Expertise Areas :

> New Technologies, Privacy & ICT
> E-payment, E-finance & Internet Banking
> Intellectual Property
> E-health & Telemedicine
> Cinema, Media, Entertainment, Sport & Gaming
> Commercial & Company law, Competition law

www.ulys.net

Warning: The purpose of this information sheet about the new Regulation on the protection of personal data is to introduce readers to its main innovations and to enable the best use of the database/tool made available online by Ulys, which contains the first article-by-article commentary on the GDPR.

During the presentation about the new Regulations, the reader is free, by clicking on an article of their choice, to access each provision, to compare the previous state of the law (in Belgian law and French law) with the new regulations and the relevant recitals, as well access to a comparison table of the legal text evolution.

The Regulation version having been used in the development of the data bank of 'GDPR Experts' of ULYS is the text published on 6 April 2016 and adopted in plenary this 14th of April.

General comments on GDPR

1. Introduction. The general Regulation on data protection marks without any doubt is a spectacular breakthrough for the protection of natural persons in the digital environment they live in today.

The Regulations were drafted in response to number of factors; the text tries to improve the protection of the persons concerned and is an answer to requests for amendment to the regime from both the supervisory authorities and officials, taking into account the experience gained during the past 20 years and the changes in technology since the Directive of 1995.

Article-by-article comments – such as those assembled on the present site – cannot be a clear indicator of the changes which have occurred without a review of the overall text.

For this reason, you will find below a concise - but nevertheless full – detail of the text, allowing readers not only an abbreviated vision of the draft text but also a focus on its basic directions.

2. A regulation that leaves significant discretion to the Member States. What initially becomes obvious is that the Regulation is supposed to have unified all the rules applicable in the various Member States but leaving them a lot of flexibility in the regimes implementation.

This flexibility is most apparent at the level of exceptions open to the Member States with respect to the common principles.

There are many examples of this. For example, Article 6 § 2 allows the Member States to adapt the provisions of the Regulation in order to ensure conformity with legitimate interests in specific processing situations by reference to a legal right or public interest such as freedom of expression, Article 8 , § 1 allows the Member States to envisage an age below 16 years - but not below 13 years - allowing children to give consent for processing without parental authorization, Article 9 relating to sensitive data widely

Thierry LEONARD
Associate lawyer (SPRL)
Lawyer at Brussels Bar
thierry.leonard@ulys.net

Didier CHAUMONT
Lawyer
didier.chaumont@ulys.net

Our Ref. : 15/00120
Your Ref. :

Date
20.04.2016

BRUSSELS

224, av. de la Couronne
1050 Brussels
Phone: + 32 (0)2 340 88 10
Fax: + 32 (0)2 340 35 80

Civil society in the form of SCRL
RPM Brussels
VAT: BE 0476.702.936

PARIS

33, rue Galilée
75116 Paris
Phone: + 33 (0)1 40 70 90 11
Fax: + 33 (0)1 40 70 01 38

Affiliate registered at the Paris Bar
in application of Directive 95/5/EC

allows national legislators to determine the exceptions permitted to the principle of prohibition of processing and the Member States have the power to maintain or to introduce more specific provisions, including limitations, with regard to genetic, biometric, or health-related data (see) Article 9 , § 4), differences between the Member States can occur with respect to the data processing related to convictions or criminal offenses or security measures as far as the conditions of data processing are determined in the national legislation (terms of public authority controls or specific legislative authorization (Art. 10), etc.)

3. The Regulation recitals. The Regulation begins with a very long list of **recitals** as part of its preamble.

As increasingly happens with EU Legislation, the reader of the Regulation faces an inflation of 'recitals': near 173 extending over almost 100 pages of the 261 pages in the latest version of the text. That is, it looks like they have not finished revealing their secrets.

As there are traditional recitals of motivation, explaining the reasons and justifications for the intervention of the European legislature in the field, notably by Regulation (see recitals 1 and seq. spec. recitals 9 and 10 which justify the margin of maneuvering left to the Member States notwithstanding the choice of a Regulation to legislate), there is usually a motivation or even an explanation of the normative provisions contained in the Regulation. For example, recitals 42 and 47 concerning Article 6 (Lawfulness of Data Processing)s provide clarification on the free nature of the consent and the consideration of the legitimate interests of the person responsible for the processing in their opposition to the rights and freedoms of the person concerned, respectively.

