Annex to Federal Minister de Maizière's letter to the Greek and Italian Presidencies

Proposed roadmap to speed up the negotiations on EU data protection reform

1. Legal form and higher data protection standards in the public sector

The Council has so far been unable to agree on the legal nature of the General Data Protection Regulation. For a number of Member States, the central concern is to preserve the specific data protection law for their public administrations, which in some cases exceeds the standards set by the General Data Protection Regulation. They also want to retain the possibility of setting higher standards of protection with regard to specific risks posed by certain authorities, digital records and public registers. For Germany, this is a very serious concern.

In this context, there has been discussion of whether a directive would be the more appropriate legal form for the area of public administration. The opening clauses currently planned have clearly been unable to bring about the necessary consensus.

To make substantial progress on this point and create clarity with regard to the many questions arising in relation to the public sector, I propose as a broader compromise an opening clause in Article 1 or 2 of the General Data Protection Regulation which would allow the Member States to go beyond the General Data Protection Regulation as needed and pass stricter national data protection legislation for the public sector (for example on the rights of data subjects, on data security measures or on record-keeping). Germany sees the same problem with regard to data protection for employees. Such an opening clause could be worded as follows:

> *"This Regulation shall not prevent the Member States from providing for a higher level of protection in their national law applicable to the processing of personal data by public authorities exercising their sovereign powers and to data protection for employees."*

2. Specifying conditions for consent

Consent to data processing is one of the central elements of data protection law. The intention of consent is to enable data subjects to decide freely which personal information to disclose. We would like to further strengthen consent as the legal basis for data processing and as a special form of the right to privacy. To be more than a merely fictive legitimation, consent should be explicit, voluntary and given after the

data subject has been informed of the essential facts of the data processing. These conditions for consent must be specified for certain situations so that responsibility is not unfairly shifted to data subjects. The voluntary nature of consent is doubtful in the case of a significant imbalance of power between the data subject and the data processor, for example, or when the data subject needs a service offered by the data processor.

3. "One-stop shop"

The discussions at the JHA Councils in October and December 2013 and most recently on 6 June 2014 have stressed the importance of a one-stop shop in the interest of businesses while noting that data protection supervision must remain close to the citizens. In its opinion of 19 December 2013, the Legal Service of the Council argued that a one-stop shop model in which duties and powers are concentrated within a single supervisory authority, with the result that data subjects must regularly address their concerns to a supervisory authority and court of another Member State, contradicts the fundamental rights of the European Union. For this reason, Germany has proposed an alternative one-stop shop model which reinforces the local supervisory authorities and ensures the necessary closeness to the citizens. The discussions at the JHA Council on 6 June 2014 showed that the German proposal is a good basis for addressing the concerns of the Legal Service. Given the strong support from the Member States, in particular France, I would like to promote this proposal while making clear that Germany will only support a solution that addresses the arguments of the Legal Service regarding fundamental rights.

4. Data transfers to third countries

In a globally networked world, the chapter on sending data to third countries is extremely important in a number of ways. I am glad we were able to make significant progress on this issue at the JHA Council on 6 June 2014. Further negotiations must quickly resolve the following three points:

- Firstly, the provisions must offer effective protection for data subjects. This applies especially to businesses' disclosure of data to government authorities in third countries. Germany has therefore proposed an Article 42a, which I believe is essential at the current stage of discussion of Chapter V. We have reminded the Council of this proposal in a protocol note.

- Secondly, we need a stable legal framework within the Regulation itself for instruments such as Safe Harbor. The Commission's evaluation has already point-

ed out the need for action with regard to Safe Harbor. The Commission's recommendations to improve Safe Harbor (improved transparency, legal redress and enforcement) should be quickly implemented and a Safe Harbor provision improved on this basis should be anchored in the Regulation as the basis for agreements of companies in relevant third companies.

- