FONDATION ROBERT SCHUMAN

POLICY PAPER

**European issues**
n°250
3rd September 2012

# What kind of European Protection for Personal Data?

**Isabelle Falque-Pierrotin**
*State Counsellor and chair of the CNIL*

**Abstract :**
*On 25th January 2012 the European Commission published a draft Regulation on the protection of personal data which recasts the entire European legal framework resulting from the 1995 Directive. Although this proposal includes a number of improvements, notably in terms of strengthening citizens' rights and compliance of businesses, the proposed regulatory mechanism, which is based on the criterion of "the main establishment", is not adapted to the digital world. Therefore the introduction of a different type of governance is suggested in this paper, making the most out of the Latin and Anglo-Saxon legal approaches, and thereby turning the protection of personal data into an asset for businesses, a new area for citizens' rights and an opportunity to enhance European integration.*

The protection of personal data has been the focus of a major European debate. Indeed, on 25th January 2012, the European Commission introduced a draft Regulation on the protection of individuals in this area as well as a draft Directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities. Both texts aim at modernizing the present legal framework introduced by Directive 1995/46/EC in 1995, notably given the development of the Internet and digital technology since the early 2000's.

All of this may seem slightly theoretical and part of the Community's extraordinary capacity to produce standards and norms that are often misunderstood by the citizens themselves. But here, we are talking about an issue that affects all of us: from our capabilities at work, at home, when we shop, our health to seeing our private life effectively guaranteed in a world that has dramatically changed over the last ten years.

Indeed, in just a few years the digital world has established itself. It is not just about the Internet. It also involves the progressive dematerialisation of all human activities which now extend from the physical to the virtual world; people pass from one to the other sometimes without even noticing and data is at the heart of this "seamless" universe.

The stakes are high for Europe: a pioneer in the area in the 90's, it now has to show that it can adapt to new digital realities – from the Internet to social networks, including video surveillance or big data – whilst maintaining a high level of protection for individuals. Europe has to show that it is able to innovate and build a credible and legitimate governance of personal data regarding an issue that has given rise to a growing mobilisation of the public.

For that is indeed the question at the very core of the matter: what balance is there between individuals' expectations, public policy goals, in particular regarding security and those of the businesses which want to enhance the potential of the digital economy, that we wish to see guide this text? Which tools and associated measures do we want to adopt govern it?

There is no single answer to these two questions. The governance selected will be the result of the social pact that has to be established between the public and private players after an in-depth debate, which is also likely to develop over time. The balance sought is therefore intrinsically dynamic.

The re-negotiation of the 1995 Directive is not a minor topic, especially in the digital age, whose real "fuel" is personal data, and in the context

of the emergence of new services such as cloud computing, of the expectations and concerns sparked off by these developments, and not forgetting of the increasing and sometimes dangerous interdependence between our countries in terms of security and infrastructures. It concerns citizens' confidence in future growth and in the institutions responsible for protecting their rights – it concerns the economic competitiveness of European businesses and the Union's consistency and credibility.

The adaptation of the Community framework is an objective which is all the more difficult, since other countries and regions of the world are thinking along similar lines, whether this involves the "Bill of Rights" on the protection of personal data published by the White House in February 2012 or the work undertaken by the APEC on international data transfers. Our work will therefore be compared against other existing international alternatives. The challenge will be to reach a high level of protection, whilst guaranteeing the mutual inter-operability of the various systems. It is against this backdrop that the European Commission's initiative is being taken.

Does this project meet the various requirements that we have just mentioned? In the main, we can say "yes". Can it be improved for it to convey a pragmatic view of personal data protection, which respects the fundamental principles applicable in this area without turning Europe into an island that the digital economy will simply bypass? We might answer – "almost certainly".

The French Data Protection Authority (CNIL, Commission nationale de l'informatique et des libertés) which has developed knowledge of the players and processes over the last thirty years intends – as part of a constructive and positive approach-to help improving the future common legal framework. The future governance established in this area will be called upon to serve as a model and to become a reference of the privacy protection, notably within French-speaking areas. Europe must emerge stronger, more integrated and better equipped to face the globalisation of data transfers without abandoning its principles and values of which the citizen is the focal point.

