RAT DER EUROPÄISCHEN UNION

Brüssel, den 6 Dezember 2012

16497/12
ADD 1

LIMITE

DATAPROTECT 131
JAI 817
DAPIX 144
FREMP 140
COMIX 651
CODEC 2738

Interinstitutionelles Dossier: 2012/0010 (COD)

ADDENDUM ZUM VERMERK

der	Deutschen Delegation
für	Delegations
Nr. Komm. dok.:	5833/12 DATAPROTECT 6 JAI 41 DAPIX 9 FREMP 8 COMIX 59 CODEC 217 + ADD 1 + ADD 2
Betr.:	Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr

Die Delegationen erhalten in der Anlage die Kommentare der deutschen Delegation.

ANNEX

Zusammenfassende Stellungnahme
der Bundesrepublik Deutschland zu den Artikeln 1 bis 8

des Vorschlags für eine

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr

1. Deutschland begrüßt, dass die Kommission mit dem Richtlinienentwurf eine Diskussion zur Verbesserung des Datenschutzes und des Informationsaustauschs im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen anstößt. Der Entwurf begegnet aber sowohl in grundsätzlicher Hinsicht als auch mit Blick auf einzelne Vorschriften noch erheblichen fachlichen Bedenken. Aus deutscher Sicht ist er nicht geeignet, zur Verbesserung des Datenschutzes und des Informationsaustauschs beizutragen.

   Insbesondere hinsichtlich der Datenübermittlung zwischen den Mitgliedstaaten stellt sich die Frage nach einem Mehrwert des Entwurfs gegenüber dem geltenden Rahmenbeschluss 2008/977/JI [*Council Framework Decision 2008/977/JHA*]. Der Rahmenbeschluss ist nach umfassenden Beratungen erst am 20. Januar 2009 in Kraft getreten und bis heute noch nicht in allen Mitgliedstaaten umgesetzt. Solange er nicht hinreichend erprobt und der Nachweis seiner Unzulänglichkeit nicht geführt ist, erscheint es aus deutscher Sicht nicht angebracht, neue datenschutzrechtliche Regelungen entwickeln zu wollen. Dies gilt umso mehr, als der Richtlinienentwurf in einigen wesentlichen Punkten hinter dem geltenden Rahmenbeschluss zurückbleibt.

Der Gedanke eines einheitlichen hohen Datenschutzniveaus ist zwar grundsätzlich zu begrüßen. Die vom Richtlinienentwurf angestrebte innerstaatliche Harmonisierung des polizeilichen und justiziellen Datenschutzrechts dürfte jedoch angesichts der inhaltlichen Nähe zum Polizei- und Strafprozessrecht sehr schwierig werden. Das Polizei- und Strafprozessrecht unterscheidet sich in den Mitgliedstaaten erheblich. Seine Harmonisierung ist politisch nicht gewollt und wäre europarechtlich auch nicht möglich. Mit Blick auf den Richtlinienentwurf führt das zu einem Dilemma: Einerseits besteht die Gefahr, dass über die intendierte Vereinheitlichung des innerstaatlichen Datenschutzes hinaus eine schleichende Harmonisierung des Polizei- und Strafprozessrechts stattfindet, die weder gewollt noch zulässig wäre. Hier wird sorgfältig darauf zu achten sein, dass diese Grenze nicht überschritten wird. Andererseits erscheint zweifelhaft, wie angesichts der heterogenen Ausgestaltung des Polizei- und Strafprozessrechts in den Mitgliedstaaten die von der Kommission angestrebte datenschutzrechtliche Harmonisierung gelingen soll. Dass sich aus diesem Nebeneinander von Datenschutzrecht einerseits und Polizei- und Strafprozessrecht andererseits erhebliche praktische Schwierigkeiten ergeben können, verdeutlicht zum Beispiel Artikel 7 des Richtlinienentwurfs, der zur Beurteilung der Rechtmäßigkeit von Datenerhebungen nahezu ausschließlich an die nationalen, sehr heterogen ausgestalteten fachlichen Aufgaben und Befugnisse von Polizei und Justiz im datenverarbeitenden Staat anknüpft und damit die in diesem Bereich zwischen den Mitgliedstaaten bestehenden Unterschiede in das Datenschutzrecht inkorporiert, so dass insoweit eine datenschutzrechtliche Vereinheitlichung nicht stattfindet.

