

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

New belgian data protection law follows the EU Directive closely

Louveaux, Sophie

Published in:
Privacy Law and Business

Publication date:
1999

Document Version
Publisher's PDF, also known as Version of record

[Link to publication](#)

Citation for pulished version (HARVARD):
Louveaux, S 1999, 'New belgian data protection law follows the EU Directive closely', *Privacy Law and Business*, no. 47, pp. 9-11.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

New Belgian Data Protection Law follows the EU Directive closely

THE NEW BELGIAN DATA PROTECTION LAW contains few surprises as it reproduces nearly word for word the terms of the EU Data Protection Directive itself. Sophie Louveaux examines what has been changed.

Even though the European Data Protection Directive (95/46/EC) is, to a certain extent, precise, it contains a number of undefined and vague terms and leaves the member states with a certain "margin for manoeuvre" in their achievement of the harmonisation of the national data protection laws¹.

Article 4.1.a provides that when a controller is established on the territory of several member states, he must take the necessary measures to ensure that each of the establishments complies with the obligations laid down by the national applicable law. Furthermore, the directive's recitals (§ 22) provide that the member states shall more precisely define in the laws they enact, or when bringing into force the measures taken under the directive, the general circumstances in which the processing is lawful. In particular article 5, taken in conjunction with articles 7 and 8, allows member states to provide for special processing conditions for specific sectors and for various categories of data covered by article 8.

Although Belgium can boast that it has nearly respected the deadline for implementation of the directive, it has made little use of this room for manoeuvre given by the directive, but has reproduced nearly word for word the terms of the directive itself². I will briefly examine the main components of this new law, highlighting the principal changes to the previous legislative system.

AMENDMENT TO THE PERSONAL DATA DEFINITION

The new Belgian law reproduces the definitions of the EU Data Protection Directive. As a general observation one can point out that the definitions convey relatively abstract and general concepts³. The law thus aims at being able to adapt itself to the evolution of new technologies.

An interesting innovation in the new Belgian law is the introduction of the concept "identifiable person" in the definition of personal data. According to the directive's recitals and the explanatory memorandum of the new Belgian law, an individual is identifiable when he can be identified either directly or indirectly by any reasonable means. Therefore, is data that has been encrypted, and for which the controller himself does not possess the means of decoding the data, still considered as personal data if a third party retains these means? Anonymous data will only be excluded from the scope of the law if the anonymous character of the data is absolute, and if there are no reasonable means in use to break down the anonymity.

FEW CHANGES TO THE PRINCIPLES

The new Belgian law does not introduce any fundamental changes with regard to the general data protection principles of fairness,

purpose limitation, quality of the data and legitimacy of the processing⁴. As far as the principle of fair processing is concerned, article 4 of the new law states that personal data must be processed fairly and lawfully. This principle, though underlying the 1992 law, was not previously described as such⁵.

The purpose limitation principle, according to which personal data must be processed only for specified, explicit and legitimate purposes, was the leading principle in the 1992 law⁶. However, whereas in the 1992 law the compatibility of the use of the data is to be determined according to the purpose of the processing, in the new law the compatibility must be judged according to the purpose for which the data was initially collected. This change will have few consequences as such. Under the old law the purpose of the processing was, in reality, determined at the time of collection of the data since the data subject was to be informed at this time of the purpose for which the data was to be processed. Further processing must not be incompatible with the purpose for which the data was initially collected⁷.

The interpretation of the concept of "compatibility" could create some difficulties. The directive itself does not provide for any guidance on this subject. According to the explanatory memorandum of the new Belgian law, new processing of the data does not necessarily imply a

further collection of personal data from the data subject.

The idea, therefore, is not to require that the controller systematically collects data from the data subject each time the data is processed for a new purpose. In this case, however, the data subject will need to be informed of the processing according to article 9 of the new Belgian law. The 1992 law already provided for this situation. However, the new law requires that the evaluation of the compatibility of the new purpose with the initial purpose for which the data was collected must be judged on a case by case basis, taking into account any relevant elements, in particular the reasonable expectations of the interested person.

