COUNCIL OF THE EUROPEAN UNION

Brussels, 20 February 2014

6798/14

Interinstitutional File: 2012/0011 (COD)

DATAPROTECT 31
JAI 107
MI 198
DRS 29
DAPIX 27
FREMP 30
COMIX 112
CODEC 513

COVER NOTE

from:	Mr Peter HUSTINX, European Data Protection Supervisor
received:	20 February 2014
to:	President of the Council of the European Union
Subject:	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) - Progress on the data protection reform package

Dear Mr President,

In view of the on-going negotiations on the data protection reform package, and in particular of the forthcoming JHA Council meeting on 3-4 March, we would like to draw your attention to a number of outstanding issues.

The modernisation of the existing EU framework for personal data protection is necessary in order to fulfil the obligation incumbent on the EU legislator by virtue of Article 16 TFEU. It is also an essential element of delivering effective protection of the fundamental rights of EU citizens to privacy and personal data protection set out in Articles 7 and 8 of the Charter of Fundamental Rights of the EU[1].

We consider that EU rules on data protection need to be reformed urgently in order to provide more consistency and uniformity in data protection across the EU, thus creating a level playing field, both for online and traditional market players. Citizens, in turn, deserve a more effective protection of their fundamental rights to privacy and data protection, which can only be delivered if the applicable legal framework is coherent (i.e. covers the broadest possible range of data processing entities and activities), as well as consistent (i.e. is applied in a manner as uniform as practicable throughout the 28 Member States).

We note with satisfaction the on-going efforts of the Greek Presidency of the Council to make progress on a number of outstanding issues. We also welcome and support the objective of reaching an agreement on a mandate for negotiation with the European Parliament before the end of the Greek Presidency, and to conclude the negotiation process before the end of 2014.

However, with regard to a number of important elements of the data protection package, it is clear that compromise solutions are not yet within sight. Even more worrying, it appears that the existing *acquis* might be weakened in some respects (such as the scope of the proposed General Data Protection Regulation ('GDPR')).

In view of the on-going discussions, we feel that it is useful to set out the position of the EDPS on three crucial outstanding issues related to the proposed GDPR. We consider this as an essential element of our role as an adviser to the EU institutions on all matters concerning the processing of personal data.

[1] See *inter alia* the Opinion of the EDPS on the data protection reform package of 7 March 2012.

1. The scope of the proposed GDPR

We understand that the option of excluding the public sector from the scope of the GDPR - or at least introducing far-reaching exceptions and derogations - is still on the table. In this respect, we would like to observe that neither the Data Protection Directive 95/46/EC currently in force, nor the Council of Europe Convention 108 (to which all Member States are party) make a distinction between the 'private' and 'public' sectors.

Excluding the public sector would thus not only considerably delay the legislative process, but it would also mean an important step back when compared with today's data protection framework. Moreover, excluding the public sector, or providing for broad exemptions, does not seem justified or necessary. Already today, the data protection rules in force provide for wide possibilities for public sector bodies to process personal data, where necessary in order to comply with a legal obligation, or for tasks performed in the public interest, and this will continue to be the case also under the proposed GDPR.

Moreover, the boundaries between the 'public' and 'private' sectors are much less clear-cut than it might appear. For example, the same type of activities (e.g. the provision of health services) may be performed by private entities in one Member State, and by public bodies in another Member State, or there may be a mix of both within one and the same Member State. **Very similar entities**, processing the same categories of personal data (such as hospitals or universities), **should be subject to the same set of rules, irrespectively of the fact whether they are public bodies or privately owned.**

Furthermore, data exchanges between public bodies and private entities - which are the bloodline of a modern economy and take place on a daily basis in the context of outsourcing or public-private partnerships - can only operate in a seamless way if the same legal framework applies. In many cases public bodies exercise market activities. Subjecting them to different data protection rules than private operators would inevitably distort the level playing field in the internal market.

Finally, such a sweeping carve-out from the EU personal data protection framework would weaken the bargaining position of the EU in its negotiations with third countries, in particular in those cases where the EU has been pushing for the adoption of a comprehensive legal framework for data protection. The same would be true if broad exemptions were provided for the public sector, unless they are strictly necessary and remain limited to very specific situations which are not yet covered by the existing exceptions.

