

Opinion of the Committee of the Regions on 'Data protection package'

(2012/C 391/13)

THE COMMITTEE OF THE REGIONS

- welcomes the proposals for a reform of European data protection law as a contribution by the European Union to the global debate on adequately protecting privacy in a digital world;
- considers it imperative that key questions surrounding protection of personal data be resolved as part of the proper legislative process, so as to ensure transparency and democratic legitimacy through the full involvement of the Council of the European Union, the European Parliament and representatives of European LRAs;
- notes that notwithstanding the unresolved issues of compliance of the regulation's underlying concept with the principles of subsidiarity and proportionality, certain detailed rules also place additional undue limits on national legislation on data processing by public bodies in the Member States;
- further considers that the proposed regulation should give greater decision-making scope to the Member States and, where appropriate, to the regions, so that, in accordance with domestic law, it regulates the general conditions applicable to members of the supervisory authority to ensure they are able to perform their duties independently.

Rapporteur	Ursula MÄNNLE (DE/EPP), Member of the Bavarian State Assembly
Reference documents	<p>Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century</p> <p>COM(2012) 9 final</p> <p>Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data</p> <p>COM(2012) 10 final</p> <p>Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)</p> <p>COM(2012) 11 final</p>

I. POLICY RECOMMENDATIONS

Given the ubiquity of data processing in the modern information society, data protection rules are of key importance for economic development, for the smooth operation and efficiency of government activity and for European citizens' individual liberties. Adapting data protection to the changed demands of a digital world, where ever more spheres of life are linked up via the internet, is thus one of the key reform projects not only for the European Union, but also for other international organisations such as the Council of Europe, and countries such as the USA. Personal data protection raises questions in all policy areas. Data protection is cross-sectoral and touches on areas such as security and justice policy, the economy, communications, education, health, administration and consumer protection. As a result, enhancing data protection law is also of key importance to Europe's towns and cities in securing and bolstering their future viability at a time of fundamental technological change and global competition.

THE COMMITTEE OF THE REGIONS

1. welcomes the proposals for a reform of European data protection law as a contribution by the European Union to the global debate on adequately protecting privacy in a digital world;

2. underlines the pivotal role of local and regional authorities (LRAs) in implementing the recommendations of the Digital Agenda for Europe. They represent the engine of economic growth at local and regional level and generate, use and manage many digital information products and services, supported by databases of public sector information. For this reason, LRAs must have extensive and effectively input into laws that will affect their data protection competences; the

regulation will introduce new red tape and costs for municipalities and regions which in the Committee's view are not offset by the benefits to citizens;

3. welcomes the reform package's general objectives of ensuring, in accordance with Article 8 of the Charter of Fundamental Rights and Article 16 of the Treaty on the Functioning of the European Union, a harmonisation at European level of the protection of individuals with regard to the processing of personal data;

4. notes that harmonising legal data protection requirements by way of binding common standards means that data protection procedures carried out by businesses, government bodies and individuals will be subject to the same requirements despite differing levels of risk and different operating environments. The Committee of the Regions believes that the regulation is unduly negative for public authorities and leaves ambiguities with regard to their competences as well as in the context of employment law. The regulation also introduces a series of requirements for local and regional authorities (e.g. increased documentation, obligation to ensure data portability) which are not offset by marked improvements in the rights of those concerned. The Committee points out that, because of its level of abstraction, the proposed legal act in the form of a regulation may open the way to a misuse of Article 290 TFEU, which gives the Commission powers to issue further rules, even on essential matters, and it is therefore incompatible with the subsidiarity and proportionality principles. It therefore calls for processing by public authorities of personal data and in the context of employment law to be excluded from the scope of the regulation so that processing by public authorities of personal data and in the context of employment law continue to be governed by a directive;

5. underlines the key responsibility of independent data protection authorities for the protection of personal data; however, a high level of data protection in a connected world with virtual ubiquity of data processing will not be guaranteed only by attempts to strengthen statutory duties, but requires also additional incentive instruments for processors to reward efforts for data protection i.e. by facilitating the burden of proof for processors who submit to demanding self regulation standards or codes of conduct or establish voluntary data protection impact assessments;

6. considers it imperative that key questions surrounding protection of personal data be resolved as part of the proper legislative process, so as to ensure transparency and democratic legitimacy through the full involvement of the Council of the European Union, the European Parliament and representatives of European LRAs;

7. recognises the general need to create binding rules for police and judicial co-operation on protecting personal data that is exchanged across borders;