Soweit sich der Anwendungsbereich der Richtlinie auch auf die Datenverarbeitung in innerstaatlichen Verfahren erstreckt, ist der Bundesrat überdies der Auffassung, dass der Vorschlag für den Entwurf der Richtlinie nicht auf die angegebene Rechtsgrundlage des Artikels 16 (2) des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) gestützt werden kann (Beschluss des Bundesrates vom 30. März 2012, Drucksache 51/12).

2. Ungeachtet des Vorstehenden ist Deutschland bereit, an der aus seiner Sicht dringend erforderlichen umfassenden Überarbeitung des Vorschlags mit zu arbeiten, um die bestehenden Schwierigkeiten, falls möglich, zu überwinden. Insoweit erscheinen zu den Artikel 1 bis 8 des Richtlinienentwurfs insbesondere folgende Anmerkungen geboten:

   a) Deutschland setzt sich dafür ein, dass für den polizeilichen und justiziellen Bereich keine Vollharmonisierung erfolgt, sondern lediglich Mindeststandards auf hohem Niveau festgelegt werden. In Fortführung der in den Artikeln 1 (5) und 12 des Rahmenbeschlusses 2008/977/JI verankerten Philosophie sollten Mitgliedstaaten auch künftig nicht daran gehindert sein, strengere nationale Datenschutzbestimmungen zu erlassen, die es in der Folge auch bei Datenübermittlungen in andere Mitgliedstaaten zu beachten gilt. Diese Philosophie unterbindet jegliches „Datenschutz-Dumping“, ohne die kulturellen und rechtlichen Traditionen der Mitgliedstaaten im Polizei- und Justizbereich anzutasten.

   b) Im Bereich der polizeilichen Gefahrenabwehr gibt es Schwierigkeiten bei der Abgrenzung der Anwendungsbereiche von Richtlinie und Verordnung. Wenn – wie dies zum Beispiel im Bereich der Luftsicherheit und der grenzpolizeilichen Aufgabenwahrnehmung der Fall sein kann – die abzuwehrende Gefahr nicht strafbewehrt ist und folglich die Polizei im Rahmen ihrer Aufgabenwahrnehmung keine Straftat im Sinne von Artikel 1 (1) des Richtlinienentwurfs verhütet *[„prevention of criminal offences“]*, bleibt die Richtlinie unanwendbar. Soweit in diesen Fällen nach den derzeitigen Vorschlägen die Datenschutz-Grundverordnung gelten soll, erscheint diese für den Bereich der Gefahrenabwehr mit seinen spezifischen Besonderheiten völlig unpassend. Auch kann bei der Gefahrenabwehr oftmals nicht trennscharf zwischen der Verhütung von Straftaten und „sonstigen“ Gefahren unterschieden werden. Deutschland hält es daher für fachlich sinnvoll, den Bereich der polizeilichen Gefahrenabwehr einheitlichen Regelungen zu unterwerfen.

c) Nach Artikel 1 (2b) soll künftig der Austausch personenbezogener Daten nicht mehr „aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten“ eingeschränkt oder verboten werden können. Dies ist wohl so zu interpretieren, dass die Berufung auf ein abweichendes Datenschutzniveau zukünftig kein zulässiges Argument mehr sein soll, die Übermittlung personenbezogener Daten an einen anderen Mitgliedstaat zu verbieten oder einzuschränken. Eine solche Vorschrift wäre problematisch, weil sie ein EU-weit homogenes Datenschutzniveau voraussetzt, das nur schwerlich zu erreichen sein dürfte (vgl. bereits unter Ziffer 1).

