Brandenburg State Commissioner for Data Protection and Access to Information
Ms Dagmar Hartge

Chairwoman of the Conference of the German Data Protection Commissioners of the Federation and of the Länder 2012

Comments

made by the Conference of the German Data Protection Commissioners of the Federation and of the Länder

of 11 June 2012

concerning the Directive 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 of 25 January 2012

Regardless of whether the competence of the EU to adopt Directives on the basis of Article 16 (2), first sentence of the TFEU concerning the principle of conferral and the subsidiarity principle also applies to purely domestic data processing activities in the fields of threat prevention, criminal prosecution and the execution of criminal penalties, the Conference of the Data Protection Commissioners of the Federation and the Länder (Conference) wishes to submit the following assessment of the proposed Directive:

Purpose of the Directive

The Directive should stipulate the highest possible level of data protection for Member States through minimum standards. Member States should continue to be in a position to provide, in their national law, for stricter privacy rules than those contained in the Directive - a general approach to be stipulated in the Directive itself.

Such a clarification would uphold the data protection principles that have emerged from rulings handed down by the Federal Constitutional Court (Bundesverfassungs-gericht, BVerfG) (e.g. rulings concerning the core area of the private sphere). Also, it would put the national constitutional courts in a position to further develop the protection of fundamental rights together with the European Court of Justice.

If this approach is not stipulated in the Directive itself, national regulations to uphold fundamental rights might be considered in breach of the Directive owing to what the Directive requires (e.g. guaranteeing data protection and the exchange of data within the Union in line with Article 1 (2) (b) with the aim of achieving full harmonization). Against the backdrop of the rulings handed down by the European Court of Justice in cases related to the existing Data Protection Directive 95/46/EC, this interpretation cannot be ruled out and would have intolerable effects, e.g. with regard to the procedural safeguards for the rights of data subjects contained in the law governing criminal procedures and the police.

Specifically:

Chapter I - General provisions

Scope (Articles 1-2)

According to Article 2 (1) the Directive is only applicable in cases where a "competent authority" processes personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This does not cover threat prevention tasks which are not related to criminal offences (e.g.: search for missing persons who are not involved in a criminal offence or are

below the age of criminal responsibility). It is likely that Member States will have different views of whether other tasks which come under border or customs controls or concern the residence or immigration law and may or may not be considered police tasks depending on the tradition of the Member States, also fall under the scope of the Directive. We hold the view that a situation should be avoided where one and the same police task is considered to come under the Regulation in one Member State and under the Directive in another one. The envisaged scope of the General Data Protection Regulation and that of the Directive mean that the German police authorities would have to apply both legal acts for their current tasks. Delimitation problems in terms of what legal act to apply are not new to the German authorities mandated with police tasks, as illustrated by the customs administration and customs investigation authorities. The Conference holds the view that future delimitation problems should however be averted by ensuring the greatest possible consistency between the General Data Protection Regulation and the Directive.

The proposed legal act makes minimum requirements also applicable to domestic data processing by the police and law enforcement authorities - a demand already raised by the Conference a number of years ago. A high data protection level needs to be ensured in all Member States, as the principle of availability - according to which data collected and processed in one Member State should also be made accessible to the police and law enforcement authorities in another Member State - has increasingly been realized (Swedish Initiative, Prüm Treaty, etc.).

Article 2 (2) defines the scope with regard to the circumstances of processing (automated/non-automated). The Conference wishes to point out that the Proposal - in particular the German version - does not make it clear whether (paper-based) files should also come under its scope. Ultimately, the Directive should apply to the collection and processing of all personal data regardless of the means by which they are processed. A distinction between automated or non-automated processing on the one hand and processing in (paper-based) filing systems does not seem to be appropriate. This should be clarified.

Article 2 (3) (a) provides that the Directive is not meant to apply to the processing of personal data in the course of an activity which falls outside the scope of Union law,

in particular concerning "national security". We think that the term "national security" needs to be defined more clearly.

The proposed Directive also exempts the Union bodies and institutions (e.g. Europol) from the scope of application - an approach we do not deem appropriate as these bodies, too, should be included in the efforts to raise data protection levels, no matter which legal instrument should ultimately be applicable to them. If one of the aims of overhauling the data protection legislation within the EU is to create a comprehensive legal framework entailing a high level of data protection, then this framework should also apply to the EU institutions. We understand that it is difficult to overhaul the complex legislative acts of the former Third Pillar in just one legal package. Great care must be taken, however, to ensure that the standards applicable for the EU institutions do not differ from those for the police and judicial authorities of the Member States. We therefore suggest that the time period for amending existing international agreements should be shorter than the period laid down in Article 60. The legislators should check, at any rate, whether the standards of the Directive which are to be declared the minimum level for all Member States could also be declared the minimum standard for all existing EU institutions.

Definitions (Article 3):

We should like to point out the following with regard to the definitions:

The definition of a "child" in Article 3 (13) should be deleted, because no specific processing rules or procedural guarantees are related to this concept.

For the term "threat to public security" a definition should be included with regard to Article 7 (d).

The definition of "restriction of processing" in Article 3 (4) should be amended with regard to the provision in Article 16 (3).

Chapter II - Principles

Principles relating to personal data processing (Article 4)

Strict requirements concerning necessity, purpose limitation and data minimisation, among other things, form the main basis for the effective protection of personal data. We hold the view that the data processing principles laid down in Article 4 need to be specified and put more precisely. Generally speaking, they should be more consistent with the principles proposed in Article 5 of the General Data Protection Regulation.

Article 4 (b) - the provision on purpose limitation - is worded in a very open manner with regard to further processing for other uses ("in a way incompatible with those purposes"). This provision should be worded in a stricter manner, especially in view of the unclear and open provision contained in Article 7 regarding the lawfulness of processing. It should be clarified that Article 4 - read together with Article 7 - must not be construed to mean that data collected under the scope of the Directive for a given purpose may be further processed for any other purpose also covered by the Directive without further legal prerequisites.

Furthermore, the principle of necessity in Article 4 (c) should be defined more strictly. In our view, the adjectives "adequate, relevant, and not excessive" are too weak to delimit the lawfulness of data processing. This is particularly true as the proposed Directive does not limit data processing to the minimum necessary in relation to the purposes for which they are processed, as stipulated in Article 5 (c) of the General Data Protection Regulation. Data minimisation is not mentioned as a principle. Rather, the impression is created that the principle of necessity amounts to hardly more than the ban on excessive data processing.

Another principle should be listed requiring those processing personal data to invariably comply with the technical and organizational data protection measures.

From a purely linguistic point of view, the German translation of Article 4 (a) should also read "Fairness" or "faires Verhalten" instead of "nach Treu und Glauben".

Distinctions between categories of data subjects, accuracy and reliability of personal data (Articles 5 and 6)

The proposed Directive requires Member States, when processing personal data, to make distinctions, as far as possible, between different categories of data subjects (suspects, persons convicted of a criminal offence, victims, witnesses etc., Article 5) as well as with regard to the accuracy and reliability of data (Article 6). Under German law, other criteria are relevant which are not provided for in the Proposal, for instance the criterion of whether such processing would infringe on the core area of the data subject's private sphere or whether the data result from particularly severe infringements of the data subject's fundamental rights (secrecy of telecommunications, privacy of the home). In order to uphold the current and constitutionally indispensable level of protection the Directive should stipulate minimum standards for domestic regulations and not upper limits.

Articles 5 and 6 fail to set out the purpose of the distinctions to be made, and what is supposed to happen if Member States fail to make such distinctions. The Conference is in favour of stricter limitations on the processing of data relating to particular groups of persons (e.g. witnesses or victims of crimes).

Lawfulness of processing (Article 7)

Article 7 is pivotal in requiring Member States to provide for the lawfulness of data processing. We hold the view that the distinctions made between lit. a), b), c) and d) need to be explained further.

It is also necessary to explain how this provision is to be read together with the principles of data processing under Article 4, in particular the one on purpose limitation.

We welcome the fact that the consent of the data subject may not legitimize data processing under the scope of the Directive. The Conference has repeatedly questioned the approach under which the data subject's consent is used as the basis

for legitimizing data processing, especially if it serves to expand the limits of legal powers.

Chapter III – Rights of the data subject

Rights of the data subject (Articles 10-17)

A high level of data protection requires that data subjects have comprehensive rights. For the proposed Directive to serve as a suitable basis for expanding the rights of data subjects within the Union, several provisions need to be clarified or amended.

This is particularly true for Article 17 read together with Recital 82. In our view it is unclear when to apply Article 17 and what its effects would be. The interpretation of this Article is made even more difficult as the German and the English versions („Gerichtsbeschluss oder einem Gerichtsdokument“ / „judicial decision or record“) may be construed to have different meanings. It is particularly important to clarify this issue as it is key to whether and to what extent the rights of data subjects apply throughout criminal investigations.

We hold the view that the rights conferred by Articles 11-16 should generally also apply during criminal investigations and proceedings. Minimum standards with regard to data subjects' rights are among the key elements of a high level of data protection and must also apply to the processing of personal data during criminal investigations and proceedings.

Furthermore, it is too easy for Member States to restrict the rights of data subjects. We object to the provisions in Article 11 (5) and Article 13 (2), because they enable legislators to exempt certain categories of data from the provision of information to the data subject without having to weigh the interests in the individual case. Rather, Articles 11 and 13 should clarify that restrictions are invariably permissible only after the examination of the specific case.

We understand why the provision of information to the data subject or his or her access to information needs to be restricted (at first) in specific cases. However, these restrictions need to be defined in a sufficiently precise manner. That is why Article 11 (4) and Article 13 (1) again raise questions, as they leave the national legislators too much leeway to restrict the rights of the data subjects.

Also, data subjects should be informed promptly of any collection of personal data (i.e. without undue delay). This means that requiring the provision of information "within a reasonable period", as stated in Article 11 (3) (b) is not precise enough.

It should be clarified whether a correction is meant by the term "corrective statement" (in German: "Korrigendum") used in Article 15.

Additionally, the Draft Directive should be amended so as to also grant data subjects the right to access to files in suitable cases, on top of the right to information.

Chapter IV - Controller and processor

Provisions governing controllers and processors (Articles 18-32)

The Conference regrets that the provision on "data protection by design" in Article 19 fails to stipulate concrete requirements, which means that it could have little or no practical effect. Furthermore, the explicit reference to the cost of implementation could be used by controllers to justify their failure to implement data protection by design or default.

Some of the provisions in Chapter IV need further clarification, for instance the relation of the "independent internal or external auditors" to the data protection officer and the supervisory authorities in line with Article 18 (3), and the contents of Article 20 and 22 (e.g. the control obligations of the processor) and the relationship of Articles 20 and 21.

Further documentation obligations should be added in Article 23 (2), namely the description of the groups of persons concerned and of the relevant data or data categories, and a definition of time limits for erasure.

The provisions pertaining to data security (Articles 27-29) should be amended to include the data protection goals.
Risk evaluations under Article 27 (2) can be considered an adequate security measure only if the risk is constantly assessed or analysed. This means that IT security requires a general strategy and the establishment of IT security and data protection management systems. Article 27 should therefore be amended to include a requirement for a security concept, which would have to be part of the documentation of procedures in line with Article 23 (2).

The delegation of power to the Commission contained in Article 28 (5) needs to be looked at. The criteria and requirements for the establishment of a personal data breach are so essential that they should be laid down in the legal instrument itself.

The obligation to inform the data subject of a personal data breach should not depend on whether the controller has taken sufficient technical protection measures, as set out in Article 29 (3).

The obligations of controllers and processors should include not only "prior consultation" of the supervisory authorities but also a "privacy impact assessment", as in the General Data Protection Regulation.

"Reliability" should be included in the requirements for data protection officers (Article 30 (2)). Also, the data protection officer should be required not to disclose information. Furthermore it should be added that data protection officers must not be discriminated against or terminated, and that they must be allowed to participate in training measures.

Article 32 should also make clear that the tasks of the data protection officer do not mean that the controller may exculpate himself on the allegation that the data

protection officer failed to discharge his task (satisfactorily). Articles 32 a), d) and h) are especially misleading here.

Chapter V - Transfer of personal data to third countries or international organisations

Generally speaking, the provisions governing the transfer of personal data to third countries are too broadly defined. Also, they are contradictory in one crucial point.

As regards the transfer of personal data to international organisations, Article 33 should clarify that this provision applies only to international organisations dealing with internal security issues. The same applies to what is called "onward transfers", which should be regulated in a specific provision.

What we find lacking is a clarification that existing adequacy decisions taken on the basis of Directive 95/46/EC are not applicable to the JHA area.

The proposed Directive provides for the introduction of adequacy decisions regarding the data protection level of third countries in line with the provisions of Directive 95/46/EC. Any decision by the Commission to that effect means that the adequacy of the data protection level has been established in a binding manner. It must be clarified, though, that, if the Commission has found the data protection level to be inadequate in line with Article 34 (5), data may only be transferred on the basis of the derogations listed in Article 36, but not on the basis of Article 35 (1). Article 34 (5) and Article 35 (1) contradict one another in this respect.

Article 35 (1) (b) allows Member States to transfer personal data to third countries following their own assessments - a provision which is not concrete enough. Reference should at least be made to Article 34 (2) (a), which lists the factors to be taken into account when making the adequacy decision. Also, the processor should not be mentioned in Article 35.

In our view, Article 36 is put far too broadly, in particular d) and e). It is hard to think of any transfer which could not be based on these derogations. With the derogations of a) to e) in mind, we therefore suggest deleting d) and e). Furthermore, controllers should be required to document transfers as in Article 35 (2).

Article 37 refers to the transfer to third countries of personal data subject to specific domestic restrictions on the use of data. It therefore requires controllers to "take all reasonable steps" to ensure compliance with these restrictions. We hold the view that this provision is too vague and should be put more precisely, in particular with regard to the technical and organizational measures to be taken. Member States should also be required to provide that recipients must be informed of any correction or erasure entitlement.

Article 37 does not apply to transfers within the Union. Therefore the Directive must make it clear, in a suitable provision, that the domestic restrictions on use and the notification requirements also apply to data transfers within the Union. To this end, the Directive should require the receiving Member States to implement the restrictions on use in place in the transferring Member State.

Finally, Article 38 should be amended to the effect that not only the Commission but also the supervisory authorities may promote the relations to third countries, in particular to third countries with an inadequate protection level.

Chapter VI and VII - Independent supervisory authorities and co-operation

We generally welcome the provisions on independence. Nevertheless, Article 39 (1), second sentence, should clarify that such independence also needs to be ensured with regard to the co-operation with the Commission and with the other supervisory authorities.

One major issue in the field of police and justice is the competence of data protection authorities when it comes to data processing by the courts acting in their judicial capacity. The wording of Article 44 (2) should make it very clear that the supervisory

authority remain competent to supervise activities of the executive even if these activities according to national law were subject to a judge's authorization (in Germany that would for instance be measures taken by the criminal prosecution authorities subject to a judge's authorization).

Article 45 (4) should make clear that the use of a complaint submission form is not mandatory, and that technical safeguards within the meaning of Article 27 need to be taken.

The Conference welcomes the fact that Article 46, in particular lit. b), allows the German supervisory authorities to continue to make use of their powers in such a way as they currently do, without excluding future changes in law (e.g. their power to impose orders). The powers of the supervisory authorities are a major concern as it is closely related to the possibilities of court action between the supervisory authority and the entity under supervision and/or the data subject (cf. Article 51).

So as to remove any doubts that may result from the comparison with the General Data Protection Regulation, it should also be made very clear in the Directive that Article 46 also includes access to official premises without a reasonable suspicion of malpractice.

Finally it must be ensured that sufficient means are set aside to facilitate practical work as part of mutual assistance (in particular with regard to translations, carried out by the Secretariat of the Data Protection Board, where appropriate). The obligation to provide mutual assistance in line with Article 48 should be amended to include exceptional provisions, for instance governing the protection of secrecy.

Chapter VIII - Remedies, liability and sanctions

We generally welcome the extended power of bodies, organisations and associations to act on behalf of one or more data subjects in line with Article 50 (2).

Article 51 (1) should clarify that judicial remedies may only be lodged against those decisions by the supervisory authority which have an administrative effect (“Regelungswirkung”) on citizens and other authorities under national law.

Article 51 (2) should be amended to the effect that the judicial remedy against the supervisory authority is restricted to its failure to act. The phrase "in the absence of a decision which is necessary to protect their rights" is unclear and should therefore be deleted.

The provision governing common rules for court proceedings (Article 53 (2)) states that each supervisory authority shall have the right to bring an action to court, in order to enforce the rights enshrined in the Directive. The Conference is in favour of amending this provision to the effect that Member States may provide such entitlement of the supervisory authorities but are not required to.

We welcome the introduction, in Article 54 (2), of the joint and several liability of all bodies involved in the processing of data.

Chapters IX and X - Delegated acts and implementing provisions, final provisions

The Conference welcomes the fact that international agreements adopted by the Member States prior to the entry into force of the Directive are to be amended within a period of five years to bring them into line with the new provisions (Article 60). It should be made clear that the Directive sets only minimum standards and that existing standards need by no means be lowered. So far, the Directive is not supposed to apply to EU institutions. This must, however, not lead to a situation where agreements concluded by the EU and third countries (such as the TFTP Agreement or the PNR Agreement) are excluded from the new provisions.

We think that a more substantial provision than the current one in Article 61 (3) should be included in order to evaluate the Directive. The evaluation clause should also include the consultation of external experts.