2. The one-stop-shop principle

Put simply, the one-stop-shop principle means that when the processing of personal data takes place in more than one Member State, one single supervisory authority should be responsible for monitoring the activities of the controller or processor throughout the Union and taking the related decisions. According to the proposal, this would normally be the national Data Protection Authority ('DPA') of the Member State where the 'main establishment' of the data processing entity is located, also referred to as the 'lead authority'. In our view, the role of a lead authority should *not* be seen as an *exclusive* competence, but rather as a structured way of cooperating with other locally competent supervisory authorities. Indeed, the lead authority would depend heavily on input and support of other DPAs at different stages of the process[1].

The one-stop-shop principle is an important element of the proposed harmonisation of the legal framework for data protection. It has been proposed by the Commission in order to increase the consistent application, provide legal certainty and reduce administrative burden for controllers and processors that are active in more than one Member State[2]. It reduces the fragmentation of the data protection landscape. It is important for businesses to be able to deal with (ideally) one interlocutor instead of (potentially) 28 national DPAs. We recall that the JHA Council endorsed the principle in October 2013, calling it – together with the consistency mechanism – 'one of the central pillars of the Commission proposal'.

1 See EDPS Opinion of 7 March 2012, para. 237.
2 Recital 97 of the Commission proposal.

Last December, the Legal Service of the Council raised a number of legal objections against the one-stop-shop principle questioning its compatibility with the Charter of Fundamental Rights of the EU, and in particular with Article 47 of the Charter which provides for the right to an effective remedy before a tribunal and a right to a fair trial, and which corresponds in substance to Articles 13 and 6(1) of the ECHR. The predominant concern seems to be the issue of 'proximity' between the DPA taking a decision in a particular case and the individual citizen, which is perceived as 'an important aspect of the protection of individual rights'.

We are of the opinion that the CLS interpretation of the one-stop-shop principle paints an **unduly negative picture** of the proposals currently on the table. Indeed, we consider that it is possible to reconcile the principle with a high standard of protection for citizens' fundamental rights, including those protected by Article 47 of the Charter. This position is based on a number of considerations. We would like to share with you the most important ones.

First and foremost, it is important to underline that today, pursuant to Article 28(6) of Directive 95/46/EC, a DPA is always competent to exercise its powers (which include the investigation of complaints) within the territory of its own Member State. However, unless the complaint concerns a controller (or a processor) with an establishment or equipment in that Member State[1], the effective powers of that DPA to enforce the data protection legislation may in practice be limited. Indeed, the necessity to apply, in a specific case, the national law of a different Member State and the lack of possibilities to conduct investigations or impose sanctions where there is no physical presence of the controller/processor may render the recourse to the DPA purely theoretical and largely ineffective.

[1] This follows from the rules on applicable law set out in Article 4(1)(a), (b) and (c).

By contrast, the proposed GDPR would ensure a uniform legal framework and put in place a mechanism to ensure effective enforcement by DPAs in practice. First of all, citizens would be explicitly given the right to lodge a complaint with the local DPA (or indeed, any other DPA) in order to exercise their rights[1]. But more fundamentally, in cases where today a DPA would have limited options, the new Regulation would ensure effective enforcement by the lead authority in the context of the one-stop-shop (and taking advantage of the consistency mechanism[2]), where necessary with the support of a locally competent DPA. In addition, an individual will always have the possibility to bring legal proceedings against a company established in their country before their national courts for an alleged violation of the regulation[3].

From this perspective, the proposed GDPR will have a **very positive impact** on the possibilities of individuals to enforce their data protection rights**,** and thus constitutes an **important improvement** in the protection of the right to an effective remedy as guaranteed under Article 47 of the Charter.

The proposed GDPR also provides for review of decisions taken by DPAs by the courts[4]. In cases where the one-stop-shop principle applies, an individual wishing to challenge a decision taken by the lead DPA would have to do so before a court in the Member State of the lead DPA, which in many cases would in practice mean the necessity to initiate legal proceedings in another Member State.

In this context, we consider that the sole fact that courts in a Member State other than the country of residence of a citizen must be called upon, does not in itself deprive him or her of effective judicial protection. In fact, under the currently applicable Directive 95/46/EC it is also possible that citizens who wish to complain about the processing of personal data by a company operating in numerous Member States must address themselves to one specific DPA and, if they wish to contest its decisions, must pursue litigation in that same Member State[5]. To our knowledge, there is no reason to call this feature of the current system into question with the Charter of Fundamental Rights.

