EUROPEAN COMMISSION

Brussels, 10.1.2013
C(2012) 9638 final

Mr Winfried KRETSCHMANN
President of the Bundesrat
Leipziger Straße 3 - 4
D – 10117 BERLIN

*Dear President,*

*The Commission would like to thank the German Bundesrat for its Opinions and reasoned Opinions, on the European Commission proposals 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) and 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 {COM(2012) 10 final and COM(2012) 11 final}, and apologizes for the long delay in replying.*

*The Bundesrat expresses the view that neither proposal is compatible with the subsidiarity principle. In addition, the Bundesrat also comments on individual provisions in each of the proposals.*

*The Commission would like to underline that the data protection reform package proposed by the Commission last January aims to build a modern, strong, consistent and comprehensive data protection framework for the European Union. It would benefit individuals by strengthening their fundamental rights and freedoms with respect to processing of personal data and their trust in the digital environment and simplify the legal environment for businesses and the public sector substantially. This is expected to stimulate the development of the digital economy across the EU's Single Market and beyond, in line with the objectives of the Europe 2020 strategy and the Digital Agenda for Europe.*

*The reform would enhance trust among law enforcement authorities in order to facilitate exchanges of data between them and cooperation in the fight against serious crime, while ensuring a high level of protection for individuals.*

*The package also responds to strong calls from the co-legislators, the Council[1] and the European Parliament[2] as well as from various stakeholders for a high quality legal framework based on a comprehensive approach.*

---

1 Council Conclusions on the Communication from the Commission to the European Parliament and the Council - A comprehensive approach on personal data protection in the European Union, 3071st Justice and Home Affairs Council meeting, Brussels, 24 and 25 February 2011.

2 European Parliament Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union P7_TA_(2011)0323.

*The Commission is of the view that both proposals are fully compatible with the subsidiarity principle and would like to set out in the annex to this letter its position in detail on this as well as on the other issues raised in the Bundesrat opinions.*

*The Commission hopes that these explanations serve to clarify the points raised in your Opinions and looks forward to continuing the political dialogue with the Bundesrat in the future.*

*Yours faithfully,*

*Maroš Šefčovič*
*Vice-President*

*ANNEX*

## *I. The proposal for a General Data Protection Regulation {COM(2012) 10 final}*

### *1. The need for a Regulation*

*According to European case-law, the current data protection Directive (95/46/EC of 1995) aims to harmonise data protection law in all Member States, but – as the ECJ has repeatedly made clear - harmonisation of those national laws should be generally complete and therefore not limited to minimal harmonisation (cf. for example, Cases C-101/01, paragraphs 96 et seq., joined cases C-468/10 and 469/10, paragraph 35).*

*Consequently, current legislation already obliges the Member States to adhere to a harmonised level of protection. Experience has shown, however, that transposition of the 1995 Directive into national law and practices in the Member States has, in some cases, produced wide-ranging differences in the interpretation and application of the rules on data protection. There are also significant differences in the position, resources and powers of data protection supervisory authorities, with the result that national data protection legislation adopted in the Member States on the basis of the Directive is being implemented differently. The fragmentation of the legal framework and the application of the law by 27 different data protection systems have created legal uncertainty with no uniform level of protection for citizens.*

*The right to the protection of personal data guaranteed by Article 8 of the Charter of Fundamental Rights and Article 16(1) of the Treaty on the functioning of the European Union (TFEU), however, requires a uniformly high level of protection in all Member States, especially as citizens are increasingly availing themselves of services abroad or having their data processed in other countries. This uniform level of protection can be attained only if a uniform law applies in all Member States and this includes provisions on the transfer of data to third countries and international organisations. Without full harmonisation it is also impossible for the European single market to function properly. If it is left to the Member States to add further conditions to data protection that go beyond the uniformly high level of protection, the different requirements imposed on businesses, depending on the Member State, will generate unnecessary costs and avoidable administrative burdens, which undermine the reform's objective of helping to unleash the potential of the digital single market and foster economic growth, innovation and employment.*

*A Regulation is the instrument best suited to laying down rules on the protection of personal data because its direct applicability remedies the current legal fragmentation, thereby increasing legal certainty and the protection of fundamental rights throughout the European Union and improving the functioning of the single market.*

### *2. Scope of the Regulation*

*As all personal data can be transferred between Member States, the applicability of the Regulation cannot – just as under the current Directive 95/46/EC – depend on whether there is a specific link in the case in question with the free movement of data between the Member States (cf. Cases C-465/00, C-138/01 and C-139/01, paragraphs 40-43). This is why "local data processing" may not be excluded from the scope of the Regulation which extends beyond the processing of data for purely personal or private purposes without any gainful interest (Article 2(2)(d).*

*The proposal for a Regulation continues the tried and tested tradition of the current data protection Directive 95/46/EC by not drawing a distinction between the public and the private sphere. As regards the protection of personal data, neither Article 8 of the Charter of Fundamental Rights nor Article 16(1) TFEU make any distinction between public authorities or other data processors dealing with the data. Moreover, depending on the legal systems in the individual Member States, problems may arise when attempting to separate the public and the private sphere. In accordance with the across-the-board scope of the existing law given and the Commission's aim for the proposed legal instrument to ensure a complete legal framework for data protection in the EU, the proposed Regulation should apply to both the public and the private sphere.*