If as a rule, these recitals don't have a normative value by themselves[1], it should be noted that there are vague normative attempts shown by the fact that some formulate and describe additional content to that provided by scpedifically outlines in the relevant provisions (see for instance recital 91 that clarifies that the impact analysis is not mandatory if the data processing in question is protectedby professional confidentiality, such as the processing of personal data of patients or clients by an individual doctor, a health professional, a hospital or a lawyer or recital 171 which states that processing already in progress at the time of the Regulation entering into

[1] The interinstitutional agreement of 22 December 1998 on the common guidelines related to the quality of drafting of Community legislation, in its section 10, indicates that "the recitals are intended to motivate concisely the essential provisions of the instrument without reproducing or paraphrasing the wording. They do not contain any normative provisions or political exhortations. ". As to the scope of the recitals and the questions they trigger: S. Lemaire, « Interrogations sur la portée juridique du préambule du Règlement Rome I », Rec. Dalloz, 2008, p. 2157 et s. (Questions on the Legal Scope of the Preamble of the Roma I Regulation)

force on 25 May 2016, that is, on the twentieth day following its publication in the European Union Official Journal on 4 May 2016, must be rendered compliant within two-years of this date , that is, not later than 25 May 2018). We should however be aware that often the text of the recitals was included for those parts that could not find sufficient political consensus to be inserted into the main text. This is obviously true as to the rules which, having first been put into the body of the text, were then disqualified and integrated in the recitals, for lack of agreement on their content (for a significant example see recital 154 partially covering the contents of the former article 80 aa entitled Personal Data Processing and Re-use of Public Sector Information).

4. The Regulation scheme. The Regulation is divided into chapters and sections, as follows:

- Chapter I: General provisions

- Chapter II: Principles

Chapter III: Rights of the data subject

Section 1: Transparency and modalities

Section 2: Information and access to personal data

Section 3: Rectification and erasure

Section 4: Right to object and automated individual decision-making

Section 5: Restrictions

- Chapter IV: Controller and processor

Section 1: General obligations

Section 2: Security of personal data

Section 3: Data protection impact assessment and prior consultation

Section 4: Data protection officer

Section 5: Codes of conduct and certification

- Chapter V: Transfers of personal data to third countries or international organisations

- Chapter VI: Independent supervisory authorities

Section 1: Independent status

Section 2: Competence, tasks and powers

- Chapter VII: Cooperation and consistency

Section 1: Cooperation

Section 2: Consistency

Section 3: European data protection board

- Chapter VIII: Remedies, liability and penalties

- Chapter IX: Provisions relating to specific processing situations

- Chapter X: Delegated acts and implementing acts

- Chapter XI: Final provisions

We admit that we will not always understand the logic of the plan followed. Why have they, for example, relegated the substantive provisions relating to liability as well as the special rules in certain situations (restriction of freedom of expression, rules applicable to the employment relationship, etc.) at the end of the Regulation, amid the procedural rules and those of the specific jurisdiction of European law? Chapter IV should have indicated more clearly the obligations of the controllers and the processors actually concerned.

5. Concerning the general provisions (Chapter I). There are few changes to the general provisions, which include the Regulation scope and objectives (Art. 1) andthe material scope (Article 2).

On the other hand, the territorial scope (Art. 3) of the Regulation (and also the applicable national laws) has been modified, taking into account the difficulties that appeared in applying the rules of protection to the controllers outside the EU. As soon as the processing activities are related to the supply of goods or services to individuals located in the territory of the Union or connected with the observation of human behaviour, as long as the behaviortakes place within the Union, the controller and/or the processor will be subject to compliance with the Regulation.

It should be noted that the criterion of the establishment location covers henceforth both the controller and the processor.

The definitions were also significantly strengthened, even if those taken from the Directive remained fairly unchanged (Art. 4).

6. Concerning the principles relating to the personal data processing (Chapter II). Article 5 of the Regulation contains and reinforces the principles relating to the personal data processing that are set out in Article 6 of the Directive by including the following new features:

- the principles of loyalty and lawfulness of the data processing are supplemented by the statement of a general principle of transparency (Art. 5, § 1, a);

- A new exception is recognized with respect to the prohibition of pursuit of purposes incompatible with the original purpose (Art. 5, § 1,b): archiving in the public interest;

- the principle of data minimisation is accepted whereby only the personal data which appear necessary for achieving the purpose can be processed (Art. 5, § 1, c).