---

1 Article 73(1) of the proposal.
2 Chapter VII of the proposal.
3 Article 75 of the proposal.
4 Article 73 of the proposal.
5 See e.g. the case of Facebook and the Irish DPA.

The proposed one-stop-shop principle is also criticised for creating excessive obstacles for citizens seeking judicial remedies due to geographical distance involved, unfamiliarity with a foreign legal system, the need to initiate and conduct proceedings in a foreign language, or the costs of such a procedure.

The alternative solution proposed in this respect appears to be the creation of an EU body with legal personality which would play the role of the one-stop-shop. Indeed, setting up such a "data protection agency" at EU level might be tempting at conceptual level. However, this would require a fundamental centralisation of the existing de-centralised structure of data protection supervision, which would – at the very least – not facilitate the decision making process within a reasonable time limit.

More importantly, it does not appear necessary to ensure better protection of fundamental rights of citizens.

It is important to keep in mind that in most cases all relevant actors - data subjects, controller and DPA - will continue to reside in one country. Consequently, the one-stop-shop principle would only apply in a relatively limited number of situations. In other words, although some of those cases may have large impact, the instances in which citizens are affected by decisions of a lead DPA located in a Member State other than their own country of residence would in practice be **much less numerous** than the 'ordinary' cases in which decisions are taken by the 'home' DPA.

Finally, the one-stop-stop principle must be seen in its proper context as an important element contributing to the overall effectiveness and consistency of the future data protection framework. Undoubtedly, a much more uniform data protection system and reduced litigation costs (as litigation would in principle be limited to the jurisdiction of the lead DPA, i.e. that of the main establishment) would be advantageous for businesses across the EU. However, **citizens will also benefit** from more consistent application of a uniform set of data protection rules as it would be the case under the proposed GDPR.

For instance, where a citizen is affected by data processing by a (subsidiary) establishment in his or her home country (and, possibly, other establishments), but all decisions are effectively taken by the main establishment of the controller in another Member State, the possibility to obtain a single decision of a DPA or a court ruling which would be valid and enforceable in all those different Member States would constitute a considerable improvement compared to the current situation.

By the same token, the one-stop-shop also reduces the likelihood of parallel proceedings and the resulting conflicts of jurisdiction, since a procedure in the Member State of the lead authority would normally be sufficient to enforce one's rights EU-wide.

Nevertheless, certain questions related to the future functioning of the one-stop-shop call for further reflection and important details still need to be worked out or further defined. We remain at your disposal to provide any assistance that you may find useful in this process.

3. The risk-based approach and accountability

We have repeatedly welcomed and supported the introduction in the proposed GDPR of the principle of accountability[1] according to which the controller must adopt policies and implement appropriate measures to ensure and be able to demonstrate compliance with the data protection rules, and to ensure that the effectiveness of the measures is verified[2]. This principle should encourage controllers to focus on providing effective protection for citizens, rather than apply a 'box-ticking' approach to satisfying bureaucratic requirements.

1 See Opinion 3/2010 of the Article 29 Working Party of 13 July 2010 on the principle of accountability (WP173).

2 Article 22 of the proposal.

Accountability also means that compliance efforts should be primarily directed at areas where this is most needed, having regard, for example, to the sensitivity of the data or the risk involved in a specific processing operation. In this respect, we appreciate the efforts made by different Council Presidencies so far to appropriately describe the notion of 'risk', which necessarily involves a measure of judgment. In the interest of legal certainty, the proposed GDPR should provide for sufficiently clear criteria according to which such risk assessment should be performed by controllers, including both objective factors (e.g. the number of individuals affected by a specific processing operation) and more subjective notions (e.g. likely adverse effects on a person's privacy). On the basis of those general criteria set out in the GDPR, further guidance could be given either by the European Data Protection Board, or in delegated acts, where appropriate. Such an approach would allow for more legal certainty for controllers, more effective protection for EU citizens, and sufficient flexibility to stand the test of time.

We remain at your disposal to provide further guidance on the issues referred to above, as well as on other elements under discussion, should you consider this useful in bringing the reform process forward.

A copy of this letter was sent to the Permanent Representations of the Member States, Mr Juan Fernando LÓPEZ AGUILAR, Chair of the LIBE Committee of the European Parliament, and Ms Viviane REDING, Vice-President of the European Commission.

(Complimentary close)

(signed) Peter HUSTINX