The draft Regulation put forward by the European Commission on 25th January primarily reflects a new balance of rights, obligations and applicable sanctions to which the CNIL has given its total support (I). Beyond its fundamental features, a number of improvements deserve to be highlighted and promoted in the upcoming negotiations. However the steering structure of personal data protection envisaged by the Commission is not adapted to the reality of the digital world, since the "main establishment" criterion that it promotes is legally uncertain and inapplicable in practice (II). In fact, the objective is to provide an answer to two distinct issues: to facilitate the completion of formalities by businesses and their compliance with the legislation; to enable the improvement of controls and sanctions applied by the national supervisory authorities when data of interest to several EU countries is being processed. It is with regard to these two questions that the CNIL is putting forward a effective, and protective system that will help towards European integration.

## I. THE DRAFT REGULATION: A NEW BALANCE IN TERMS OF RIGHTS, OBLIGATIONS AND SANCTIONS

### *1. Real progress*

The European Commission, and more particularly its Vice-President Viviane Reding, has been determined to bring an effective message: "*one continent= one applicable rule*". The CNIL cannot but support this perspective, even though it does not agree with all the results that the Commission expects to draw from it.

It is indeed certain that, on this basis, the 1995 Directive is no longer a perfectly appropriate instrument. Whilst globalisation is moving forward, leading to greater data exchange, and Europe has an interest in creating a single personal data market, the Directive has been implemented differently at national level giving rise to discrepancies among Member States, owing to the national rules applicable in this area. As an example, since 2004 the CNIL has been granted the authority to apply sanctions, which it does regularly, whilst many national authorities do not enjoy the same powers or have only been conferred the same power well after. A reform of the normative framework there-

fore seems appropriate in order to do so.

In this area that affects individuals' fundamental liberties, the adoption of a Regulation would undeniably enable to partially reduce these inconsistencies via the application of a single text across the entire EU. Such a step is incidentally both a guarantee for the citizen, a means to enhance legal certainty for data controllers – primarily businesses – and a means to improve cooperation between supervisory authorities.

But beyond the nature of the normative vector used, the Regulation leads to a change in paradigm in the regulation of personal data, not as far as the principles themselves are concerned but regarding the regulation tools made available to both players and regulators.
As a matter of fact effect the present system is marked by the importance of preliminary formalities, notably as part of the "notifications" regime for automatic data processing to make with the national supervisory authorities. These formalities illustrate the quintessence of the "data protection" principles and are *a priori* supervised by the regulator. As an example, the CNIL registers 80,000 notifications per year. This process is considered to be extremely cumbersome, sometimes fragmentary – since all of those involved are not always aware of what they are obliged to declare – and in certain cases, it is not conducive enough to achieve scalable compliance on the part of "data controllers". In concrete terms, once the preliminary formalities have been completed, the main means of ensuring effective compliance with a measure is the introduction of a posterior monitoring mechanism that can lead to the adoption of coercive measures, the issuance of a warning and even the imposition of a sanction.

In addition to this strong but somehow binary logic, the draft Regulation proposes a ternary vision consisting in significantly reducing preliminary formalities, strengthening monitoring and sanctioning powers and between these two, adding a further layer of responsibility of the players, referred to as, *accountability*. The idea is simple: given the sharp rise of personal data, data controllers must include the principles of "IT and liberties" in their everyday practices because the sanction policy and preliminary formalities alone cannot govern it all. The introduction of internal compliance policies involving a certain number of tools provided for in the Regulation is therefore a new objective for regulators, who are concerned about effectively taking on board the dynamic and progressive reality of the digital world.

The CNIL supports this general direction which is part of a "co-regulation" approach, vital in a complex world such as the digital environment. Such a process is necessary both from the citizens' point of view and that of the business world. For the latter, and in particular those mainly involved in a digital activity, personal data can have a commercial value and even be a financial asset. But above all, the effective protection of this data is now a major and shared expectation of citizens, who are also consumers, from an economic point of view. Reliability in this area is therefore a decisive commercial and economic requirement because it impacts both individual and collective confidence. The protection of personal data has now become an element of responsibility and competitive advantage.