- the obligation for security and confidentiality of processing (Art. 5, § 1, f), requiring the controller to ensure appropriate security and confidentiality.

Article 6 contains the now classic processing legality-related assumptions: consent of the subject, performance of a contract, compliance with a legal obligation, protection of the vital interests of the person concerned or of another person, the implementation of a task in the public interest or related to the implementation of a task in the public interest and finally the balance of rights, legitimate interests and freedoms of the controller or of a third party on one hand, and of the persons concerned on the other. Let's notice that logically, this last assumption is excluded for the responsible public authorities, which highlights, as far as they are concerned, the strict application of the processing legality that they pursue.

The new purposes that are incompatible with those initially pursued are prohibited, except in special cases for the purposes of archiving in the public interest, historical and scientific research and statistics (in this regard, see Article 5, § 1, b). Despite an intense debate about these provisions, the only change to the evolution of the purposes is the acceptance in the event of compatibility only, except when there is consent of the person concerned or where a specific legal text allows this, given the conditions of article 23, § 1 (Art. 6, § 4).

On the basis of the definition contained in Article 4 , 11), Article 7 of the Regulation defines various consent-related rules: burden of proof, level of accuracy in a written text of a more general coverage, a generalized right of withdrawal, assessment of the consent as to whether it is a condition for the performance of the contract.

Article 8 , introduces a rule of specific protection for children's consent - an undefined concept - in the case of the offer of a service by the information society: as a rule, their parents are those who have to give consent to the processing.

The sensitive data processing is covered by two specific provisions (Section 9 and Section 10).

The material scope is not very different from that of the Directive (see however the inclusion of genetic and biometric data). The exceptions are however extended to processing needed for reasons of public interest in the public health area (see Article 9, § 2, i)) as well as to processing needed for archiving purposes in the public interest or for historical, statistical or scientific purposes in the conditions set out in Article 89 and on a legal basis of the Union or the Member StateArticle 9, § 2, j).

It should be noted that the Member States may maintain or introduce more specific provisions, including restrictions regarding genetic, biometric or health-related data (Article 9 § 4).

The processing of data relating to convictions for criminal offenses or security measures is only permitted as long as it is performed under the control of the public authority or is authorized by the Union law or by national law (Article 10).

Finally, Article 11 of the Regulation introduces a specific provision concerning the processing which does not require (more) identification of the persons concerned. The controller is not required to process other identification enabling information and where the individual cannot be identified from the information held, the controller normally will not be required to act on the listed rights of these people (access, erasure, restriction to processing, etc.).

7. Regarding the rights of the data subjects (Chapter III)

Two significant trends appear with respect to the regulation of the rights of the data subjects:

(1) increasing the duty for transparency . Article 12 requires the controller to provide procedures and mechanisms for the data subjects to exercise their rights. A general principle of transparency is proclaimed: any information to the public or to the data subject should be easily accessible and easy to understand in a concise and transparent form, and formulated in clear and simple terms - in particular for any information addressed specifically to a child.

The provision sets out the information modalities (written or otherwise). The maximum time limits for response are set according to the rights in question. The principle of free exercise of rights is widespread.

The information duty in the case of collecting from a data subject is still extended to the additional information (the legitimate interest that justifies the processing, data transfers to third countries, the right to claim in front of the control authority, etc.). Additional information may need to be disclosed if needed for fair and transparent processing (the period of data storage, or at least the elements enabling their determination, the existence of all the rights recognized as applying to a data subject, the existence of automated decision-making including profiling and meaningful information about the logic involved and the envisaged consequences of such processing for the data subject, etc.) (Art. 13).

A similar disclosure scheme is organized by the Article 14 in cases of collection from a third party. Exceptions are then provided (the data subject already has the information, if proven to be impossible or would require disproportionate efforts, etc.).

The right of access envisaged byArticle 15 is not actually innovative. The data subject shall have the right to obtain confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data. Specific information must be given pursuant to the right of access. If so requested, the data subject is entitled to be issued a copy of the data.

The right to rectification under Article 16 of the Regulation is also in line with the provision previously contained in the Directive.

Article 19 sets up a notification obligation of the data controller that requires them to communicate to each data recipient any rectification, erasure or restriction of processing on the basis of Article 16, Article 17 (1) and Article 18 of the Regulation. The controller, however, can avoid this obligation if they prove that such communications is impossible or involves disproportionate effort.