***3. Room for manoeuvre for national Parliaments***

*The choice of a Regulation would not mean that national Parliaments are denied any room for manoeuvre. As with the current data protection Directive, the proposed Regulation provides that the circumstances under which data processing is lawful include the situation where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority (Article 6(1)(e)). The proposed Regulation also states that the basis of the processing must be provided for in Union law or the law of the Member State to which the controller is subject (Article 6(3)).*

*As data processing by public authorities requires a legal basis that takes account, in particular, of the principle of proportionality, this means for the public sector that specific Member States' laws would still have to define the details of the public interest in data processing, the purposes thereof and the conditions for processing within the framework of the Regulation proposal in specific laws. As the proposed Regulation is confined to providing rules on data protection in specific sectoral legislation, it does not interfere with the general procedural law of the Member States.*

*In particular fields the proposed Regulation also makes express provision for regulation by the Member States, for example, defining the relationship between the processing of personal data and the freedom of expression (Article 80), the processing of personal data concerning health (Article 81) or data processing in the employment context (Article 82). Similarly, other provisions refer to Member States' law with regard, for example, to the processing of particular, sensitive data, the requirement to safeguard personal data (Article 9(2)(g)) or necessary restrictions on the application of specific provisions (Article 21). National law is also still necessary to establish data protection supervisory authorities (Article 46(3)), and the proposed Regulation takes account of federal structures, allowing for more than one supervisory authority to be established in a Member State (Article 46(1)). Within this framework Member States most definitely have the possibility to take account of national, historical or culturally determined characteristics -within the framework of the proposed Regulation.*

***4. Delegated acts***

*Where the proposed Regulation provides for the Commission to lay down more detailed rules by means of delegated acts, this is for the application of specific provisions on the basis of Article 290 TFEU, if and when this is necessary. The powers to adopt delegated acts do not concern any essential element of the proposed legislative act. The key provisions are contained in the proposal, which makes it applicable without any delegated acts needing to be adopted beforehand.*

*The alternative, laying down detailed rules on the application of the individual provisions in specific sectors and situations in the proposal, would result in an inflexible and unwieldy legal text which would not be open to innovation and new technologies and would also restrict scope for finding common approaches in the European Data Protection Board.*

***5. The consistency mechanism and the independence of the data protection supervisory authorities***

*The proposed Regulation strengthens the independence and powers of the supervisory authorities in accordance with ECJ rulings (Article 46 et seq.). The consistency mechanism does not give the Commission the possibility to influence the independent data protection supervisory authorities in the Member States; it is intended to foster consensus among data protection supervisory bodies in the European Data Protection Board and leaves decisions on specific cases and implementation in principle to the appropriate national data protection authority. Not only is every member independent, the European Data Protection Board is also independent in the performance of its duties (Article 65(1)).*

***6. Adapting national law, particularly with regard to electronic communications services***

*Article 88(2) of the proposed Regulation, which deems references to Directive 95/46/EC – which would be repealed under Article 88(1) – to be references to the proposed Regulation does not relate just to Directive 2002/58/EC; it also concerns any reference to the provisions of the current data protection Directive.*

*As Article 89 of the proposed Regulation makes clear, the proposal does not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union, in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC. In most cases, the proposal provides for a two-year period of transition for the amendment of national law (Article 91(2)).*

***7. Delineation between the two legal instruments***

*In contrast to the proposal on General Data Protection Regulation, the proposed Directive is a specific legal instrument 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 by the authorities responsible (Article 1(1), Article 2(2) of the proposed Directive; Article 2(2)(e) of the proposed Regulation). Where the authorities responsible have tasks other than processing data for the purposes of the Directive, the Regulation applies. This does not create any fundamentally new situation, as any given authority and any official are currently already subject to completely different data protection laws, for example, a police officer who is responsible for police checks at an external border and also for immigration control, whereby the latter is covered by Directive 95/46/EC. However, the difference with regard to the current legal situation is that the proposed Directive is part of a complete legal framework, with two legal instruments pursuing the twin objectives of safeguarding fundamental rights and the free movement of data on the basis of the uniform data protection principles.*

## *II. The proposal for a police and criminal justice Directive {COM(2012) 11 final}*

### *1. Legal basis for the Directive*

*As the Directive is intended to harmonise the Member States' data protection rules in the field of police and criminal justice, the proposed Directive does not distinguish between cross-border exchanges of data and national data processing by the competent authorities. In this respect the proposed Directive follows the same approach as Directive 95/46/EC and the proposed Data Protection Regulation, the provisions of which equally do not differentiate between national data processing and cross-border data processing.*

