Suggestions of MEDEF

Position of MEDEF

on the European Commission's proposal

for a General Data Protection Regulation

2012

INDEX

KEY ELEMENTS

A balanced, technologically neutral legal framework that limits competition distortions. It is essential to guarantee the right balance between the legitimate demands to protect individuals' personal data and the economic reality. In this respect, the neutrality of European legislation must be preserved as regards technology. It is necessary to make sure that the rules pertaining to data protection do not create any distortion of competition between companies based in the European Union (EU) and those based elsewhere.

A framework that ensures companies legal security and limits referrals to delegated acts and implementing acts to the non-essential elements of the regulation. Referrals to delegated acts and implementing acts are often misused. At times they pertain to essential elements of the legislative act, which should be specified in the body of the regulation. They are also excessively numerous (46). These referrals make it difficult to understand the provisions introduced in the draft regulation and to measure their concrete consequences, thereby creating serious legal uncertainty for companies. The method is all the more questionable in that this is a regulation, for immediate implementation in the Member States and which, therefore, should have precise provisions.

A general framework on data protection that should not be led astray by sector-based concerns. The introduction of sector-based measures (right to be forgotten, right to data portability, etc.) muddles the general framework's clarity on personal data protection. Initially envisaged for specific cases (social networks, etc.) and integrated into a general framework, they will entail consequences not yet measured or even measurable for all sectors.

A framework that preserves the foundations of lawful processing and flexibility in obtaining data subject's consent. It is crucial to preserve the various rationales legitimizing personal data processing and, in particular, the controller's pursuit of legitimate interests. In the event that the processing depends on obtaining the data subject's consent, some flexibility shall be preserved in terms of collection methods, notably in order to adapt to different situations and to the expectations of the data subjects concerned and to preserve the principle of technological neutrality.

A framework instituting proportionate sanctions. Allowing for administrative sanctions that can amount to 2% of a company's annual worldwide turnover is disproportionate and unjustified; at the very least, the new framework should institute a maximum ceiling (in absolute value). Moreover, the possibility for the supervisory authority to give a warning (or an injunction to comply) should not be restricted to certain cases; the warning should be a prerequisite to taking any sanction against a company.

SUMMARY

On the references to delegated acts and implementing acts. MEDEF considers that referrals to delegated acts or implementing acts should be limited (i) by abolishing unnecessary referrals and (ii) by specifying the essential provisions in the body of the regulation.

On the territorial scope. MEDEF takes a positive view of the intention to subject companies based outside the EU to the European rules governing personal data protection.

On the lawfulness of processing. MEDEF notes with satisfaction that several conditions to legitimize processing of personal data and particularly the condition pertaining to the controller's pursuit of legitimate interests are upheld. However, there appears to be a need to provide a rationale and clarification on the provisions stipulating the impossibility of founding the processing on the controller's pursuit of legitimate interests when the purpose of the subsequent processing is incompatible with that for which the personal data was collected. Furthermore, MEDEF requests the abolition of the referral to a delegated act to specify the conditions for founding the processing on the controller's pursuit of legitimate interests.

On consent. MEDEF attaches great importance to the need to preserve some flexibility in the procedures in order to obtain data subject's consent and, to that end, it would like to preserve in the draft regulation the definition of consent provided for in Directive 95/46/EC (Article 2-h). Furthermore, MEDEF questions the meaning and the objective targeted by Article 7-2 of the draft regulation, which stipulates that "*If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter*".

On the transparency of information and communications. MEDEF agrees that companies should inform the data subject in an intelligible way using clear and simple terms. However, MEDEF questions the feasibility and the proportionality of providing information and communication in terms "*adapted to the data subject*".

On the controller's deadline to respond to the data subject's request. MEDEF recommends that companies should have two months to reply to data subjects who exercise their rights.

On the information to the data subject. MEDEF asks to replace the information about retention periods by information given by companies limited to the criteria used to determine the period for which the data are stored, for each type of purpose, as part of the exercise of the right of access. Moreover, MEDEF supports the abolition of companies' duty to provide information on judicial remedies and complaints to the supervisory authority as well as on the degree of protection offered by the third country in case of data transfer.

On the right of access. MEDEF questions the opportunity to require the controller to answer the data subject in electronic format when the latter exercises his or her access right in that format.

On the right to be forgotten and to erasure. MEDEF considers that it is preferable to reinforce the effectiveness of existing rights rather than to create a right with unclear boundaries. Moreover, the right to be forgotten may entail major and unjustified consequences for all sectors even though its introduction is only justified for certain services (social networks, etc.).

On the right to data portability. MEDEF believes that it is inappropriate to create a right to data portability in a regulation of general scope without measuring the concrete consequences of its introduction. Furthermore, MEDEF requests the abolition of the referral to an implementing act to determine which technical standards and which electronic format can be used for data transmission.

On privacy by design and by default. While the introduction of such requirements into a regulation may be questioned, companies will have to determine the means to implement them in any event, according to a certain number of criteria, particularly the nature of the products and services proposed. Consequently, the MEDEF requests the deletion of the referral to an implementing act to define a technical standard on this matter.

On the documentation. MEDEF affirms the need to limit the information companies have to keep in respect of their documentation duty and to define, in the case of the exception provided for in Article 28-4-b of the draft regulation, what is meant by "*ancillary*".

On the notification of personal data breach. The concrete consequences of introducing a duty to notify data breach in the electronic communications sector need to be assessed before proceeding with its generalization. At the very least, there would be a need to gradually adjust the notification duty depending on the type of data concerned by the breach and its degree of seriousness, and to align the notification deadline with that provided for in the Directive 2002/58/EC as amended ("*without undue delay*").

On the data protection impact assessment. MEDEF requests clarification of the provisions pertaining to data protection impact assessment, modification and clarification of the list of processing operations presenting specific risks referred to the rights and freedoms of data subjects, as well as the abolition of the controller's duty to seek the views of data subjects during a data protection impact assessment, prior to any processing.

On the prior authorization and consultation. The prior authorization and consultation mechanisms require clarification and simplification. Furthermore, MEDEF is not in favour of national supervisory authorities having the option to establish their own list of processing operations and wishes the stipulation in the draft regulation of a two-month deadline for authorities to respond to companies' requests.

On the codes of conduct. MEDEF takes a positive view of the fact that establishing codes of conduct is encouraged. These codes should effectively illustrate current normative measures and guarantee some flexibility by making it easier to adapt legal rules to technological developments.

On the liability of the controller and the processor. MEDEF requests clarification of the controller's and the processor's respective liability regimes.

On international transfers. MEDEF supports the insertion into the draft regulation of the current systems allowing for data to be transferred abroad under conditions that guarantee a high level of protection (binding corporate rules, standard data protection clauses, etc.). However, it is concerned about the European Commission having the option to establish a "blacklist" of countries that do not provide an adequate level of protection.

On the competence of the supervisory authorities. MEDEF underlines the importance of creating a "one-stop shop" system to simplify relationships between companies and authorities. MEDEF suggests that when a company operates in several Member States and that one authority is competent, the ex-ante control is carried out by the competent authority of the main establishment, and that the ex-post control is carried out by the authority where the company's headquarters are located.

On the European Data Protection Board. MEDEF requests that companies be represented in the European Data Protection Board.

On remedies. MEDEF reiterates its objection to the introduction of legal measures for collective remedies.

On administrative sanctions. MEDEF considers that the draft regulation provides for maximum sanctions that are disproportionate and excessive. At the very least, MEDEF suggests applying a maximum ceiling in absolute value to the sanctions that a national supervisory authority can pronounce. A warning (or an injunction to comply) shall be a prerequisite for the authority deciding upon a sanction.

INTRODUCTION

Directive 95/46/EC of 24 October 1995 has governed the protection of personal data in Europe for nearly seventeen years. In view of the numerous challenges to the protection of personal data arising from technological developments and the globalisation of exchanges, the European Commission has decided to revise the general framework of data protection in Europe, **while acknowledging that the guiding principles and objectives of Directive 95/46/EC** were satisfactory.

The European Commission stated that the harmonisation of legislation on personal data protection among Members States would also enable businesses to save as much as 2.3 billion euros each year[1]. Nonetheless, MEDEF questions the outcome of this assessment in view of the impreciseness in the draft regulation (references to forty-six delegated acts and implementing acts) and of the new burdens that this legislative act could impose on businesses (impact assessment, notification of data breaches, etc.). **It is to be feared that the cost of implementing the regulation will prove greater for businesses than the savings announced.**

On 25 January 2012, the European Commission adopted its proposals to reform the data protection rules. This reform includes a **proposed regulation defining a general framework on data protection for the European Union** and a proposed directive on the protection of personal data processed for the purposes of prevention and detection of criminal offences, investigations or prosecutions, as well as related judicial activities[2].

MEDEF recalls that data protection is a fundamental issue for both the individuals whose data are processed (data subjects) and business. It involves the trust of data subjects and rests on a logic of responsibility. **Applicable European rules on the processing of personal data must ensure an adequate level of protection while guaranteeing the free movement of data within the European Union and the competitiveness of businesses in the context of strong international competition.**

The dovetailing of data protection regulations with other existing regulations (insurance law, banking law, etc.) must be achieved consistently, since the right to data protection interacts with other fields.

All stakeholders must devote some thought to ways of improving the provisions currently in force, with the aim of making the rules effective. It is crucial to provide information and raise awareness among actors and data subjects of **the need to adapt practices so as to deal with the issues involved.**

MEDEF insists on the need to maintain a general framework that is technologically neutral and which, in particular, must not inhibit technological innovation. Data protection rules must not restrict trades between enterprises and hinder their competitiveness. The reform shall not introduce distortion of competition between businesses established in the European Union and those established outside it.

[1] **See the European Commission's press release of 25 January 2012: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=1&language=EN&guiLanguage=en**

[2] **These observations do not relate to this latest proposal for a directive, as it concerns the areas of judicial co-operation in criminal matters and police co-operation.**

1. REFERENCES TO DELEGATED ACTS AND IMPLEMENTING ACTS

Forty six provisions refer to delegated or implementing acts by the European Commission. On the one hand, MEDEF believes that there are too many such references and, on the other hand, questions the possibility of relying on a delegated act for some essential provisions of the draft regulation (right to be forgotten, right to data portability, right of access, impact assessment, etc.) insofar as the Treaty on the Functioning of the European Union (TFEU) expressly provides that delegation cannot be used when it comes to the essential elements of a legislative act[3].

These numerous references:

- **make it difficult to understand the provisions** of the regulation which are limited to providing principles, thus precluding assessment of the practical repercussions on the economic activity of businesses,
- **create legal uncertainty** and
- **weaken the principle of technological neutrality** (which the directive of 1995 provides, and which must be maintained in the proposed regulation).

While this legislative power provided by the TFEU may appear justified for some provisions, it proves unacceptable, irrelevant and a source of uncertainty for many other provisions.

For example, the following legislative references are disputable:

- A delegated act to specify the conditions under which a business can ground data processing in the existence of legitimate interests for various sectors and data processing situations (Article 6.5 of the draft regulation).
- Implementing acts to determine the technical standards and electronic formats for data portability or even privacy by design and by default. In addition to being irrelevant, these implementing acts could have harmful repercussions, e.g. by impoverishing technological innovation, while failing to guarantee the protection of privacy (Articles 18.3 and 23.4 of the draft regulation).

MEDEF strongly criticises the method used, which consists of quasi-systematic reference to delegated and implementing acts; it is recalled herein that a regulation, with immediate effect in Member States, must contain specific provisions. **Accordingly, MEDEF seeks (i) the removal of unnecessary references and (ii) that the relevant provisions be specified within the body of the regulation itself.**

2. APPLICABLE LAW

MEDEF emphasises the need to keep to a minimum the distortion of competition between businesses. It is essential to examine the law applicable to businesses that are established outside the EU and that process the personal data of European citizens, although without applying the relevant existing European rules. This issue is indeed likely to affect the competitiveness of French and European businesses in comparison to businesses established in third countries (principle of reciprocity).

The draft regulation provides that, in some cases, businesses established outside the EU will be subject to the European regulation on data protection (Article 3 of the draft regulation). **Although MEDEF welcomes this approach, it nonetheless questions the effectiveness of such a measure:** how could these rules be imposed on such third-country businesses, and how could sanctions be applied to them?

Besides this, **MEDEF supports the development of international standards on the protection of privacy through international agreements.**

[3] **Article 290(1) of the Treaty on the Functioning of the European Union provides that "*A legislative act may delegate to the Commission the power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of the legislative act*".**

3. LAWFULNESS OF PROCESSING

Article 6(1) of the draft regulation maintains the possibility for the controller to base the lawfulness of his or her processing on various cases[4].

MEDEF welcomes the measure and recalls its attachment to maintaining the existence of several conditions legitimising the processing of personal data. More specifically, **MEDEF insists on the importance of maintaining the rule allowing controllers to process data provided (i) they do so in pursuit of legitimate interests** and (ii) the processing does not affect the fundamental freedoms and rights of the data subject. The latter must be able to exercise his right to object, if he so wishes. This ground allows satisfactory processing in terms of protection of individuals.

For example, in the **direct marketing** sector, canvassing by post is based on the pursuit of legitimate interests. The data subject is informed, when his or her data are collected, of his or her rights and the scope for his exercising his right to object. Moreover, professionals in the sector have set up mail preference service opt-out lists which allow individuals to object to receiving unsolicited commercial mailings[5]. **If the pursuit of legitimate interests can no longer justify processing, postal canvassing could no longer be viable for actors in the sector concerned, since securing prior consent would raise an insurmountable obstacle.**

Under Article 6(4) of the draft regulation, where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis in one of the grounds for lawfulness provided in Article 6(1) of the draft regulation. However, paragraph (f) in Article 6(1) – concerning the legitimate interests pursued by the controller – is excluded from this provision. Article 6(4) specifically states that this provision shall in particular apply to any change in the terms and general conditions of a contract. **MEDEF seeks clarification of this provision and of the justifications provided for excluding point (f) (legitimate interests of the controller).**

According to Article 6(5) of the draft regulation, a delegated act may be adopted by the European Commission for the purpose of further specifying the conditions provided in point (f) of paragraph 1 (which concerns the legitimate interests pursued by the controller) in various sectors and data processing situations, including the processing of personal data relating to a child. MEDEF considers it irrelevant to refer to a delegated act in this case as the case law handed down on this issue currently provides sufficient protection. **MEDEF thus seeks removal of the reference to a delegated act in this matter.**

4. CONSENT

The draft regulation modifies the definition of consent. Article 4(8) of that draft defines consent as "*any freely given specific, informed and **explicit** indication of his or her wishes by which the data subject, **either by a statement or by a clear affirmative action**, signifies agreement to personal data relating to them being processed*".

MEDEF restates the importance of maintaining flexible regulation of the terms and procedures for securing consent and promoting the creation of innovative methods. Imposing methods to be used by the controller for obtaining the data subject's consent of the data subject appears unjustified and counterproductive. The methods of obtaining consent should not be fixed provided consent is granted under conditions that respect the rights of individuals; to do otherwise would be unduly and heavily burdensome to businesses.

[4] These are the cases: where data-subject consent has been given, necessity for the performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task carried out in the public interest or in the exercise of official authority, necessity for the pursuit of legitimate interests by a controller.

[5] Robinson lists exist in many states. In France, the Robinson list is managed by the Union française du marketing direct (UFMD).

For these reasons, MEDEF is seeking the maintaining and use in the draft regulation of the definition of consent provided in 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.

Article 7(2) of the draft regulation provides that "*If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter*". **MEDEF questions the intention and objective pursued by this provision. Consequently, it seeks clarification of this article.**

5. TRANSPARENT INFORMATION AND COMMUNICATION

While MEDEF welcomes the fact that the business shall inform the data subject in an intelligible form, using clear and plain language, **it questions the feasibility of ensuring information and communication in terms "*adapted to the data subject*"** (Article 11(2) of the draft regulation). **It may be questioned what criteria must be taken into consideration by the controller to adapt its information, with the risk of subjectivity this entails. This provision will also have cost implications for businesses**, since they may be required to set up numerous and differentiated information resources to cater for different data subjects. **The proportionality of such a measure is open to question.**

6. CONTROLLER'S TIME OF RESPONSE TO THE DATA SUBJECT

Article 12(2) of the draft regulation provides that businesses must respond to the data subject who has exercised his or her rights within one month of receipt of the request. **MEDEF suggests maintaining the two-month period currently provided by the French regulation[6] which appears reasonable both for businesses and data subjects.**

7. INFORMATION TO THE DATA SUBJECT

7.1. Information on the length of storage

Under the terms of Article 14(1)(c) of the draft regulation, controllers must provide data subjects with information in advance on "*the period for which the personal data will be stored*".

MEDEF restates the necessity of taking into consideration the principles of reality and proportionality. Personal data about an individual are often kept by a business for several different reasons[7] or such data fall under a legal or contractual obligation, which requires a different storage period. **It is thus very difficult for businesses to indicate a data storage period in advance, which varies according to the intended objective and the nature of the relationship that will exist between them and the data subject.** Article 14(1)(c) of the draft regulation would involve data controllers having to customise the information, which could prove scarcely practicable. This would considerably lengthen information clauses at the risk of making them difficult to read and unintelligible. It may be questioned whether there is any real benefit for data subjects.

Hence, MEDEF seeks that only criteria that allow the data storage period to be determined for each type of purpose should be communicated to data subjects, for purposes of exercising the right of access.

[6] Article 94 of Decree No. 2007-451 of 25 March 2007, amending Decree No. 2005-1309 of 20 October 2005 passed for the application of the Data Protection Act of 6 January 1978, amended by Act No. 2004-801 of 6 August 2004, provides that "*the data controller shall respond to the request submitted by the relevant party within two months following its receipt*".

[7] For example, an insurance company may keep information about one of its policyholders, for the policyholder's car insurance as well as for his or her home insurance.

7.2. Information on legal action and complaints to the supervisory authority

Articles 12(3), 14(1)(e) and 15(1)(f) of the draft regulation introduce an obligation on controllers to inform data subjects of the right to institute judicial proceedings or bring a complaint to the supervisory authority. **MEDEF does not regard this information as falling within the responsibility of businesses. Consequently, MEDEF seeks the removal of the abovementioned provisions.**

7.3. Information on the level of protection offered by third countries in the case of a transfer of data

No grounds justify, in the case of transfer to a third country or international organisation, the controller having to inform the data subject of the level of protection offered by the third country or international organisation, by reference to a protection-level adequacy decision by the Commission. **MEDEF therefore seeks removal of this information requirement.**

8. RIGHT OF ACCESS

When the data subject exercises his or her right of access in electronic form, the draft regulation provides for the information listed in Article 15 to be transmitted to the data subject in electronic form (Article 15(2) of the draft regulation). MEDEF restates the need to maintain a certain technological neutrality in order not to introduce distortion of competition via methods of distribution or communication. **MEDEF thus questions the advisability of requiring controllers to respond to a data subjects in electronic form when he or she has exercised right of access in this form.**

Furthermore, **MEDEF is at pains to recall the difficulties encountered by businesses in identifying the data subject who is exercising his or her right of access.** What assurance can be secured that the person making the request actually is indeed the data subject?

9. RIGHT TO BE FORGOTTEN AND TO ERASURE

Article 17 of the draft regulation provides "*a right to be forgotten and to erasure*".

Data subjects will be entitled to obtain the erasure of personal data relating to them and the abstention from further dissemination of such data for particular reasons (Article 17(1) of the draft regulation). Article 17(2) of the draft regulation imposes a requirement on the controller to take all reasonable steps, in relation to data for whose publication it is responsible, in view of informing third parties that process these data that a data subject requests them to erase any links to, or copy or replication of it.

This right already exists in the directive of 1995 through the possibility afforded to any individual to request the removal of inaccurate, incomplete, equivocal or expired data concerning them and the removal by the controller of data that are no longer necessary for the purposes for which the data were originally collected. These provisions are maintained in the draft regulation. Consequently, **the introduction of a "right to be forgotten" in the draft regulation is unnecessary and could create redundancy with these provisions** (rights of access, to information, to object and to rectification). In addition, modifications made by the draft regulation to the right to object (Article 19 of the draft regulation) are intended to reinforce the rights of persons and thus already include the concept of the "right to be forgotten". **MEDEF recalls furthermore that the right to be forgotten also exists in other enactments (right to privacy, judicial limitation rules, etc.).**

The obligation provided in Article 17(2) of the draft regulation, essentially drafted to deal with issues entailed in the functioning of social networks, is completely at variance with the digital environment. **The controller has no control over data published by individuals and used by third parties. Moreover, this obligation will prove virtually impossible to enforce technically.**

MEDEF also notes that no distinction is made between information made public (accessible to an undetermined number of people) and that made accessible to specific third parties.

Also an issue for MEDEF is the nature of the authorisation and in particular its format (whether explicit, implicit, written, etc.), mentioned in Article 17(2): "*Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for the publication*". Can the fact that information has been made public and thus accessible to third parties on its website be interpreted as authorisation for its reuse by third parties? Finally, there is confusion between information published by the user himself, thus on his own liability, and data made public by the controller. **MEDEF is furthermore concerned about the possible liability implications for website hosting service provider if this wording is maintained.**

The insertion in a general framework of such a provision, which, from a reading of the text is only justified for particular services (social networks, for example), is worrying in that it will have serious and unwarrantable consequences for all sectors. Moreover, we note that the French version of the draft regulation mentions a "*right to be forgotten online and erasure*"[8] whereas the English version provides a right to be forgotten and erasure without specifying "online". This adds confusion to the scope of this provision.

MEDEF believes that it is preferable to strengthen the effectiveness of existing rights rather than creating a right of uncertain scope and meaning, which is likely to have serious and unwarrantable consequences for all sectors.

10. RIGHT TO DATA PORTABILITY

Article 18 of the draft regulation provides that "*The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used*".

MEDEF questions the universal approach applied to the right to data portability and the proportionality of such a measure.

The right to data portability is similar to that which exists in the electronic communications sector for telephone numbers. With a considerable difference through: this new right would require controllers to restore the data of individuals to a "*structured and commonly used format*" so that the person can transmit these data to another system.

MEDEF notes that this provision will have a considerable impact on businesses in a situation of competition. The replication of data will raise the issue of transmission security, besides, the introduction of such a measure will lead to considerable expense for businesses even though, to date, no impact assessment has been carried out.

Experiments are currently being carried out in some countries on the retrieval of personal data for individuals[9]. **The results of these experiments could undoubtedly give an insight into the implications for businesses of setting up such a service before deciding to create, at a European level, a data portability obligation borne by businesses.**

Furthermore, MEDEF questions whether this provision is actually of any data-protection value to data subjects (individuals will receive a substantial amount of data without necessarily knowing what to do with them).

Consequently, MEDEF believes that it is inappropriate to introduce such a right in a general framework.

[8] The French text addresses a "droit à l'oubli numérique et à l'effacement".

[9] For example, the government-run programme in the United Kingdom called "*MiData*", launched on 22 October 2011.

Article 18(3) of the draft regulation provides a reference to an implementing act to determine which technical standards and electronic format may be used for the transmission of data. **MEDEF seeks the removal of this reference: an implementing act in this case would prove inadvisable (since it would take no account of innovation and technological developments).**

11. DATA PROTECTION BY DESIGN AND BY DEFAULT

MEDEF is in favour of businesses taking into consideration data protection by design (privacy by design) and by default (privacy by default).

Article 23(4) of the draft regulation provides a reference to an implementing act concerning the definition of technical standards. **MEDEF does not believe that this reference is justified and the definition of a technical standard would hinder technological innovation, without providing any assurance that privacy would be protected.**

While the introduction of such obligations in a regulation is open to question, **MEDEF believes that the terms and procedures for their implementation must in any case be determined by businesses**, based on a number of criteria and particularly the nature of the products and services offered.

12. DOCUMENTATION

The controller must keep a documentary record of a number of information items. The information concerned is listed in Article 28(2) of the draft regulation. It should be emphasised that this measure entails a sizeable burden for businesses, in terms of both organisation and cost. **MEDEF believes that it is necessary to limit the storage requirement to this information and, consequently, proposes removing the words "*at least*".**

Moreover, the obligation to keep documentation does not apply to businesses employing less than two hundred and fifty employees that process personal data only as an ancillary activity to their main activities (Article 28(4)(b) of the draft regulation). **A definition should be inserted of what is meant by "*ancillary*".**

13. NOTIFICATION OF DATA BREACH

MEDEF recalls that the revision of the "Telecoms Package" in 2009 led to the introduction of an obligation for providers of electronic communications services accessible to the public to provide notification of personal data breaches. **The actual consequences should be assessed, particularly in terms of effectiveness, of the application of this obligation to the electronic communications sector before it is generalised.**

Regardless of whether this concerns electronic communication or covers the generalising of this obligation to all sectors, MEDEF voices concern as to the implications of such notification to data subjects. **A blanket notification of all personal data breaches to data subjects appears unwarranted and dangerous** (creation of a climate of uncertainty, incomprehension and confusion for individuals receiving notifications, overburdening of the data-protection authorities, etc.). **Moreover, the introduction of these obligations will undoubtedly introduce cost and organisation constraints on businesses, particularly SMEs.**

If this general notification of all data breaches to data subjects were nonetheless maintained in the draft regulation, **MEDEF believes that it would be necessary to graduate the notification obligation of businesses according to the type of data concerning which the breach was committed** (for example, the obligation to notify the breach must not be imposed on businesses where the data concerned are encrypted or made anonymous) **and according to the degree of seriousness of the breach** (for example, providing a notification obligation only in the case of a clear risk of serious damage to the data subject).

The notification period should also be reviewed and aligned with the regime provided in Directive 2002/58/EC, as amended by Directive 2009/136/EC. Article 4 of Directive 2002/58/EC provides that "*in the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority*". **MEDEF proposes applying as it stands the wording of Article 4 of Directive 2002/58/EC as amended, concerning the notification period, to Article 31(1) of the draft regulation.**

14. DATA PROTECTION IMPACT ASSESSMENT

Under the terms of Article 33(1) of the draft regulation, the controller or processor working on the controller's behalf must carry out an assessment of the impact of the processing operations where they present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes ("specific risks").

Article 33(2) of the draft regulation mentions a general list of these processing operations that present specific risks. Due to its general nature, this list does not differentiate according to the nature, scope or even the purpose of the processing operations implemented. Thus, for example, all video surveillance devices (Article 33(2)(c) of the draft regulation) must be subject to an impact assessment. If, however, such a device is used for the purpose of ensuring personal safety and does not present specific risks in view of its nature, scope or even its purpose, one may question why it must be subject to an impact assessment. If this general list is maintained, processing operations will require an impact assessment even though their nature, scope or even purpose does not require it.

Consequently, MEDEF seeks modification and clarification of the list of processing operations presenting specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes.

MEDEF notes that the list of processing operations in Article 33(2) of the draft regulation is not exhaustive and the standards and procedures for scalability, verification and auditability of the impact assessment will be defined by implementing acts (Article 33(8) of the draft regulation). The non-exhaustive nature of the list of processing operations presenting a specific risk and the reference to an implementing act involve a real legal uncertainty for businesses, which would not be able to fulfil their obligation to carry out an impact assessment (it is recalled that the failure to comply with this obligation could be sanctioned by a fine that can reach 2% of the annual worldwide turnover of the business). The cost generated by impact assessments will itself be difficult for businesses to quantify. **MEDEF seeks clarification and greater precision of the provisions on impact assessments.**

Furthermore, Article 33(4) of the draft regulation provides that the controller shall seek the views of data subjects on the intended processing. **This obligation for the controller to consult the data subject during the impact assessment, before any processing, seems impractical.** MEDEF wonders what weight is to be given to this consultation by the controller.

It should be noted nonetheless that when processing is carried out in performance of a legal obligation providing rules and procedures regulated at European Union level and concerning data processing, the impact assessment is unnecessary (unless the Member State deems otherwise).

15. PRIOR AUTHORISATION AND PRIOR CONSULTATION

MEDEF notes ambiguity concerning the mechanism for prior authorisation and prior consultation (Article 34 of the draft regulation). These two mechanisms result in the same consequences for the controller: it cannot carry out the processing until the authorisation or opinion has been issued by the supervisory authority. It can be inferred from Recital 74 of the draft regulation that prior consultations are ultimately intended to establish recommendations concerning the introduction of data processing. Article 34(3) of the draft regulation introduces

vagueness by mentioning the possibility of the supervisory authority prohibiting the processing or making appropriate proposals where it is of the opinion that the intended processing does not comply with the regulation. **These provisions appear unreasonably complex for such similar systems**, whose respective scopes are uncertain and likely to bring about differing interpretations between Member States.

Article 34(2)(b) of the draft regulation provides that the controller or processor acting on behalf of the controller should consult the supervisory authority prior to processing operations, where an impact assessment (Article 33 of the draft regulation) indicates that this processing is, by virtue of its nature, scope or purpose, likely to present a high degree of specific risk. A delegated act may specify the criteria and requirements applicable in determining what is a high level of specific risk. To what criteria will the controller refer in determining whether the processing presents a high degree of specific risks? Will the controller identify processing operations that present a high degree of specific risks, on its own liability?

According to Article 34(4) of the draft regulation, the national supervisory authorities draw up a list of the processing operations which are subject to prior consultation (and hence, require an impact assessment). **The possibility granted to the national authorities to draw up their own list of processing operations could create considerable legal uncertainty for businesses and could lead to distortions between different Member States.**

MEDEF recommends clarification and simplification of the mechanisms for prior authorisation and prior consultation.

The draft regulation provides no time limit for response to authorisation and consultation requests made by controllers to the relevant supervisory authority. **MEDEF recommends setting a two-month response time for the supervisory authority, so as to allow businesses to set up, adapt, etc. their processing of personal data.**

16. DATA PROTECTION OFFICER

The draft regulation provides for the appointment of a data protection officer where processing is carried out by a business employing two hundred and fifty persons or more or when the core activities of the controller or processor consist of processing operations which, by virtue of their nature, scope and/or purpose, require regular and systematic monitoring of data subjects. The rules governing the data protection officer are also modified, and his functions have evolved.

MEDEF's position on these issues is currently being developed.

17. CODES OF CONDUCT

MEDEF welcomes the encouragement to the drafting of codes of conduct. These codes must illustrate existing legal provisions and they must ensure a measure of flexibility by facilitating the adaptation of legal rules to technological developments. **Certain provisions in the draft regulation,** particularly questions on data portability and privacy by design and by default **could thus be covered by the adoption of codes of conduct or recommendations.**

For the extension of the application by the European Commission of codes of conduct adopted by certain associations or other bodies, there must be a prior procedure for consulting stakeholders.

18. RESPONSIBILITY OF THE CONTROLLER AND THE PROCESSOR

Under the terms of Article 26(4) of the draft regulation, "*if a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers*".

MEDEF recalls that the processor is contractually bound to the controller. According to the current regulations, if the processor fails to comply with the instructions given by the controller, its responsibility shall be contractual. In this case, the processor assumes the capacity of controller since it applies new purposes to the processing of the data transmitted.

In the draft regulation, several obligations are imposed indiscriminately on the controller or the processor. This creates legal uncertainty: the lack of definition of the respective roles of the controller and the processor contributes to diluting (and not reinforcing) their responsibility.

It is therefore necessary to clarify in the draft regulation the respective responsibilities and obligations of the controller and the processor.

19. INTERNATIONAL TRANSFERS

MEDEF welcomes the insertion in the draft regulation of current systems (binding corporate rules [BCR], contractual clauses, etc.) which allow the transfer of data abroad under conditions that ensure a high level of personal data protection. **It is indeed important to ensure the movement of data within the European Union and internationally while guaranteeing a high level of protection.**

MEDEF recalls that the BCR system has benefited from the setup of the mutual recognition procedure[10] set forth by the "Article 29" Data Protection Working Party (G29), under the terms of which the approval of BCR may be centralised by a supervisory authority designated as an "entry point". To become a dynamic tool as well as to ensure the protection of data during international transfers, the BCR system must be simplified in particular to avoid extended verification and approval periods. MEDEF stresses that the effort to standardise approval procedures and consistency mechanisms surrounding the implementation of BCR must be carried out, particularly in terms of time period and accessibility, for businesses of all sizes.