Naturally, supervisory authorities will have to help businesses define binding internal ethical rules regarding data protection, the introduction of which will obviously have to be assess by the same authorities to the advantage of the company – for example in the event of a security loophole leading to the infringement of personal data confidentiality or in the event of an ex post audit revealing a lack of compliance. *In fine*, the abolition of notifications, synonymous with a simplification for businesses, will therefore be compensated for, in terms of protection, by these compliance mechanisms. The draft Regulation is therefore extremely innovative and adapted to the digital era in that it strikes a new balance between preliminary formalities, compliance and sanctions.

### *2. …whose sustainability has to be guaranteed.*

The main progress of the draft Regulation focuses on two points: the strengthening of individual rights, and the conditions according to which businesses can process and exchange personal data.
Regarding individual rights, and without drawing up an exhaustive list, we may note the strengthening of

individual consent, which must now be explicit, the acknowledgement of a right to "be forgotten" and the right to portability, which are major steps forward.

The "right to be forgotten" seems to be especially vital whilst the development of social networks in particular is leading to an increasing exposure of individuals' private lives, particularly that of young people, and that it is now possible to take out insurance designed to protect one's "e-reputation"! The right to be forgotten is the desire of us all to keep control over our digital tracks and our private or public life online. In this respect, the Regulation could nevertheless be more ambitious: although it is specified under the draft Regulation that citizens will not have to justify their request to delete their data except when the company can legitimately justify their retention, there is no obligation to "de-referencing" by search engines, even though these are r the main entry in the search for personal data on the Internet. Finally, the draft text provides for the specific protection of children under 13, which is of course positive even though the age defined will necessarily be subject to debate.

As for the positive aspects for businesses the simplification of preliminary formalities and the development of compliance processes reconciles the demands for pragmatism and protection on the whole: the obligatory appointment of a data protection officer – which France, like Germany and the Netherlands, has introduced in law as the "CIL- Correspondant Informatique et Libertés" – or *accountability* will help to involve all stakeholders and also to guarantee a high standard of quality of European businesses vis-à-vis the consumer. It is true that the proposal includes some significant steps forward as regards the rights and obligations; however the means of implementation designed is far from being adequate.

## II. BUT AN ENVISAGED MEANS OF IMPLEMENTATION THAT IS POORLY ADAPTED TO THE REALITY OF THE DIGITAL ENVIRONMENT

The protection of personal data is a stand-alone right which overlaps with other fundamental rights, notably that of property rights, the right to the respect of privacy and the freedom of expression. It is also linked to economic and commercial principles, particularly in the area of consumer protection and advertising rules. It also influences company organisation whatever their size. It is exactly this central position in the exercise of liberties, vital from an economic point of view, notably regarding the digital economy, which is the source of expectations but also of deep concern on the part of European citizens. And such concern cannot be eased, nor can rights be guaranteed just because legislation has been passed.

Governing the use of personal data – vital for the individual, from the point of view of citizens as well as of consumers, and therefore vital for democratic life and for businesses – implies the implementation of a measure likely to win the confidence of all. We believe this is where the problem lies in the draft Regulation.

As its base the latter intends to use a formula that appears simple and effective: "one continent= one rule = one competent supervisory authority when data processing takes place in several countries". Although we support the first two terms in the formula, the third, as defined by the Commission, is neither likely to find confidence amongst citizens nor such as to enable effective supervision personal data protection.

What does the draft Regulation say on this point? Article 51-2 specifies that "*When the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.*" In other words, when data is to be processed across several Union countries, the national authority of the country where the company's HQ (main establishment) in question is located would be the only one competent to supervise it.
The criterion hence set out is legally vague on the one hand, and it does not provide a satisfactory answer

to the authorities, or to businesses, or to the citizens.

