

30.03.12

**Decision**Of the Bundesrat

---

**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.**

**COM(2012) 10 final; Council document 5833/12**

In its 895th session on 30th March 2012, the Bundesrat adopted the following Decision pursuant to Article 12, Point b, TEU:

1. The Bundesrat welcomes the draft Directive's objective of facilitating police and judicial cooperation in criminal matters whilst respecting the fundamental right to the protection of personal data.
2. Submission of a reasoned opinion on non-compliance with the subsidiarity principle pursuant to Article 12, Point b, TEU also encompasses the question of EU competence – see the Bundesrat Opinions of 9th November 2007, BR Official Document 390/07 (Decision), Point 5, of 26th March 2010, BR Official Document 43/10 (Decision), Point 2 and of 16th December 2011, BR Official Document 646/11 (Decision). The subsidiarity principle concerns principles pertaining to the exercise of competences. The subsidiarity principle is also violated if the European Union is not competent to adopt legislation in the area in question. For that reason the question of the legal basis must first be addressed when scrutinising compliance with the subsidiarity principle.
3. The proposal for a directive on the protection of individuals with regard to the processing of personal data for the purposes of prevention, investigation detection or prosecution of criminal offences cannot take Article 12, Sub-section 2, TFEU as its legal basis in as much as the scope of the directive also

encompasses data processing in domestic proceedings. The Commission proposal is therefore not covered by the legal basis stipulated (Article 16, Sub-section 2, TFEU) insofar as the proposal encompasses purely national exchanges of information by police authorities. Pursuant to the principle of conferral enshrined in Article 5, Sub-section 2, TEU, the EU may only take action within the limits of the competences transferred to the EU in the Treaties in order to attain the objectives stipulated therein. Article 16, Sub-section 2, TFEU only authorises the EU to adopt provisions on protection of individuals in respect of processing of personal data by the Member States in the course of activities that fall within the scope of application of European Union law. However, domestic criminal law procedures only fall within the scope of application of European Union law to a limited extent. The restricted competences of the EU to adopt directives on criminal law matters (Article 82, Sub-section 2, TFEU) therefore also limit the data-protection competence of the EU in this policy area. This constitutes an impediment to harmonisation of purely domestic data processing in criminal procedures. Processing of personal data is a decisive component of criminal law procedures. The draft directive would therefore lead to far-reaching encroachments on criminal procedural law, which are not necessary in order to facilitate mutual recognition of decisions and cooperation in criminal matters with a cross-border dimension. For example, the draft directive comprises provisions with comprehensive stipulations for the Member States on how to organise files pertaining to criminal proceedings (Article 5 and 6), on investigative measures deploying particular categories of personal data (Article 8) and on access to files and provision of information (Article 11 to 14).

The substantiation for the proposed directive states with reference to the inclusion of purely national data processing that the competent authorities would not be able to distinguish readily between national data processing and cross-border exchange of personal data or to foresee whether certain personal data would subsequently be involved in cross-border data exchanges. This however does not provide a justification for the broad scope of application envisaged for the directive.

Competent authorities are readily able to appraise cross-border transfers of data applying the provisions pertaining to such data transfers for data collected prior to such transfers in keeping with the provisions of national criminal procedural

law Should there be legal shortcomings in data transfer in the context of judicial and police cooperation, these sector-specific provisions could be revised. The Commission's assumption that practical difficulties exist in drawing a legal distinction between national data processing and cross-border exchange of personal data does not however constitute a justification for extending its existing competences. These comments apply *mutatis mutandis* to processing of personal data in the realm of police law.

4. The framework competences stipulated in Article 16, Sub-section 2, TFEU ("Scope of application of European Union Law") are rendered more specific by Article 87 TFEU in respect of the police authorities pursuant to Article 2, Sub-section 6, TFEU. Article 87, TFEU encompasses only cooperation between Member States' police and judicial authorities. Article 87, Sub-section 1, TFEU therefore does not confer competences to adopt provisions governing matters that pertain exclusively to the activities of these authorities within a Member State and that hence do not relate to any form of cooperation between the Member States. The scope of the empowerment to adopt provisions regarding exchange of information by the police stipulated in Article 87, Sub-section 2, Letter a, TFEU corresponds through the reference to the objectives of Article 87, Sub-section 1 to the stipulation in this article that the sphere of competence in question concerns cooperation between Member States' authorities. Consequently, in terms of data protection too, data transfers by the police are only subject to EU competence to adopt provisions with regard to cooperation between Member States' law enforcement agencies.

In addition, pursuant to Article 51 of the EU Charter of Fundamental Rights, Article 8 of the Charter encompasses Member States' activities only inasmuch as these implement European Union law; an extension of competences as a consequence of application of the Charter is also excluded pursuant to Article 51, Sub-section 2 of the Charter. By interpreting Article 8 of the Charter and Article 16, Sub-section 2, TFEU without taking into account the particularities of the provisions on the Area of Freedom, Justice and Security, the proposed directive constitutes an interpretation of primary law that extends the provisions therein to such an extent that it gives rise to a constitutionally significant conflict between the principle of conferral and the constitutionally enshrined responsibility of individual Member States for integration, with ramifications for practical measures to guarantee security and public order; this is the type of

conflict identified in a ruling by the German Federal Constitutional Court of 30th June 2009 (Reference.: 2 BvE 2/08 inter alia). The formulaic wording of Article 2, Sub-section 3, Letter a of the proposed directive does not avoid this extension of substantive competences, which is particularly detrimental to the sovereignty of the federal states (*Länder*) in matters pertaining to the police.