The data quality requirements provided for in article 4 of the new law, according to which the data must be adequate, relevant and not excessive in relation to the purposes for which it is collected, were already present in the previous Belgian legislation.

DIRECTIVE'S CATEGORIES FOR LEGITIMATE PROCESSING

Whilst the 1992 law opted for the principle of admissibility under certain conditions of the processing of personal data save for sensitive data, the new Belgian law prohibits, in accordance with the directive, the processing of personal data except in a limited number of situations. In this sense, article 5 of the new law reproduces nearly word for word article 7 of the directive, stating the limited situations in which the processing of personal data is *a priori* permitted⁴.

This new provision implies that the controller will need to check under which criteria, as laid down by the law, the processing falls. The processing of personal data that does not fall within these criteria cannot take place. It is important to note that, according to the Belgian law, the fact that the processing falls within one of the criteria mentioned in article 5 does not necessarily imply that the processing is legitimate in the sense of article 4§1,2°. Articles 4 and

5 of the new law must, therefore, be applied simultaneously.

MUCH EMPHASIS ON CONSENT FOR SENSITIVE DATA

As far as special categories of personal data are concerned, the law makes a distinction between sensitive data in the strict sense (i.e. data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning sex life), health data and judicial data⁵.

With regard to the first category of *sensitive data*, the new law, just as the 1992 law, prohibits the processing of this data apart from in a number of limited situations. In the previous regime, this prohibition could be lifted only by a specific law enacted for that purpose. By contrast, the new law itself expressly states the situations in which the prohibition can be lifted. One of these exceptions is when the data subject gives his written consent to the processing of the data. Belgium did not make use of the opportunity to provide that the data subject's consent could not lift the prohibition to process such data. Yet one can think of a number of situations in which the data subject's consent does not carry the person's free acceptance, for example, in an employer/employee relationship.

As for *medical data*, the 1992 law conditioned the processing of such personal data to monitoring by a health practitioner unless the data subject's written consent had been obtained. The new law maintains this prohibition, but enlarges the scope of the data by referring to "*data relating to health*" rather than medical data, and extends the persons who may process such data to all healthcare professionals (i.e. health care providers). According to the new regime, the collection of such data must, in principle, be obtained from the data subject himself.

Also with *judicial data*, the principle is once more to impose the prohibition of the processing of such data except for in a limited number of cases which the King can determine.

CONTROLLERS' DUTIES AND OBLIGATIONS CHANGE

The new law imposes a number of duties and obligations on the controller, notably a duty to provide information, to notify, and the duty of confidentiality and security of the processing. These duties were already present in the 1992 law.

With regard to the obligation to notify the national supervisory authority, the Commission de Protection de la Vie Privée, prior to any processing of the data, there are no major changes to the present system apart from the terms used, and the simplification of, and exemptions to this obligation. Regrettably the Belgian government has not made use of the possibility of exemption from notification when the controller appoints an internal data protection official⁶. As for the processing of data that may lead to specific risks to the rights and freedoms of data subjects, the King must determine the conditions in which such data may be processed. The appointment of a data protection official could be one of these conditions.

The new law transposes articles 16 and 17 of the directive on the obligation of confidentiality and of security. These articles bring a certain number of changes to the present regime. Notably one notices the suppression of the obligation to write up an '*état*' for each processing of the data⁷. Furthermore, the new law ties in the relationship between the data controller and the processor, requiring the obligation that they write a contract laying down the security measures to be respected and the liability of the processor towards the controller. It is further stated that the processor may act only on the instructions of the controller.

NEW RIGHTS FOR DATA SUBJECTS

The data subject, as in the previous system, is granted a right of access and of rectification. Two new rights are also granted to the data subject in accordance with articles 14 and 15 of the directive: the right to object, and the right not to be subject to an automated individual decision.