Hinzu kommt, dass sich die (weitere) Verarbeitung von zuvor EU-intern übermittelten Daten nach dem Richtlinienentwurf lediglich an den allgemeinen Rechtmäßigkeitsvoraussetzungen des Artikels 7 messen lassen muss. Abweichend von der gegenwärtigen Rechtslage der Artikel 11 und 12 des Rahmenbeschlusses 2008/977/JI könnten personenbezogene Daten damit im Anschluss an eine EU-interne Übermittlung unabhängig von etwaigen im übermittelnden Mitgliedstaat geltenden Verarbeitungsbeschränkungen genutzt werden. Durch eine EU-interne Datenübermittlung könnten dabei selbst zentrale Prinzipien des nationalen Gefahrenabwehr- und Strafprozessrechts „abgestreift“ werden, soweit diese im Empfängerstaat nicht existieren. Betroffen könnten etwa Geheimhaltungsvorschriften (Amtsgeheimnisse, Berufsgeheimnisse, Steuergeheimnisse, Sozialgeheimnis etc.) oder Regelungen sein, die die Weitergabe von Daten mit Blick auf die bestehende Gefährdung einer Person (z. B. eines Zeugen) oder der drohenden Gefährdung des Untersuchungszwecks untersagen. Denn die entsprechenden Verbotsnormen könnten – unabhängig von ihrer polizei- bzw. strafprozessrechtlichen Bedeutung – immer auch als eine datenschutzrechtliche Verarbeitungsbeschränkung angesehen werden, die gemäß den Artikeln 1 (2) und 7 unbeachtlich zu bleiben hat. Dies würde zu einer unzulässigen Dominanz datenschutzrechtlicher Aspekte über das Polizei- bzw. Strafprozessrecht führen.

d) Nach Artikel 2 (3b) ist die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union nicht vom Anwendungsbereich der Richtlinie umfasst. Deutschland wendet sich gegen diese Abweichung von Artikel 1 (2) des Rahmenbeschlusses 2008/977/JI und plädiert für eine inhaltliche Einbeziehung dieser EU-Institutionen in den Anwendungsbereich der Richtlinie. Allein die Tatsache, dass die Regelungen für die im gefahrenabwehrrechtlichen und strafprozessualen Bereich tätigen EU-Institutionen rechtstechnisch nicht in der Richtlinie selbst, sondern in einer gesonderten weiteren Verordnung ergehen müssten, ist kein Grund für eine inhaltliche Herausnahme aus den Vorgaben der Richtlinie. Gleiches gilt für die behauptete bestehende Existenz eines hohen Datenschutzniveaus in den Organen: Dies bedeutete lediglich, dass der Umsetzungsbedarf gering wäre.

e) In Artikel 3 (5) wäre eine Klarstellung wünschenswert, ob auch die in Papierform geführte Strafakte unter den Begriff der „Datei“ fällt.

f) Die in Artikel 4 statuierten Grundsätze der Datenverarbeitung orientieren sich ausweislich der mündlich gegebenen Erläuterungen der Kommission an den entsprechenden Vorschriften der Richtlinie 95/46/EG (Datenschutzrichtlinie). Im Vergleich zu den bereichsspezifischen Regelungen insbesondere der Artikel 3, 4, 5 und 11 des Rahmenbeschlusses 2008/977/JI bedeutet diese Rückkehr zu den allgemeinen Formulierungen der Datenschutzrichtlinie für den polizeilichen und justiziellen Bereich einen Rückschritt, mit dem eine Absenkung des Schutzniveaus einherzugehen droht. Das gilt insbesondere mit Blick auf die Zweckbindung, für die der Rahmenbeschluss strengere Vorgaben enthält, die nicht übernommen worden sind. Zudem fehlen im Richtlinienentwurf Regelungen zur Archivierung und zur Festlegung von Lösch- und Prüffristen.

g) Die Löschungsverpflichtung des Artikels 4 (d), dessen Verhältnis zu Artikel 6 (1) und 16 im Übrigen unklar bleibt, ist zu weit gefasst und sollte um eine Ausnahmeregelung ergänzt werden. In bestimmten Fallkonstellationen, insbesondere wenn gesetzliche Dokumentations- oder Aufbewahrungspflichten bestehen, die Daten zur Wahrung der Rechte des Betroffenen benötigt werden oder aber die Löschung technisch mit unverhältnismäßigem Aufwand verbunden ist, sollte anstelle der Berichtigung oder Löschung die bloße Sperrung der Daten treten. Entsprechendes gilt auch für Artikel 4 (e).