(2) *recognition or consecration of new rights granted to the data subject* The new web2.0 environment and social networks in particular have increased the loss of control of people on the information about them. The new regulation therefore tries to allow the data subject to regain the control on the data projected and disseminated in their virtual peregrinations, recognizing "new" rights to those concerned by the data.

Amongst the new rights under the Regulation, the following should be specifically retained:

- the right to be forgotten and to erasure - inspired by the Costeja- case law (Article 17). The major contribution of the future Regulation is to establish hypotheses to obtain erasure and the conditions for exercising the right to be forgotten. To note for example, the requirement to inform the third parties to whom the data erased have previously been transmitted for the purpose that they are required to erase any links to such data or copies or reproductions that were made but also the exceptions (exercise of the freedom of expression and information, compliance with a legal obligation, etc.)

- the right to restriction of processing (Article 18) allowing the data subject to suspend the processing and thus, where applicable, the publication of data in various situations: when contesting the accuracy of any data, the period enabling the controller to verify the accuracy of the personal data; if the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead, when the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims, etc.

- The right to data portability is the most innovative right of the future Regulation (Art. 20). The latter appears as an improved right to access, which is associated with a requirement for interoperability and withdrawal. The purpose of the right is to take back the data that was communicated to the claimant and to (cause to) transmit the data via an automated processing system from one controller to another. The exercise of this right is conditioned on the fact that it must necessarily come to automated processing legitimized by the consent of the data subject - either with respect to any sensible data or the need for performance of a contract concluded between the data subject and the controller.

Two other rights have been still reshaped by the Regulation.

The general right to object (Article 21) exercised for reasons relating to the particular situation of the data subject, is only open in the case of processing legitimization based on the necessity of executing a task of public interest (Article 6 § 1, e) or on the basis of legitimate interest overriding the controller or a third party, including the profiling done on these bases (Art. 6 § 1 , f). The Regulation also provides – like Directive did before it– that the data subject may object at any time to the processing of their personal data for marketing purposes, including profiling done for this purpose (Art. 19 § 2).

The right to not be subjected to an automated decision-making is provided for in Article 22 of the future Regulation. This is the decision exclusively resulting from automated processing that produces legal effects concerning or significantly affecting the data subject. It specifically includes profiling. However, this provision extends the possible exceptions to the prohibition. The prohibition is reinforced for decisions based on sensitive data processing in the meaning of Article 9 §1 of the Regulation which are still prohibited unless the subject data has given their explicit consent under Article 9 § 2 a) or if the processing is necessary for reasons of significant public interest within the meaning of Article 9 § 2 g) (Art. 22 § 4).

Finally, the Regulation Article 23 being directly inspired by Article 13 of the Directive states that the Member States may maintain or introduce statutory restrictions to the data subject rights under sections 12 to 22 and Article 34 relating to the notification to the data subject about a breach of personal data and the principles set out in Article 5, provided that those restrictions comply with the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard certain interests that are listed restrictively.

8. Regarding the controller and the processor (Chapter IV). Chapter IV contains two types of provisions: the first type relates to the qualification of the data controller and the processor, their status and internal organization and their reciprocal duties (1), the second type outlines the general and special duties with regard to the implementation of the protection measures provided by the new Regulation that are vested in the mentioned controllers (2) or both (3).

(1) Status, qualifications and reciprocal duties of controllers and processors: Article 26 of the Regulation defines the specific duties of joint controllers who must sign an arrangement between them to determine their respective responsibilities for compliance with the obligations under this Regulation and notify the arrangement contents to the data subjects affected.

The Regulation Article 28 concerns the specific regime of processors. The article extends the previous duties of controllers and processors while organizing a separate plan for the processors with respect to the duties of security set out in Article 32 and seq. The principle remains that of a specific contractual organization between the controller and the processor. The content of the written arrangement - including in electronic format - i.e., the obligations of the processor is greatly extended. The Regulation organizes the question of processing entrusted to third parties - secondary processors

by the direct processor of the processing controller, very common cases in practice.

Article 29 of the new Regulation now states that any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process that data except on instructions of the single controller (regardless of the provision of Article 32, § 4, which includes the processor), unless otherwise specified by the law of the Union or of a Member State.