*As in the case of the proposal for a Regulation, the legal basis for this is Article 16(2) TFEU, which requires the legislator to lay down comprehensive provisions on the protection of individuals when personal data is processed and the free movement of data in the European Union. Neither this requirement nor the protection of the individual, which is guaranteed by Article 8 of the Fundamental Charter of Human Rights and Article 16(1) TFEU, is restricted to data processing with cross-border implications. This is also in keeping with ECJ case law, which holds that application of Directive 95/46/EC cannot presuppose the existence of an actual link with free movement between Member States (cf. Cases C-465/00, C-138/01 and C-139/01, paragraphs 40-43).*

*As all personal data can be transmitted between the Member States – as some Member States confirmed during the Commission consultation – the distinction between national and cross-border data processing may even create practical problems for the authorities concerned, for example, where there is a need to distinguish between data of differing provenance in investigative proceedings so that different rules can be applied when processing said data. Furthermore, in practice there is in any event unlikely to be a clear line separating personal data gathered in a country and data that may also be exchanged between countries.*

*The Directive proposal concerns the protection requirements regarding data processing by the competent authorities in the field of application set out in Article 2 in conjunction with Article 1(1), but does not impinge upon the powers of Member States in criminal proceedings or police law or for maintaining public order or safeguarding domestic security. This is why there is no need for recourse to special Treaty provisions on police and judicial cooperation in criminal matters beyond the general legal basis for data protection legislation contained in Article 16(2) TFEU. Therefore the proposal does not affect Article 72 TFEU. It equally does not apply to data processing by competent authorities in relation to other duties not within the scope of the proposed Directive.*

### *2. Compatibility with the subsidiarity principle*

*When preparing its proposals, the European Commission attached particular attention to the subsidiarity principle and conducted a detailed analysis of aspects related thereto, basing itself not just on individual studies, but also on in-depth consultation with the parties concerned, in particular, by holding hearings with representatives of law-enforcement authorities in addition to the two public consultations in 2009 and 2010/2011. On 29 June 2010 a workshop was held involving the Member States' authorities on the application of the data protection rules in public offices, which also involved police and judicial cooperation in criminal matters. On 2 February 2011 the Commission organised a workshop with the Member States' authorities to discuss*

*implementation of Framework Decision 2008/977/JI and, more generally, data protection issues in the context of police and judicial cooperation in criminal matters.*

*The subsidiarity evaluation revealed that – in addition to the uniform level of data protection required under Article 8 of the Charter of Fundamental Rights and Article 16(1) TFEU – measures on police and criminal justice matters are needed at EU level for the following reasons:*

*Law-enforcement bodies in the Member States have an ever-increasing need for ever-faster data processing and exchanges of data to prevent and combat crime and terrorism, which do not stop at national borders. Uniform and clear rules on data protection at EU level would help enhance cooperation between these authorities.*

*The practical difficulties involved in implementing data protection rules and the necessary cooperation between the Member States and their authorities make organisation at EU level necessary to ensure uniform implementation of European Union law. In certain situations the EU is best-placed to ensure that when personal data are communicated to third countries all concerned are effectively and equally protected.*

*Alone, the Member States cannot overcome the existing problems, especially those caused by the lack of uniformity of national laws. There is therefore a particular need for a harmonised and consistent system which makes possible the smooth transfer of personal data within the EU while guaranteeing all concerned effective data protection throughout the EU.*

*The nature and extent of the problems, which are not confined to one or several Member States, would make a Directive on data protection in this field overall more effective than comparable measures at Member State level.*

***3. Member States' existing international agreements***

*The obligation on Member States to examine and, where necessary (i.e. if the agreement is not compatible with the provisions of the Directive) to amend international agreements they concluded prior to the entry into force of this proposed Directive (Article 60), is necessary to ensure uniformity of data protection throughout the EU in accordance with it. Otherwise there would be a danger that data is transferred to third countries which do not guarantee adequate data protection, undermining the level of protection guaranteed by the Directive proposal and thereby also the mutual trust between the Member States on which the proposal's provisions on the transfer of data to third countries or international organisations is based (Articles 33-38). As an integral part of European Union law, the standards contained in the Directive proposal must take priority over measures adopted by Member States, including agreements concluded earlier. Amending existing agreements is part of the duty incumbent on Member States to take all measures necessary to meet obligations arising out of the Treaties or acts by the EU institutions (Article 4(3) of the Treaty on European Union). Article 351 TFEU relates to international agreements concluded prior to the date mentioned in the first paragraph of this provision.*

*Only agreements concerning the exchange of data which are not compatible with the Directive will have to be amended. The time allowed for amendments – five years following the entry into force of the proposed Directive – is also significantly longer than the time allowed for implementation of the Directive, which is two years (Article 62(1)).*

### *4. Data Protection Officers*

*The provisions on data protection officers in the Directive proposal are confined to requiring officers to be designated (Article 30), their position (Article 31) and core tasks (Article 32). These elements are necessary to describe the function of data protection officers. However, Member States continue to have the right to determine the structure of the authority (cf. Article 30(3)) and, as can be seen from the words "at least" in Article 32, may entrust data protection officers with other tasks.*