h) Artikel 5 („Unterscheidung verschiedener Kategorien von betroffenen Personen“) und Artikel 6 („Unterscheidung der personenbezogenen Daten nach Richtigkeit und Zuverlässigkeit“) können nicht mitgetragen werden. In den Verhandlungen zum Rahmenbeschluss 2008/977/JI haben sich die Mitgliedstaaten bewusst gegen eine Regelung wie jetzt in Artikel 5 des Richtlinienentwurfs entschieden. Auch die nunmehr in Artikel 6 aufgegriffene Frage nach der sachlichen Richtigkeit von Daten wurde seinerzeit lange diskutiert – Ergebnis war die anlassbezogene, ausschließlich im Vorfeld von Übermittlungen durchzuführende Prüfpflicht des Artikels 8 (1) des Rahmenbeschlusses. Es besteht aus hiesiger Sicht kein Grund, von diesen Lösungen abzuweichen. Die Notwendigkeit pauschaler Unterscheidungs- und Kategorisierungspflichten erschließt sich nicht, ihre praktische Umsetzbarkeit scheint fraglich, der damit verbundene Bürokratie- und Kostenaufwand erheblich (aufwändige inhaltliche Prüfungen bei häufig wechselnden tatsächlichen Gegebenheiten; technische Anpassung von IT-Systemen etc.). Die Sinnfrage stellt sich umso mehr, als es beiden Vorschriften an einer Rechtsfolgenanordnung fehlt und infolgedessen offen bleibt, welche juristischen Konsequenzen an die Unterscheidung nach Personenkategorien bzw. nach der Richtigkeit und Zuverlässigkeit von Daten geknüpft werden sollen.

i) Deutschland bittet um Prüfung, inwieweit Artikel 7, insbesondere Buchstabe b, eine ausreichende rechtliche Grundlage für die Befugnis von Polizeibehörden, Staatsanwaltschaften und Gerichten enthält, Daten auch an andere Behörden zur Erfüllung deren (!) gesetzlicher Aufgaben, die nicht in der Verhütung oder Verfolgung von Straftaten bestehen, zu übermitteln. Die Polizei- und Justizbehörden müssen in zahlreichen Fällen Informationen, die sie im Zuge ihrer Ermittlungen erhalten, an andere Behörden weitergeben, damit diese von relevanten Umständen erfahren und selbst notwendige Maßnahmen ergreifen können. Dies gilt beispielsweise im Kinder- und Jugendschutz oder bei der Gewerbeaufsicht.

Zudem sieht Deutschland Prüfungsbedarf bei der Frage, ob Artikel 7 die Datenübermittlung an Private in ausreichendem Umfang ermöglicht. Sofern diese nur auf den dortigen Buchstaben c, nicht jedoch auch den Buchstaben b gestützt werden könnte, dürfte sie zu eng sein, da Ersterer die Notwendigkeit der Datenverarbeitung zur Wahrung lebenswichtiger Interessen einer anderen Person voraussetzt. Auch unterhalb dieser Schwelle können Private jedoch ein berechtigtes Interesse an einer Datenübermittlung haben, z.B. um eigene Rechtsansprüche durchzusetzen.

j) Deutschland sieht das in Artikel 8 (1) statuierte grundsätzliche Verbot der Verarbeitung sensibler Daten sehr kritisch. Gerade im Bereich der Strafverfolgung und der Gefahrenabwehr müssen in vielfacher Weise auch sensible Daten verarbeitet werden. So setzt z.B. die Verfolgung von Sexualstraftaten oder extremistischen Taten die Erhebung sensibler Daten geradezu voraus. Ein grundsätzliches Verbot der Verarbeitung genetischer Daten würde zahlreiche moderne Ermittlungsansätze von vorneherein erschweren oder zumindest doch diskreditieren.