(2) Duties of the processing controller: The first general duty of the controller is a "general principle of responsibility" (Article 24). The article confirms the special responsibility of the controller in the implementation of the appropriate technical and organizational measures to perform the processing in accordance with the Regulation. To determine this responsibility, account must be taken of the nature, the scope, the context and the purpose of processing as well as the likelihood and the severity of risks with respect to the rights and freedoms of natural persons. The burden of proof of such implementation then rests on the shoulders of the controller.

Two specific duties therefore result and try to give it a more specific content.

According to paragraph 1 of Article 25, the principle of *data protection by design* (the design protection) requires the controller to take measures and appropriate technical and organizational procedures - in both the processing design and implementation - to be in compliance with the Regulation, taking into account the relevant risks. Among these measures, paragraph 1 mentions the minimization (see Article 5, § 1,, c) and the pseudonymization (see Article 4, 5).

The second paragraph of Article 25 addresses the principle of *data protection by default* (default protection). The provision requires the controller to adopt measures to limit by default the personal data processing to what is strictly necessary, with regard to the amount of data processed, their accessibility and the period of their storage.

Article 33 of the Regulation generalizes the duty of notification of data breaches to the supervisory authority by specifying them. Any data breach must be subject to a notification by the controller, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The processor shall notify the controller without undue delay after becoming aware of a personal data breach. The provision also addresses the minimum content of the notification and the deadlines, part of which can be delayed.

Article 34 requires the controller to notify the data subject only when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons in a manner similar to those intended for the supervisory authority. Article 34 § 3 provides, however for various exceptions to the notification to the data subjects.

Article 35 states that where a type of processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data to assess, in particular, the origin, the nature, the scope, the context and the severity of that risk. The provision specifies the assumptions requiring or not such an analysis as well as its content.

The controller must consult the supervisory authority before the implementation of the processing only, and according to the specified terms, when the impact assessment conducted by the controller in application of Article 35 indicates that the processing would result in a high risk in the absence of appropriate measures taken by the controller in order to mitigate the risk (Article 36).

(3) Common duties of the controllers and the processors: In the case of application of Article 3 , § 2, Article 27 of the Regulation requires the controllers and the processors who are not established in the Union to appoint a representative, when the Regulation applies to their processing activities.

In Article 30 of the Regulation, the EU legislature has decided to replace the duty of notification to the supervisory authority by an obligation to the controllers **and** the processors to maintain a record of processing activities under their responsibility. Thus, both the controllers and the processors (and, if applicable, their representatives) will have to keep records for all categories of processing activities under their responsibility, that is, for each processing that they implement. These records will be made available to supervisory authorities at request.

Article 31 of the Regulation establishes a specific duty to the controllers and the processors - as well as to their representative, as appropriate - to cooperate at the request of the supervisory authorities, in the performance of their tasks.

Article 32 of the Regulation includes in essence the Directive related to the duty of security , by extendingthe content of the provisions . The main purpose of this duty remains the implementation of appropriate technical and organizational measures by the controller and the processor to ensure a level of security that is appropriate to the risk. However, these are largely exemplified by the text itself.

Article 37 of the Regulation specifies three cases in which the designation of a data protection officer is mandatory within the organization of the processing controller and processor:

- when the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (Art. 37, paragraph 1, a) ;

- when the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale (Art. 37, paragraph 1, b) ;

- when the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 of the Regulation (Art. 37, paragraph 1, c).

The controller, the processor or associations or other bodies representing categories of controllers or processors may or, where appropriate, must designate a delegate for the data protection if the EU law or the law of a Member State so requires (Art. 37, § 4).

Article 38 imposes - under the title of function ('position') of the data protection officer - to the controller or to the processor a series of obligations to allow the latter to assume the tasks provided for in Article 39 (associate them timely to all questions relating to the data protection, ensure their independence, bind them by an obligation of secrecy or confidentiality...).

The data protection officer receives several minimum tasks described in Article 39: to inform and advise (1); a control task (2); to act as a point of contact with the supervisory authority (3).

Article 40 organizes the system of codes of conduct developed by the bodies representing categories of controllers and processors. They are intended to clarify the terms of application of the Regulation provisions. These codes will be submitted to the supervisory authority which is competent pursuant to Article 55, before submitting them to the European Data Protection Committee if they concern the processing implemented in several Member States (Art. 40, § 5 and 7).

