must be informed of all of the following:

- The data controller's identity and, if applicable, the identity of their representative in Monaco
- The purpose of processing
- The obligatory or optional nature of replies
- The consequences for data subjects 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 disclosure to and use of personal data by a third party, or the disclosure for the purposes of the third party's commercial use, including marketing

ONLINE PRIVACY

Prior to the use of traffic data, location data and cookies the CCIN must be notified. The use of traffic data, location data and cookies will have to comply with the provisions of the DPL.

In its Deliberation No. 2019-083 of May 15, 2019, the CCIN has specified the main principles applicable to the methods of depositing cookies and other tracers on the terminals of network users.

In this recommendation the CCIN insists on the requirement to insert a banner appearing as soon as an Internet user arrives on the visited site. It is also requested that no cookie other than those necessary for the operation be deposited in the user's terminal without its consent.

The banner must not be solely for information purposes but must allow the approval or deactivation of the deposit of cookies directly on the site by a positive action of the user.

According to the CCIN, the employer cannot access the contents of private messages sent or received from the professional e-mail system without the employee presence and agreement.

However, in order for messages to be considered private, it is necessary for employees to identify them as such for example by specifying in the message's subject key words such as "private", or "personal".

KEY CONTACTS

Gordon S. Blair Law Offices
gordonblair.com/

Gilbert Delacour
CEO
Gordon S. Blair Law Offices
T +377 93 25 84 00
gilbertdelacour@gordonblair.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.