Angesichts des im Richtlinienentwurf gewählten Grundsatz-Ausnahme-Verhältnisses erlangt der in Artikel 8 (2a) benutzte Begriff der „geeigneten Garantien“ zentrale Bedeutung. Es bleibt indes unklar, was damit gemeint ist. Insbesondere wird nicht deutlich, inwieweit diese Garantien über das hinausgehen müssen, was bereits für die Verarbeitung sonstiger Daten gilt. Hilfreich wäre zudem eine Klarstellung, ob und inwieweit innerhalb dieser Garantien Raum für Abwägungen bleibt, die auch gegenläufige (*i.e.* polizeiliche und justizielle) Interessen angemessen berücksichtigen. Aufgrund der aufgezeigten Probleme sollte daher überlegt werden, ob Artikel 8 – wie auch Artikel 21 der EU-Grundrechtecharta – nicht eher als Antidiskriminierungsregelung ausgestaltet werden sollte.

3. Auf die in den bisherigen DAPIX-Sitzungen vom 16. April 2012 und 26. September 2012 mündlich vorgetragenen Ausführungen wird Bezug genommen. Zudem wird nochmals darauf hingewiesen, dass Deutschland gegen alle bisher erörterten Vorschriften Prüfvorbehalt eingelegt hat. Da die Artikel 1 bis 8 allgemeine Bestimmungen und Grundsätze enthalten, deren Bedeutung vollumfänglich erst im Zusammenspiel mit anderen, bislang noch nicht diskutierten Vorschriften des Richtlinienentwurfs zutage tritt, behält sich Deutschland weitere Stellungnahmen vor.

COUNCIL OF THE EUROPEAN UNION

Brussels, 6 December 2012 (10.12)
(OR. de)

16497/12
ADD 1

Interinstitutional File:
2012/0010 (COD)

LIMITE

DATAPROTECT 131
JAI 817
DAPIX 144
FREMP 140
COMIX 651
CODEC 2738

NOTE

from:	German delegation
to:	Delegations
No. Cion prop.:	5833/12 DATAPROTECT 6 JAI 41 DAPIX 9 FREMP 8 COMIX 59 CODEC 217 + ADD 1 + ADD 2
Subject:	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

Delegations will find attached the comments of the German delegation.

ANNEX

Summarised comments of the

Federal Republic of Germany on Articles 1 - 8

of the 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

1. Germany welcomes the fact that, with this draft Directive, the Commission has initiated a discussion on improving data protection and information sharing in the area of police and judicial cooperation in criminal matters. However, our experts still have considerable misgivings as regards both the substance of the draft Directive and its individual provisions. Germany does not believe that it will help to improve data protection or the exchange of information.

   It is questionable whether the draft Directive provides added value over the current Council Framework Decision 2008/977/JHA, particularly with regard to data transmission between Member States. After extensive consultations, the Council Framework Decision did not come into force until 20 January 2009 and has not yet been implemented in all Member States. Until the Framework Decision has been sufficiently tested and shown to be inadequate, Germany does not find it appropriate to develop new data protection legislation. This is particularly true as the draft Directive falls short of the current Framework Decision on several key points.

Although we welcome the idea of a uniform high level of data protection in principle, the draft Directive's aim of harmonising national police and judicial data protection law is likely to be very difficult to achieve given the subject-matter's proximity to police law and the rules on criminal procedure. The laws on the police and the rules on criminal procedure differ considerably between the Member States. Harmonising these laws is not a policy objective, nor would it be possible under European law. Bearing in mind the draft Directive, this leads to a dilemma: on the one hand, there is a danger that the intended harmonisation of national data protection would lead to the creeping harmonisation of police law and the rules on criminal procedure, which is neither desirable nor permitted. We must take care not to cross this line. On the other hand, it seems doubtful that the Commission will be able to achieve its aim of harmonising data protection law given the different systems of police law and criminal procedure in the Member States. The juxtaposition of data protection law on the one hand and police law and the rules on criminal procedure on the other could lead to major practical difficulties. This is illustrated for example by Article 7 of the draft Directive, in which the lawfulness of data processing is assessed almost exclusively on the basis of the national and very differently structured tasks and powers of the police and courts in the processing state. This means that the differences between the Member States that exist in this area are incorporated into data protection law, with the result that data protection law is not harmonised.