The right to object grants data subjects the right to oppose the processing of their data on serious and legitimate grounds relating to their particular situation. It is regrettable that neither the directive nor the Belgian law determines what is to be understood by serious and legitimate grounds. The right of opposition is not *a priori* granted to the data subject in two cases. Firstly, when the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to the entering into a contract, and secondly, if the processing is necessary for compliance with a legal obligation to which the controller is subject. As in the directive, the right to object is granted unconditionally in the case of personal data collected for the purposes of direct marketing.

The introduction of the right not to be subject to an automated individual decision is an innovation in the Belgian data protection regime. Once again, the law reproduces the terms of the directive. The law states that a decision which produces legal effects, or which significantly affects the data subject, may not be taken on the sole basis of an automated processing of the data intended to evaluate certain aspects of his personality. Examples are his performance at work, creditworthiness, reliability and conduct.

This article aims at avoiding situations where decisions would be taken based solely on an automated decision without any human intervention. According to the explanatory memorandum of the new law, there must be some sort of human intervention between the result of an automated processing of the data and the actual decision making. The prohibition of such decisions is lifted either if the decision is taken in the course of a contract or is authorised by law. In both cases the contract or the law must provide for suitable measures to safeguard the legitimate interests of the data subject or which, at least, allow them to put forward their point of view.

TRANSFERS OF DATA TO THIRD COUNTRIES

The law prohibits the transfer of data to third countries, unless these countries provide for an adequate level of protection. In this sense, the law has reproduced the regime laid down by the directive. Similarly, it has provided for the same derogation: data subject's unambiguous consent.

The law further stipulates that the King, after having consulted the national data protection authority, can determine which categories of processing, and under which conditions the transmission of personal data to third countries is not permitted (this can be interpreted as a possibility for the King to establish a black list of third countries). The King has also been given the power to authorise, after having consulted the national data protection authority, a transfer or a category of transfers to countries which do not ensure an adequate level of protection. This is possible when the controller offers adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals.

Footnotes:

¹ *The recitals of the directive mention that the Member States will be left with a "margin for manoeuvre" (see §9).*

² *The Belgian law on data protection implementing the European directive 95/46/EC was adopted by the Chambre des Représentants on 12th November 1998 (see Doc. Parl., 1997-1998, n° 1566/13). Once ratified, it will come into force at the date established by the King modifying the existing law of 8th December 1992.*

³ *See notably the definitions of "processing" and of "personal data".*

⁴ *Article 7 of the new law reproduces nearly word for word the terms of article 6 of the directive.*

⁵ *It does, however figure in article 5 of the Council of Europe Convention 108 of the 28 January 1981 for the Protection of Individuals with*

regard to Automatic Processing of Personal Data.

⁶ *See article 5 of the 1992 law.*

⁷ *Article 4§1, 2° of the new law.*

⁸ *The EU Data Protection Directive left no choice for the member states concerning the possibility of including further criteria for making the processing legitimate, nor for excluding certain criteria listed in article 7 of the directive. The directive did, however, enable the member states to be stricter in their formulation of the provided criteria. Belgium has not, however, made use of this possibility.*

⁹ *See articles 6, 7 and 8 of the new law.*

¹⁰ *See article 18 of the directive on this possibility.*

¹¹ *According to article 16 of the previous law, the controller was under the obligation to write an 'état' which stated the nature of the personal data which was being processed by him, the purpose of the processing, the possible links and interconnections between the data and any consultations of the data and the persons or categories of persons to whom the data was transmitted. This 'état' was conceived as an internal element of control for the controller himself, and as an element of external control because the national data protection authority (Commission de protection de la Vie Privée) could request it at any time.*

i

This report was written by Sophie Louveaux, Centre de Recherches Informatique et Droit, Faculté Notre Dame de la Paix, Rempart de la Vierge 5, 5000 Namur, Belgium, Tel: + 32 81 724769, Fax: + 32 81 228858, e-mail: sophie.louveaux@fundp.ac.be