Article 41 authorizes, on the conditions therein specified, an independent body to monitor the compliance with a code of conduct approved and referred to article 40 without prejudice to the tasks and powers of the competent supervisory authority. A specific approval procedure is envisaged.

Article 42 of the Regulation - supplemented by Article 43 - implements a mechanism of certification of controllers and processors required to comply with the protection rules. The certification can be issued only by a specially authorized body in accordance with Article 43 or, where applicable, by the competent supervisory authority, or by the data protection board brought to intervene with, in this case, recognition by a potential European label.

9. Concerning the transfer of data to third countries or international organizations (Chapter V). The rules relating to the transfers of data to third countries have been amended even if the resulting basic principle of the Directive has been maintained: the prohibition to transfer to countries, territories, or international organization which do not ensure an adequate level of protection, even if its statement has been modified. Indeed, Chapter V was intended to set out the cases and the conditions in which such transfers are still allowed.

This 'positive' approach is initially stated in Article 44 of the Regulation. This provision is intended to state the general principle governing the transfers to third countries or international organizations in the EU. These

transfers can only be effected if the controllers and the processors falling under the scope of the Regulation comply with the rules provided for in Chapter V.

The provision gives however a new extension to the rule: transfers of personal data to a third country or to an international organization operated as part of planned or ongoing processing are covered, but also the future processing by the recipient third country to another country or another organization. They must also comply with Chapter V of the Regulation.

From now on, the Commission is the only one to determine if the third country, the territory, one or several areas identified in that third country or international organization in question ensures an adequate level of protection, in application and according to the terms of the Article 45 of the Regulation. The Commission may also revoke, modify or suspend a decision on adequacy if the third country, territory or international organization no longer provides an adequate level of protection.

In the absence of a Commission decision finding an adequate level of protection, Article 46 of the Regulation provides that the transfer can only be done by the controller or the processor if the controller or processor has provided appropriate safeguards. The choice of safeguards is expanded and the national supervisory authorities will be able to intervene in a formalized procedure if the conventional safeguards cannot be implemented for reasons specific to the controller or the processor.

Article 47 of the Regulation addresses the consecration of the system of binding rules to businesses, which can be adopted by groups of companies facing intra-group transfers outside the Union. These binding business rules must meet several conditions defined by Article 47 , § 1 and 2, be approved by the competent supervisory authority and contain a range of information listed in that provision.

It should be noted that the final version of the Regulation introduces a new Article 48 under the terms of which judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data, may only be recognised or enforced in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State.

As in the regime of the Directive, the Regulation provides in its Article 49 specific exemptions for the absence of a decision on adequacy by the Commission (explicit consent, transfer necessary for the performance of a contract between the data subject and the controller, etc.). The essential element of Article 49 is the introduction of a new derogation based on the need for the transfer for the purpose of compelling legitimate interests pursued by the controller or the processor (Art. 49, § 1 *in fine*).

Finally, in relation to the third countries and the international organizations, the Article 50 requires the Commission and the supervisory authori-

ties to take certain measures in order, in fine, to facilitate the application of the data protection principles.

10. Concerning the supervisory authority (Chapter VI). The strengthening of the powers and tasks of the supervisory authorities is clearly one of the strong elements of the revision of the data protection scheme implemented by the new Regulation.

As provided for in the Directive, the Regulation, in its Article 51 , requires the Member States to set up one or several independent supervisory authorities responsible for the monitoring of the application of the Regulation. The purpose of their intervention is clear: on the one hand, to protect the fundamental rights and freedoms of the people during the processing of their personal data and, on the other hand, to facilitate the free movement of data within the Union. They shall also contribute to ensuring the uniform application of the Regulation within the Union. To this end, they must cooperate with each other and with the Commission, in accordance with the mechanisms provided for in Chapter VII.

Article 52 is intended to clarify the conditions guaranteeing the independence of the supervisory authorities, in accordance with the case law of the Court of Justice of the European Union (CJEU, 9 March 2010, C-518/07), and on the basis also of Article 49 of Regulation (EC) No. 45/200135.

Article 53 sets out the general rules of the status applicable to the members of the supervisory authority, in accordance with the case law of the CJEU (see CJEU, 9 March 2010, C-518/07), and on the basis also of article 42, paragraphs 2 to 6 of the Regulation (EC) No. 45/2001 on the processing of data carried out by the institutions and bodies of the European Union.