Insofar as the scope of the Directive extends also to data processing at national level, Germany's Bundesrat is furthermore of the opinion that the draft Directive cannot use Article 16(2) of the Treaty on the Functioning of the European Union (TFEU) as its legal basis (Bundesrat decision of 30 March 2012, printed document 51/12).

2. Notwithstanding the above, Germany is willing to assist with what it views as an urgently needed revision of the proposal to overcome, if possible, the existing problems. We feel that the following comments are called for in particular with regard to Articles 1 to 8 of the draft Directive:

(a) Germany opposes full harmonisation in the police and judicial spheres and instead favours laying down only minimum standards at a high level. Following on from the principle set out in Articles 1(5) and 12 of Council Framework Decision 2008/977/JHA, Member States should not in future be prevented from enacting stricter national data protection legislation which other Member States would then have to abide by when data are transferred to them. This principle prevents any form of "data protection dumping" without interfering with the Member States' cultural and legal traditions in the police and judicial spheres.

(b) With regard to threat prevention by the police, it is difficult to distinguish between the scope of the Directive and that of the Regulation. If the threat to be averted is not punishable - as may be the case, for example, in the area of aviation security or border protection, and hence there is no police "prevention of criminal offences" as defined in Article 1(1) of the draft Directive, then the Directive still cannot be applied. If, in accordance with current proposals, the General Data Protection Regulation is supposed to apply in such cases, the latter seems entirely unsuitable for the area of threat prevention with its specific characteristics. It is also often impossible in threat prevention to make a clear distinction between the prevention of criminal offences and "other" threats. Germany therefore thinks it appropriate for threat prevention by the police to be covered by uniform provisions.

(c) Article 1(2)(b), proposes that in future it should no longer be possible for the exchange of personal data to be restricted or prohibited "for reasons connected with the protection of individuals with regard to the processing of personal data". This should probably be interpreted to mean that a different level of data protection is no longer to be invoked as an acceptable argument for prohibiting or restricting the transfer of personal data to another Member State. Such a provision would be problematic, as it presupposes a single, uniform level of data protection throughout the EU which could prove difficult to achieve (see 1 above).

In addition, under the draft Directive the (further) processing of data previously transferred within the EU will have to satisfy only the only general lawfulness requirements in Article 7. By way of derogation from the law as it currently stands - Articles 11 and 12 of Council Framework Decision 2008/977/JHA - personal data could, after being transferred internally within the EU, then be used without regard for any processing restrictions applicable in the Member State that transfers them. In this regard data transfer within the EU could have the effect of "wiping away" even central principles of national law on threat prevention and criminal procedure if these principles do not exist in the recipient Member State. This could affect for example provisions on confidentiality (official secrecy, professional secrecy, tax secrecy, confidentiality of social welfare data, etc.) or regulations prohibiting the forwarding of data which could endanger an individual (such as a witness) or constitute an impending threat to the purpose of an investigation. That is because - regardless of their significance in terms of police law or criminal procedure - such prohibitions could always be seen as processing restrictions under data protection law to be disregarded under Article 1(2) and Article 7. This would have the unacceptable consequence of data protection law aspects taking precedence over police and/or criminal procedural law.

(d) Under Article 2(3)(b), the processing of personal data by the institutions, bodies, offices and agencies of the European Union falls outside the scope of the Directive. Germany is opposed to this derogation from Article 1(2) of Council Framework Decision 2008/977/JHA and calls for these EU institutions to be substantively included in the scope of the Directive. The mere fact that the rules for EU bodies active in the area of threat prevention and criminal procedure are for legal reasons not set out in the Directive itself but have to be laid down in a another, separate Regulation is no reason for their substantive removal from the provisions of the Directive. The same applies to the alleged existence of a high level of data protection in those bodies, meaning only that there would be little need for implementation.

(e) In Article 3(5), it would be helpful to clarify whether paper-based criminal files are also included in the definition of "filing system".

(f) According to the Commission's oral comments, the data processing principles given in Article 4 are focused on the relevant provisions of Directive 95/46/EC (the Data Protection Directive). Compared to the sector-specific provisions of, in particular, Articles 3, 4, 5 and 11 of Council Framework Decision 2008/977/JHA, this return to the general wording of the Data Protection Directive for the police and judicial areas constitutes a step backwards which threatens to reduce the level of protection. This is especially true as regards purpose limitation, for which the Framework Decision has stricter requirements which have not been included in the draft Directive. Furthermore, the draft Directive has no provisions on archiving or on setting time limits for erasure and review.

(g) It remains unclear how Article 4(d) relates to Article 6(1) and Article 16, and the erasure requirement in Article 4(d) is too broad and should include a provision dealing with exceptions. In certain cases, in particular when the law requires that data be documented or retained and when data are needed to uphold the rights of the data subject, or when erasure would involve a disproportionate technical effort, the data should simply be blocked rather than rectified or erased. The same applies to Article 4(e).

(h) Germany cannot endorse Article 5 ("Distinction between different categories of data subjects") or Article 6 ("Different degrees of accuracy and reliability of personal data"). During the negotiations on Council Framework Decision 2008/977/JHA, the Member States consciously decided against a provision such as Article 5 of the draft Directive. At that time, the Member States also discussed at length the issue of data accuracy now dealt with in Article 6; the result was the requirement in Article 8(1) of the Framework Decision to verify the quality of personal data only before they are transferred or made available. In Germany's view, there is no reason to seek different solutions. We see no need for general requirements to distinguish between different categories; it is questionable whether they can be implemented in practice, and they will involve significant administrative and cost burdens (time-consuming assessment of content under frequently changing circumstances; technical adaptation of IT systems, etc.). The need for these provisions is all the more questionable given the fact that neither provision entails legal consequences, and so the question remains as to what legal consequences should be attached to the distinction between categories of persons or degrees of accuracy and reliability of data.

(i) Germany requests a review to determine whether Article 7, in particular (b), offers a sufficient legal basis for authorising police, public prosecutors and courts to transfer data to other authorities to fulfil *their* (!) legal obligations which do not involve preventing or prosecuting criminal offences. In many cases, the police and judicial authorities must forward information acquired during the course of their investigations to other authorities so that they are informed of relevant circumstances and can themselves take the necessary measures, for example as regards the protection of children or young persons or trade supervision.

Germany also thinks it necessary to examine whether Article 7 enables data to be transferred to private individuals to a sufficient extent. If such transfer could be based only on (c) and not also on (b), it might well be too restrictive, as (c) requires that data be processed to protect the vital interests of the data subject or of another person. However, private parties may have a legitimate interest in data transfer that falls below this threshold, e.g. for the purpose of enforcing legal rights.

(j) Germany is very critical of the absolute prohibition on the processing of sensitive data that is laid down in Article 8. It is precisely in the area of law enforcement and threat prevention that such data very frequently have to be processed. For example, prosecuting criminal offences of a sexual or extremist nature virtually necessitates the collection of sensitive data. An absolute ban on the processing of genetic data would make it difficult a priori to use many modern investigative approaches or would at least bring them into disrepute.

The principle - exception relationship chosen in the draft Directive lends the term "appropriate safeguards" used in Article 8(2)(a) primary importance. What is meant, however, is unclear. In particular, it is unclear to what extent these safeguards must go beyond what already applies to the processing of other data. It would also be helpful to clarify whether and to what extent these safeguards provide room for due consideration to be given to opposing (i.e. police and judicial) interests. In view of these problems, consideration should be given to whether Article 8 should not instead be formulated as an anti-discrimination provision, like Article 21 of the EU Charter of Fundamental Rights.

3. We refer to the oral remarks made at the previous DAPIX meetings of 16 April 2012 and 26 September 2012. We would also like to point out once again that Germany has entered scrutiny reservations on all the provisions discussed so far. As Articles 1 to 8 contain general provisions and principles whose full significance will become clear only in combination with other provisions of the draft Directive which have not yet been discussed, Germany reserves the right to make additional comments.