8. warns against imposing excessive constraints on individuals in the exercise of their right to control of their own information in an effort to increase the protection of personal data, depriving them of the possibility of giving consent, particularly in relation to public authorities, within the scope of both the General Data Protection Regulation and the Data Protection Directive;

9. with these considerations in mind, feels that the following individual issues need to be addressed at later stages of the legislative process:

Subsidiarity and proportionality

10. is convinced that, insofar as it concerns the private sector, there is good reason to try to fully harmonise parts of European data protection law by replacing it with a regulation;

11. notes, however, that given the fact that numerous European and national data protection laws relating to telecommunications in particular are being retained, the package of the General Data Protection Regulation and the Directive relating to the police and justice have repeatedly prompted basic objections in consultation concerning its compliance with the principles of subsidiarity and proportionality. Objections have been raised about:

— the scope of EU jurisdiction under Article 16(2) TFEU, which places limits on the desired full harmonisation of public sector data processing in particular, and raises questions about encroachment on purely national level affairs when it comes to the Directive relating to the police and justice;

— the level of abstraction of the regulation, which is comparable to an EU directive, but provides too little legal certainty in the absence of transposing measures by the

Member States, and the European Commission's power to adopt delegated acts (cf. Article 86) on issues that are no matters of detail, which is problematic;

— the lack of clarity concerning the scope of application of the national laws (Chapter IX), in those cases where more than one Member States are involved;

— the lack of coordination between the rules to be introduced by the Regulation and large sections of directives – provisions concerning telecommunications that form a key part of the legal framework governing use of the internet (e.g. Directive 2002/58/EC);

— the failure to secure adequate legal protection against violation of fundamental rights, given that there is no direct appeal process to the Court of Justice of the European Union offering legal protection for individuals;

— the failure to adequately address tensions between data protection interests and other fundamental rights, such as freedom of speech and the principle of public access; and

— the lack of clear borders between the scope of the draft regulation and the draft directive.

12. underlines that these objections reflect the misgivings of many European LRAs about draft regulations that, for example, make national exceptions impossible when protecting data in social services, or burden public bodies with data protection requirements like the right to data portability, that may seem only relevant to the data processing procedures of business and that entail heavy administrative sanctions in view of local authorities' financial resources;

13. feels that the proposed Data Protection Regulation should make it clearer that the restrictions set out in Article 83 regarding the processing of personal data for historical, statistical and scientific research purposes must not curtail the ability of public bodies to store documents in line with national legislation on archives and on access to administrative documents;

14. therefore underlines the need at later stages of the legislative process to reflect even more on which legal instrument is chosen and how the borders are drawn between the scope of the draft regulation and that of the draft directive, investigating potential alternatives that are more in line with the principles of subsidiarity and proportionality than this package. These would include the option of processing by public authorities of personal data and in the context of employment law continuing to be governed by a directive, so that processing of personal

data by public authorities and processing of data in the employment context would be excluded from the scope of application of the general data protection regulation;

International consistency rather than the principle of the marketplace

15. supports the objective of also applying European data protection standards to international suppliers of information services;

16. is convinced that the initiative for a legal framework for privacy protection in a global information economy, which is being proposed at the same time by the US government, offers an opportunity to combine reform efforts for common protection standards in key spheres of international data traffic, thus not only implementing effective data protection rules but also avoiding divergent conditions for competition more effectively than through application of the marketplace principle, which is limited in its practical application;

Future viability of the reform proposal

17. notes that the draft General Data Protection Regulation is essentially based on the principles of the Data Protection Directive 95/46 EC, which are only improved in certain cases such as the principle of "privacy by design", but are certainly modified. Unlike when the Data Protection Directive was drafted, the risks involved in processing personal data in an information society, be it in the private or public sector, are no longer shaped by one-to-one relationships. Digitalisation and networking are instead creating systems in which several authorities are involved in processing data, e.g. combining of records or sharing of data between authorities;

18. underlines that the questions this raises about protection of personal data cannot be adequately addressed with such traditional bipolar concepts as "controller", the "right to be forgotten" or the principle of prohibition concerning the relationship between government and citizen (Articles 6 and 9 of the draft regulation). Some changes to the provisions in the Directive, such as the redefinition of "personal data" and "consent", do more to exacerbate legal ambiguities than resolve them;

19. therefore believes that if the Commission maintains its preference for a regulation, the proposal should specify that an employer may process data based on the employee's consent; the same applies to public authorities, within the scope of both the General Data Protection Regulation and the Data Protection Directive; in accordance with the Regulation, Member States may, by law, regulate the processing of employees' personal data in the employment context;