It is legally vague because at present no one is able to see what the reality of the main establishment is. The draft Regulation defines the main establishment as the place where "*effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements*" is undertaken. Not only has the option of case by case processing been chosen – which means that potentially the same group will have as many main establishments as it carries out processing tasks – but it also implies an assessment of pure fact, subject to interpretation and debate, thus tantamount to legal uncertainty for the citizen, the company and the supervisory authority. A different definition has sometimes been mentioned, quoting the place where the company's data protection policy is defined. But again, this implies an assessment based on facts and not on a criterion of law. Moreover the mechanism that has been drawn up is difficult to apply from an institutional point of view: first it means that the supervisory authority will determine the main establishment, which the company may challenge, at the risk of a possible, ulterior failure of the procedure. But above all, it turns the national authorities to which the matter is referred by their short-changed nationals, into simple "letter boxes", void of all competence over the request insofar as the Regulation provides for the exclusive competence of the authority of the country where the so-called "main establishment" is located. To address the adverse effects of this, the draft Regulation designs a system in which the supervisory authorities may, on the request of their respective nationals, challenge one another's decisions. But even though such a mechanism is driven forward by a laudable desire for simplification, it would actually lead to the opposite effect from that intended: reduced European integration, competition between the different authorities and in fine reduced protection for the citizen.

And this is where the main danger lies: the proposed mechanism weakens citizen protection. Early in the process, it will encourage circumvention strategies from unscrupulous players, notably depending on the means available to the supervisory authorities in each Member State. To a certain extent, there will be risk of "data-dumping" depending on the effective capabilities of the supervisory authorities, as well as on other legislations with which data protection must be reconciled (social law, labour law etc ...). At later stages, in the event of complaints and inspections, the competent authority might possibly be that of the instigator of the offence and not that of the citizen-victim. This system, which is typified by the territoriality of both administrative and jurisdictional supervision, that favours the potential perpetrator of the offence, is evidently greatly to the citizens' disadvantage. Beyond this, we might question the efficiency of the right to a remedy available to the latter, which is however promoted in the preamble of the Regulation, and more generally of the respect of defence rights. It is not difficult to imagine the feeling of powerlessness, concern and even mistrust felt by a citizen who does not know who to turn to, considering his/her nearest authority as a simple letterbox and obliged to seek remedies before jurisdictions of other Member States, notwithstanding what this would mean in terms of cost, translation and ignorance of the legal systems of other States.

Finally, such mistrust would combine with compliance difficulties for the companies themselves. At no moment does the Regulation define the "main establishment" and other entities' (notably the headquarters or subsidiaries) respective responsibilities. The system that has been drawn up is actually intended for a specific type of business, i.e. the main players on the Internet and online sales companies. However most businesses in the industrial or tertiary sectors are not organised centrally, on the contrary, they are decentralized in accordance with the principle of subsidiary independence. Therefore, the proposed system is not very clear for the citizen and not very effective in terms of the right to appeal; it is ill-suited to the organisational diversity of the business world and difficult to implement between regulation authorities who are also called upon to work together in order to ensure the uniform application of Community Regulation. Quite simply the measure is not operational.

## III. TOWARDS ANOTHER TYPE OF GOVERNANCE

### *1. In support of an effective European Regulation for the protection of personal data.*

The present system, which comes from the 1995 raises two substantial difficulties. The first one, which arises at the preliminary formalities stage, is that the "territorialisation" of these formalities requires businesses that want to process data automatically in several countries, to overcome huge amounts of paperwork. These repetitive processes are expensive – the European Commission quotes 2.4 billion € per year, which however has to be considered in the context of the total number of companies in the Union. But more importantly, they give rise to puzzlement and even legal uncertainty for businesses, because of the variety of applicable procedures and deadlines. The second difficulty lies, at the stage of examining complaints and inspections, in the impossibility for the supervisory authorities to take a joint decision on sanctions when common processing in several EU countries is being questioned.

The European Commission believed it necessary to provide a single response to this dual problem. The CNIL proposed instead to distinguish the two and thus to set up a legible system for the citizen, easy for the company to implement, and which can be more effectively supervised by the national supervisory authorities. In our opinion, data protection means satisfying two requirements: placing the citizen at the centre of the system; creating a supervisory system that is both decentralised and integrated.

The starting point is the criterion used to determine the ordinary jurisdiction of the national authorities. We suggest opting for the criterion of the citizen's place of residence, and as an alternative, that of the data controller's establishment. In other words, when a citizen's personal data is to be processed, the authority of his/her country of residence, must, as a principle, be acknowledged as competent to ensure that data is processed in conformity with the Regulation. From this point the two details that were previously mentioned should be distinguished one from the other:

a) On the first point – "upstream" business compliance - we suggest offering businesses that have several establishments in the EU the opportunity of appointing the unit responsible for protecting data and on this basis of having one contact point for this purpose. Since businesses need both a certain amount of organisational flexibility and in some cases "a single entry point" to deal with formalities, we suggest they be given the possibility of having "a reference point", that would be legally responsible for data processings that are common to several EU countries; it would be the responsibility of the authorities of the countries whose residents are involved to make contact with each other as part of the cooperation mechanism.
Such a solution offers the advantage of being adapted to the structure of the businesses in question. Those do not need to be told how to organise internally. On the contrary they need to be able to decide which organization suits them best, according to their industry and strategic priorities; this means that the public authorities should in a position to monitor compliance with the substantive requirements, by interfering as little as possible with the company's internal organisation. In this respect, by offering businesses the opportunity of appointing a reference unit to pursue the compliance policy and to complete the preliminary formalities and by giving them one point of contact, various types of economic models from the traditional industrial group to the digital economy operator can then be covered. Such mechanism is synonymous with legal certainty, since the reference unit is actually the data controller for processings common to several Union countries.

In concrete terms, the criteria put forward (place of processing, headquarters, and place of definition of privacy policy) might all be used as a body of evidence to help businesses choose the "reference unit", as in competition Law. Hence, they will be able to select the most relevant unit according to their economic reality.

As for the supervisory authorities, the present draft Regulation would result in the selection of a criterion in deed, applicable case by case – leading the authorities to interfere with a company's organisation and daily life as far as defining the main establishment is concerned. Our proposal however, whereby the reference unit

is the one responsible for processing, is to opt for a criterion of law, as far as the "lead" authority, in terms of accountability is concerned: if the company so wishes it will be the criterion of the main data controller. If this not what the company wants then the present situation will hold sway – there will be as many contact points as countries involved – but as part of a legal framework marked by a significant reduction of preliminary formalities. In practical terms, the supervisory authorities will have to cooperate with the "lead" authority – the only point of contact.

b) Regarding the second point – competence over inspections and sanctions – we suggest, in line with the Art. 29 Working Party's opinion on the data protection reform proposals, the introduction of a lead authority mechanism. Every national authority that receives a complaint lodged by a national or, on its own motion,, would be competent to investigate on processings carried out within its borders. The main competence criterion is therefore one of "targeting" the place where the citizen resides – as for example in EU consumer Law – wherever the data controller is located. When several European countries are involved, the various competent authorities would have to appoint a "lead authority" to lead the joint investigation on their behalf. This "lead" authority would obviously be able to use the expertise and means available to the other authorities. The decision to take out sanctions would then be made, either jointly by the authorities involved (co-decision), or following an opinion procedure that could give rise to "a dissenting opinion."

In practical terms the lead authority might be selected according to criteria such as – and by order of priority - the date or number of complaints; the country where the "reference unit" is located- it would then be the same as the lead authority responsible for ensuring "accountability"; the country where the processing takes place. For the citizen, this system would be legible: it is actually the authority in his/her country which is competent once the citizen has been involved in the data processing– it is the responsibility of this authority to make arrangements with its counterparts if necessary. The citizen's right to remedy is totally protected since the place of administrative supervision corresponds to the country of potential jurisdictional litigation. Finally, it is very consistent for the citizen whatever the company's situation: whether the operator is established in the EU or not, the criteria of competence of the supervisory authority remains the same: the place of residence of the citizen. The system also means legal certainty and institutional clarity for companies: they can be audited wherever they process data, but according to common criteria and as part of a procedure which guarantees them a uniform supervision and administrative sanction. Finally, for the national authorities, this mechanism enables to protect a competence close to the field and business reality.