Article 54 allows the Member States to provide by law the conditions of establishment of the supervisory authorities. Each Member State shall set the terms of appointment of the members of the supervisory authorities.

As to the competences of the supervisory authorities, Article 55 reminds that each authority is competent, on the territory of the Member State in which it falls, to accomplish the tasks and to exercise the powers vested in them and excludes the jurisdiction of another authority known as 'lead supervisory authority' (see Article 56) in some cases, mainly when the processing is carried out by public authorities.

In the case of cross-border processing (see the definition in Article 4, 23), Article 56 of the Regulation defines the 'lead' supervisory authority (known as the 'lead' control authority) for the processing activities of the controller in the Union on the basis of the principal establishment of the controller or of its unique establishment. The purpose is to have a single supervisory authority competent to monitor the activities of the controller or the processor carried out throughout the Union and to make the relevant decisions.

Article 57 defines the tasks assigned to the supervisory authorities. These responsibilites are of different types: the task of surveillance, investigation

and control, the tasks of providing information and advice, for mutual assistance, management of complaints, etc.

Article 58 defines quite precisely three types of powerswhich the Member States must, by law, grant to their national supervisory authority: investigative powers, power to take corrective action and powers of authorization and advice.

Finally, Article 59 sets out a duty for each supervisory authority to issue and publish an annual report of their activities.

11. Concerning the cooperation and consistency (Chapter VII). Article 60 of the Regulation impose upon the 'lead' supervisory authority the obligation to cooperate with the other supervisory authorities concerned with a view to reach a consensus in cases of potential debate on the designation of the competent supervisory authorities. A procedure - quite complex - is envisaged by this provision intended to achieve a balance that will be (too) subtle between the joint competencies of the different authorities.

Article 61, on its part, sets explicit and consistent rules on the mandatory mutual assistance between the national supervisory authorities and foresees the consequences in case of refusal to comply with the request by another supervisory authority.

Article 62 establishes the principle that the authorities may, when necessary, conduct joint operations of various nature, such as joint investigations or joint repressive measures, under conditions defined by them.

Since the tasks and the competencies of the supervisory authorities increase, and the margin of maneuvering given to the Member States in the implementation of the Regulation is still quite broad, the risk of divergent interpretations of the protection rules or of incompatible decisions inevitably increases. This is why Article 63 introduces the principle of control of consistency imposing to the supervisory authorities to cooperate with each other and, where appropriate, with the Commission through the mechanisms implemented by Article 64 to Article 67 in order to ensure the overall consistency of the application of the Regulations across the EU.

These mechanisms include:

- Requesting the opinion of the European Data Protection Board on some draft decisions of national authorities before adopting them (Art. 64);

- Requesting a binding decision of the European Board in case of disputes between national authorities (Art. 65);

- Allow an authority, in some cases, to adopt provisional measures under a urgency procedure (Art. 66 § 1) or even definitive measures after having requested the urgent opinion of the European Board (Art. 66 § 2).

Article 67 of Regulation also grants implementing powers to the Board to set the terms of the exchange of information electronically between the national and/or European supervisory authorities.

The European Data Protection Board intended to replace the former Group 29 will play a major role in this system of consistency control. Therefore, it is not surprising to see the Regulation to devote many provisions to the Board (Articles 68 to 76).

Article 68 provides for the establishment and composition of a European Data Protection Board, which will have legal personality and will be represented by its Chair, instead of the Group Article 29. Article 69 stipulates its independence.

The many assignments of the Board are set in the Article 70 of the Regulation: ensuring a monitoring mechanism to advise the Commission, issuing guidelines and recommendations, etc. Article 71 requires the Board to report annually on its activities and Article 72 sets out the terms of its decision-making (quorum, etc.). Article 73 prescribes the rules for the appointment and the status of the Chair of the Board. Article 74 defines specifically the tasks assigned to the Board.

Article 75 states that the Board secretariat is provided by the European Data Protection Supervisor and defines its tasks. In general, the secretariat should provide analytical, administrative and logistical support to the Board. Article 76 expressly states that discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

12. Regarding the remedies, liability and penalties (Chapter VIII). This is probably one of the chapters that will have the greatest implications for the future. It actually strengthens considerably the means of protection of the data subjects and the penalties applicable to the controllers and the processors.

Article 77 of the Regulation vests in any data subject the right to lodge a complaint with a supervising authority, if the data subject considers that the processing of personal data relating to him or her infringes the European rules.