5. The Bundesrat also takes the view that the EU is not competent to adopt provisions on non-crime-related security law. Here too there are grounds for concern: unless clarification is introduced exempting competence for data protection pursuant to Article 16, TFEU, there is a risk of the EU extending the scope of its competences and applying provisions to a wider range of subject matters to the detriment of Member States' competences for non-crime-related security measures in the sense of the German Federal Constitutional Court ruling of 30th June 2009 (Reference.: 2 BvE 2/08 inter alia). The formulaic wording of Article 2, Sub-section 3, Letter a of the proposed directive does not suffice to avert the transfer of competences inherent in the individual provisions of the directive.
6. The proposed directive also violates the subsidiarity principle in the strict sense of the term as enshrined in Article 5, Sub-section 3, TEU, in as much as the proposal comprises provisions on purely domestic data collection and processing. Consequently it is not possible to identify any European added-value arising from the envisaged uniform provisions across Europe. On the contrary, the Member States can introduce adequate provisions on purely national data protection (collection, storing and transfer of data) and indeed sufficient provisions governing this area already exist in German law in the form of the legislation on data protection currently in force.<sup>7</sup>The principles derived from primary law provisions apply equally in all Member States. These principles are enforced by the European Court of Justice, which, pursuant to Article 19, Sub-section 1, Sentence 2, TEU, has the role of ensuring that the law is observed in the interpretation and application of the Treaties.
7. The substantiation pertaining to the inclusion of purely national police information transfers and compatibility of this with the subsidiarity principle also violates the provisions to be respected by the Commission laid out in Article 5 of Protocol 2 to the Lisbon Treaty, which are binding for the Commission pursuant to Article 51 TEU. The comments in the substantiation in

Point 3.2 of the draft directive assert only that the directive complies with the subsidiarity principle without providing the requisite quantitative and qualitative information as stipulated in Article 5 of the Protocol. The Commission Working Paper (SEC (2012) 73) refers on page 3 only to the speculative assumption that exchange of information between competent authorities in the Member States is impeded. However, as the impact assessment document (SEC (2012) 72) indicates on page 34, Letter d, this assumption is based solely on the appraisal of a study which has not been made public by a migration policy institute. In respect of this study by an institute that does not work directly in the relevant field, the basis taken for its comments cannot be verified and is not comprehensible, and hence this study does not constitute a suitable foundation for this kind of appraisal. Further comprehensible information on this point is not provided.

8. The provisions also impinge upon the areas granted specific protection pursuant to Article 72, TFEU. Article 72, TFEU comprises provisions on the police authorities and supplements Article 5, Sub-section 3, TEU. The particularly intensive scrutiny to determine whether interventions in this field are necessary, as stipulated in Article 72, TFEU, is not apparent either in the proposed Directive or in the accompanying working documents. The envisaged restrictions to be placed on purely national information transfers by the police, as well as the option envisaged in Article 27 of the proposed Directive of introducing binding provisions utilising national information technology procedures and systems, which would determine whether such procedures and systems are admissible from a data protection perspective, would impinge upon the responsibility and ability of the police to fulfil its duty to guarantee domestic security and public order, activities which are protected pursuant to Article 72 TFEU. If certain procedures and systems are declared inadmissible from the perspective of data protection legislation, it would no longer be permitted to deploy such procedures and systems, which would give rise to enormous operational constraints on the police in exercising its duties.
9. The obligation in Article 60 of the proposed Directive to alter existing bilateral or multilateral agreements between police forces would impinge on the provisions of the Vienna Convention on the Law of Treaties and on Member States' foreign policy competences. Article 351, TFEU envisages only that the Member States shall use all appropriate means to overcome possible

incompatibilities between treaties that have already been concluded and the EU treaties. The Bundesrat therefore takes a critical view of the rigid wording of Article 60 of the draft Directive. Consideration should be given to recasting this article as a “sunset-clause”.

10. It has not been demonstrated that the Member States would not be able to ensure a sufficient level of data protection within police and judicial authorities by developing descriptions of the tasks and activities of Data Protection Officers in these authorities. In addition the draft Directive does not demonstrate that the number and complexity of provisions comprised in Article 30 ff. of the draft Directive would provide a better means of ensuring data protection in police and judicial authorities than national provisions, which in some cases are already in force; this constitutes a further violation of the subsidiarity principle.
11. Furthermore the Bundesrat also draws attention to its Opinion on the Commission Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A comprehensive approach on data protection in the European Union, COM (2010) 609 final; BR Official Document 707/10 (Decision), Point 8.