The CNIL is therefore putting forward an alternative solution to that of the main establishment criterion, by using known legal concepts and which serves the goals that have guided the European Commission's work. The challenge is to allow greater cooperation, and even an integrated decision making between the sovereign national authorities, in conformity with the Community's subsidiarity principle. Clarity, legal certainty, simplicity, effectiveness: these are key ideas in this proposal which aims at protecting citizen's confidence. This proposal also defines quite precisely what is meant by accountability.

### *2. Effectively defining the meaning of the term accountability*

Firstly, we toned to define what it really means: the concept of accountability which is fashionable is nevertheless, rather vague. However, given the central position played by this concept in the draft text, it needs to be properly defined. We suggest the following meaning: *the permanent and dynamic compliance process of a company with the principles of IT and liberties through the use of a set of binding rules and corresponding good practices*, while the company can enjoy the assistance of the regulation authority in this endeavour.

In particular, the draft Regulation provides that data controllers and data processors will have to introduce internal rules and transparent policies regarding data protection and in particular, to conduct impact assessment of risky data processings to personal data protection, to warn the person in the event of data breach, to appoint a data protection officer and to implement technical and operational measures in order to guarantee data security. The proposal thus meets some of the requirements that the CNIL has always prescribed when assisting businesses in ensuring personal data protection: protection and information of the individual; early inclusion of data protection right from the policy design stage or when making a strategic choice, and finally, logical and physical data security measures.

In the end, the real question regards the content to be given to this objective. There are two views on this: Some believe "accountability" means a list of "passive" requirements, such as "checkboxes" that the company will simply have to tick in order to achieve compliance;

here, accountability would be synonymous with a liability disclaimer! Others, like the CNIL, take the view that beyond this, accountability refers to a real and virtuous compliance, ie one that is likely to both strengthen consumer confidence and generate added value for companies which must become part of a sustainable responsibility process. It is precisely because it affects the heart of the matter that accountability could be included by regulators in their sanction policies.

In this regard, the CNIL can be nothing but reluctant about measures that open the way for businesses to transfer personal data to "third" countries that do not have the same level of protection, by using non-binding legal instruments, formulated in the wake of an internal assessment of the dangers involved in the transfer. It is not the company's responsibility to assess itself, but rather to adopt a corporate social responsibility approach that includes personal data protection in conjunction with the competent supervisory authorities. It is precisely this relationship that will guarantee an optimal protection of personal data.

### *3. Making new personal rights effective*

People fear the new digital world and yet benefit widely from its services. They worry they will not have control over their digital records; they fear the establishment of a big brother society and finally they fear that modernity might turn against them.
Hence expectations about the future Regulation are high in this respect. In our opinion, the strengthening of citizens rights means in this regard the introduction of a real "de-referencing right" which is the corollary to the right to be forgotten in the digital era. Indeed how can we conceive the right to be forgotten as a simple right to erasure, if these can be used rapidly on a large scale and on a permanent basis regardless of time or borders? Only an effective and duly supervised right to de-referencing, will make the future "right to be forgotten" effective in the way that the European Union did it in the past with the right to erasure.

## CONCLUSION

The Commission's proposal is now being debated in Parliament. Europe – like the rest of the world – faces a major challenge in order to ensure appropriate protection of its citizens' personal data without impeding the formidable development of the digital environment, notably in the economic area. Basically, it is now a question of applying the Regulation, territorial by definition, governing a partially de-territorialised phenomenon.. In this context personal data protection is based on three pillars: citizens, data controllers - more specifically businesses and their processors- and supervisory authorities. For the former, it means fundamental freedom; for the latter it must become a component of their social responsibility and for authorities, protection requires close cooperation, possibly a co-decision mechanism in certain cases.

This is what CNIL's proposal is aimed at: – at the service of the citizen, for the benefit of businesses and in support of the Union that is responsible for protecting them.

**Isabelle Falque-Pierrotin**

State Counsellor and chair of the French Data Protection Authority (CNIL-Commission nationale de l'informatique et des libertés) since 21st September 2011. Former Chair of the Policy Board and Delegate General of the Internet Rights Forum from 2001 to December 2010. She has been a member of the CNIL since January 2004.

You can read all of our publications on our site:
**www.robert-schuman.eu**

Publishing Director: Pascale JOANNIN