20. therefore considers it necessary, given that a completely new concept is no longer possible at this stage of the legislative

process, to rethink the enforcement mechanisms that have so far focused too much on regulatory, equally bipolar legal instruments and sanctions. In the view of LRAs, which are closest to data subjects, the following may be of key importance:

- measures to raise awareness of data protection issues among all generations and sections of the population;
- mechanisms for sharing proven and technologically advanced approaches to data protection, for example as part of a seal of quality scheme;
- standardised, easily comprehensible information and public awareness campaigns using the traffic light principle;
- binding and regulated certification mechanisms; and
- mechanisms for self-regulation;

21. stresses here that these tasks, which are to be discharged mainly by the supervisory authorities, are currently given a lower priority in the draft General Data Protection Regulation, for example as part of information sharing under Article 52(2) of the draft regulation, or in the codes of conduct in Article 38;

Retaining latitude for national legislation

22. notes that notwithstanding the unresolved issues of compliance of the regulation's underlying concept with the principles of subsidiarity and proportionality, certain detailed rules also place additional undue limits on national legislation on data processing by public bodies in the Member States;

23. therefore considers that processing by public authorities of personal data and the sphere of employment law should continue to be governed by a directive;

24. therefore takes the view that, if the Commission maintains its preference for a regulation that would also govern public bodies and the context of employment law:

- the conditions for Member State regulation of the basis of data processing obligations, provided for in Article 6(3) of the draft regulation, should not be further complicated by invoking the limits contained in Article 52 of the Charter of Fundamental Rights in a way that exceeds its intended scope;
- the same applies to giving the Commission powers to issue delegated acts further specifying the limits on regulatory areas given over to the Member States, such as processing of health or employee data, or data processing for historical or statistical purposes, or for the purpose of scientific research;

- in both fields, the possibility of consent must be expressly mentioned; in relation to public authorities, this also applies within the scope of the Data Protection Directive;
- in order to comply with the principles of proportionality and subsidiarity, the Commission should, with regard to all delegated acts (Article 86), be obliged to carry out a comprehensive impact assessment and to consult the Council, the parliaments of the Member States and affected members of the public, as well as the Committees, which under the TFEU must be involved when introducing legislative acts, and the European Data Protection Board; similarly, when issuing implementing acts, procedures should be chosen that ensure timely and full participation by all affected groups;
- in addition to the rights given to Member States to grant exceptions stipulated in Article 21, the regulation should also at least allow Member States scope for national legislation that subjects data processing used in exercising public authority to different safeguards in line with the objectives of Article 8 of the Charter of Fundamental Rights, as currently provided for in the regulation;
- in fixing the scope of the regulation, it should be made clear that its rules only apply to activities within "the scope of Union law", in which the European Union is empowered to issue binding regulations, and not in areas that still fall within Member State competence, or in which the Treaties expressly preclude the power to harmonise legal and administrative requirements, for example in education systems (Article 165(4) TFEU);
- Article 82 of the regulation should stipulate that specific rules may be adopted for processing of personal data in the context of collective agreements in the employment context;
- the regulation must ensure that management rights are not limited, e.g. in the context of recruitment or dismissal of a controller;
- it must be ensured that powers to penalise non-compliance with data protection requirements should clearly differentiate between private, profit-oriented bodies and other bodies, particularly government bodies, for which fines levied on profits are not appropriate and where political control mechanisms are more effective;

Reinforcing democratic responsibility

25. is deeply concerned that if and when the regulation takes effect, the elaborated and extended legal requirements for data protection will translate into procedures that offer no guarantee of transparency or sufficient democratic legitimacy, unlike legislation by the Member States or the European Union or implementation of national and European law by administrative bodies supervised by parliaments in the Member States;

26. justifies this concern with reference to the draft regulation's creation of deeply abstract, binding, yet standardised and enforceable obligations in an area that is to be pivotal in securing various fundamental rights, and which is already characterised by a barely comprehensible array of different areas of application, ranging from private address directories and public registers of residents to data from social networks and internet search machine providers. Moreover, all but unavoidable shortcomings in clarity of rules, legal certainty and enforceability are, on the one hand, meant to be offset by a series of powers to issue delegated acts that often touch on fundamental aspects of the regulatory framework, such as the power granted in Article 6(5). On the other hand, independent data protection authorities are given powers well beyond their traditional implementing tasks to create what are, in effect, equally abstract and general rules as part of general guidelines on interpreting the Data Protection Regulation. They are thereby subject to undue powers by the Commission to exert influence under the "consistency mechanism", throwing into question the independence granted to them under Article 16(2)(2) TFEU;