Recognition of processor BCR (Article 43(3) of the draft regulation) may contribute to facilitating the management of transfers of data and would benefit from being further explained in the draft regulation.

Furthermore, **MEDEF is concerned by the possibility offered to the European Commission to set up a "blacklist" of countries that do not ensure an adequate level of protection** (Article 41 of the draft regulation).

20. COMPETENCE OF SUPERVISORY AUTHORITIES

The draft regulation provides a "one-stop shop" system for businesses carrying out their activities within several Member States of the European Union. The businesses may thus contact a single supervisory authority. This "one-stop shop" system should eliminate the need for businesses present in several Member States of the European Union to deal with several supervisory authorities. **MEDEF stresses the importance of this measure which aims to simplify relations between businesses and supervisory authorities.**

Nonetheless, MEDEF raises a number of points which need to be clarified.

While it is understood that under the terms of Articles 51 and 4(13) of the draft regulation, the one-stop shop system is intended in the case of a processing operation decided by a parent company and implemented by all its subsidiaries, it may be questioned whether this one-stop shop will also apply when this processing operated nationally is subject to adaptations to cater for specific features of national laws in other fields (labour, insurance, banking, etc.): depending on the

[10] This procedure allows the approval of BCR by the national data protection authorities through the designation of a co-ordination authority. See the Working Document Setting Forth a Co-operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting from "Binding Corporate Rules" adopted by the 29 Group on 14 April 2005:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp107_en.pdf.

specificities and national requirements, the processing operated nationally may differ between subsidiaries as regards the data processed, security measures, etc. In this case, would only one authority remain competent?

Furthermore, Article 51 of the draft regulation gives competence to the supervisory authority for supervising the processing activities of the controller or processor in all Member States. MEDEF questions the scope of the supervision that can be carried out by the single competent authority. Is that supervision ex ante (issue of authorisation) and/or ex post (supervision of compliance with the regulation)?

MEDEF believes that, if a business carries out its activities in several Member States and that only one authority is competent, a distinction should be made depending on whether the supervision carried out by the authority is ex ante or ex post. **Ex ante supervision should be carried out by the single competent authority according to the criteria of the main establishment and ex post supervision should be carried out by the supervisory authority at the place where the headquarters of the business is located.** In other words, while it appears clear to us that the authority in the place where the controller's main place of business is located can issue an authorisation for the implementation of a processing operation for the whole group, it does not appear either realistic or desirable for this authority to supervise this implementation.

21. EUROPEAN DATA PROTECTION BOARD

MEDEF is calling for representation of businesses on the European Data Protection Board.

22. REMEDIES

The European Commission intends to allow national data protection authorities and some citizen or consumer representative bodies or associations to initiate judicial proceedings, where applicable through a collective claim. **MEDEF has repeatedly[11] expressed its opposition to the introduction of collective legal redress measures.** It believes that this is a poor response to a valid question, as collective claims are judicial proceedings, i.e. they are necessarily long, complex and costly. Preference must be given to alternative dispute resolution mechanisms, which have the advantage of being simple, quick and effective[12]. **MEDEF accordingly seeks removal of this provision.** In addition, the Commission should soon make public a communication on collective claims clarifying its position and the initiatives it intends to take, generally, in this field. It is therefore particularly inappropriate for the issue to be tabled in the context of a specific regulation.

23. ADMINISTRATIVE SANCTIONS

While turnover provides the reference for sanctions in, for example, competition law, **its relevance to personal data may be questioned, especially since the percentages laid down in the draft are clearly disproportionate (from 0.5 to 2% of the annual worldwide turnover of a business). As a minimum, MEDEF proposes capping at an absolute value the amount of to the sanctions that may be imposed by national supervisory authorities.**

Article 79(3) of the draft regulation specifies cases in which the supervisory authority may send businesses a written warning without imposing any sanction. These cases are very limited. **MEDEF seeks the issuing of a warning (or an order to comply) prior to a sanction being imposed by the supervisory authority and, consequently, MEDEF seeks express inclusion of this possibility in Article 79(2) of the draft regulation.**

---

[11] See in particular MEDEF's response to the green paper on consumer collective redress of 26 February 2012:
http://ec.europa.eu/consumers/redress_cons/responses/MEDEF_fr.pdf

[12] See MEDEF's position on alternative dispute resolution, dated March 2012:
http://www.conso-confiance.fr/Position-du-MEDEF-sur-les-propositions-de-directive-et-de-reglement-de-la-Commission-europeenne-relatives-au-reglement_a81.html