The right to a judicial remedy against a decision by a supervisory authority is stipulated in Article 78 as an essential element of the protection of individuals with regard to the processing of personal data.

Article 79 gives the people affected by processing, a genuine right to an effective judicial remedy against the controller or the processor in case of infringement of their rights resulting from the processing of their data in violation of the Regulation. A specific procedural regulation (suspension or junction) is provided for in Article 81 in cases of referrals to courts in the different states.

Article 80 specifies and supplements the possibility for representation by an association already provided for by the Directive. The third paragraph allows the Member States to grant major powers of action to the associations charged with the protection of rights and freedoms in the data processing.

Article 82 of the Regulation confirms by specifying the principle of compensation for the material or immaterial damage suffered by any person as a result of an infringement of this Regulation (§ 1). The compensation may be received from the 'controller' or the 'processor'. In its second paragraph, the provision also specifies the generating facts and exclusions of liabilities for the controller and the processor. The article also provides for joint liability between the controllers but also between the controller and the processor involved in the processing.

Pursuant to Article 83 of the new Regulation, the supervisory authorities receive the competence to impose administrative fines for most violations of the Regulation. This provision provides many criteria to consider in determining the amount of the fine. The provision also specifies two types of ranges (up to EUR 10 million or 2% of total annual turnover / up to EUR 20 million or up to 4% of annual turnover) specific to certain violations covered by the provision.

As to the other penalties, Article 84 indicates that the Member States shall determine the regime and take all necessary steps to ensure their implementation.

13. Concerning the provisions relating to specific situations of data processing (Chapter IX). This chapter contains some specific regimes specific to particular categories of processing. In reality, most of the time, the Regulation leaves to the Member States in determine the content of the rules.

Article 85 of the Regulation provides that the Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information.

Article 86 on its part stipulates that the personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in order to reconcile public access to official documents with the right to the protection of personal data.

Like the Directive, Article 87 allows the Member States to set specific conditions for the processing of a national identification number or of any other identifier of general application. The Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application, provided that the rights and freedoms of the data subject pursuant to this Regulation are safeguarded.

Article 88 of the Regulation also leaves the states to decide on any adjustments of data protection in the employment relationship. More precise rules for the protection of rights and freedoms may in fact be provided by the Member States, either by law or through collective agreements.

Article 89 of the Regulation provides for specific exceptions to certain rules contained in the Regulation for scientific, statistical or historical purposes. It also extends the scope by adding the purpose of archiving in the public interest.

Article 90 authorizes the Member States to adopt special rules to protect professional secrecy or other equivalent secrecy obligations under the exercise of investigative powers of the supervisory authorities.

Article 91 allows churches and religious associations or communities to continue to apply the rules on data protection in force at the date of entry into force of Regulation, 25 May 2016, provided that these rules are brought into line with the provisions of the Regulation.

14. Concerning the delegated acts and the implementing acts (Chapter X). Article 92 defines the conditions for the exercise of Commission power to adopt delegated acts (to specify certain criteria or requirements, for example), in implementation of certain provisions of the Regulation.

Other provisions require the Commission to take enforcement action that must comply with the procedures set out in Article 93 of the Regulation.

15. Concerning the final provisions (Chapter XI). Article 94 abrogates the Directive from the moment when the Regulation becomes applicable, or 2 years after the 20th day following its publication in the Official Journal of the European Union and addresses the question of the acts under its cover once adopted.

Article 95 clarifies the link with Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Article 96 specifies that the international agreements involving the transfer of personal data to third countries or international organizations which were concluded by Member States prior to 24 May 2016, and which comply with Directive 95/46/EC, shall remain in force until amended, replaced or revoked.

Article 97 of the Regulation renews the task of evaluation and revision by the Commission to submit assessment reports to the Parliament and the Council at regular intervals (4 years). The Commission is also granted, by Article 98, the power to submit legislative amendments to any other legal instruments under the EU law on data protection.

Article 99 specifies that this Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. The Regulation was published on 4 May 2016 in the Official Journal of the European Union and will therefore enter into force on 25 May 2016.

However, the Regulation will only be applicable after the two years following its entry into force, i.e., from 25 May 2018.

The Regulation does not provide for a transitional regime, but, strangely, gives some transition principles in recital 171.

Brussels, May 2016

Thierry LEONARD and Didier CHAUMONT