27. considers it therefore necessary to fundamentally change the arrangements for Commission participation through the consistency mechanism to guarantee the independence of data protection authorities, particularly their competences under Articles 60 and 62(1)(a) of the draft regulation, as well as the definition of "serious doubts", under the same Articles, on the basis of which the Commission interferes;

28. further considers that the proposed regulation should give greater decision-making scope to the Member States and, where appropriate, to the regions, so that, in accordance with domestic law, it regulates the general conditions applicable to members of the supervisory authority to ensure they are able to perform their duties independently;

29. is also convinced that the control instruments for the independent supervisory authorities that are also recognised by the Court of Justice of the European Union, such as reports and other regular forms of consultation with lawmaking bodies, should be further developed to allow the Parliament, the Council and the Committee of the Regions, as part of their rights of participation, a regular overview of how European data protection law is implemented, and to give them the opportunity to launch initiatives to improve it. In addition, in accordance with the fundamental right to be heard, additional procedural regulations should be introduced to oblige supervisory authorities and the European Data Protection Board to involve associations and interest groups materially affected by decisions, for example under Article 58(2), in a transparent process of developing and improving data protection law, for example by way of hearings or consultation procedures;

Limits of harmonisation of data protection relating to the police and justice

30. doubts whether regulation of exclusively national-level data processing by way of a proposal for a directive relating to the police and justice falls within the legislative competence of the European Union or complies with the principles of subsidiarity and proportionality. Apart from crime-fighting tasks related to terrorism, organised crime and cybercrime, large databases are still available to the police and law enforcement authorities that are only processed at national level and therefore do not require data protection regulation at European level. A further consequence of data protection regulations that needs to be taken into consideration is their direct impact on other police and law enforcement legislation, and thus their indirect harmonising force even though the European Union does not have adequate competence in this area;

31. is surprised that the European institutions and organs, starting with Eurojust and Europol, are excluded from the scope of the directive;

32. besides these general reservations, calls on the Commission to review the following at later stages of the legislative process:

- the extent to which obligations to extensively document and report on their activities can lead to delays in police investigations and law enforcement;
- whether the provisions under (b), (c) and (d) of Article 7 of the draft directive are compatible with Article 1 (1), which defines the subject matter and objectives of the directive;
- that while proven forms of data sharing with third countries should not be unduly limited or impeded, adequate safeguards should be applied for derogations related to international transfers in individual cases (Article 36); and
- which powers for the Commission to issue delegated acts and stipulate implementation rules could be replaced by the Member States with more specific rules in a normal act or with an equivalent opening clause;

33. reserves the right to submit another opinion including detailed proposed amendments as soon as the positions of the Council of the European Union and of the European Parliament on the aforementioned issues becomes clear at a later stage of the legislative process.

II. RECOMMENDATIONS FOR AMENDMENTS

Amendment 1

Article 36

Text proposed by the Commission	CoR amendment
<p>By way of derogation from Articles 34 and 35, Member States shall provide that a transfer of personal data to a third country or an international organisation may take place only on condition that:</p> <p>(a) the transfer is necessary in order to protect the vital interests of the data subject or another person; or</p> <p>(b) the transfer is necessary to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; or</p> <p>(c) the transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third country; or</p> <p>(d) the transfer is necessary in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; or</p> <p>(e) the transfer is necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal penalty.</p>	<p>By way of derogation from Articles 34 and 35, Member States shall provide that a transfer of personal data to a third country or an international organisation may take place only on condition that:</p> <p>(a) the transfer is necessary in order to protect the vital interests of the data subject or another person; or</p> <p>(b) the transfer is necessary to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; or</p> <p>(c) the transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third country; or</p> <p>(d) the transfer is necessary in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; or</p> <p>(e) the transfer is necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal penalty.</p> <p><u>The use of these derogations shall be duly documented.</u></p>

Reason

The expression "is necessary" is far too vague and leaves room for non-restrictive use of the derogations, which is against the spirit of this particular article.

Amendment 2

Article 86.6

Text proposed by the Commission	CoR amendment
	<u>The Commission shall consult, with regard to all delegated and implementing acts, the Council, the parliaments of Member States, as well as the committees, which under TFEU must be involved when introducing legislative acts, and the European Data Protection Board.</u>

Reason

Including an obligation for the Commission to consult the European Data Protection Board (EDPB) with regard to all delegated and implementing acts constitutes a vital safeguard.

Brussels, 10 October 2012.

The President
of the Committee of the Regions
Ramón Luis VALCÁRCEL SISO
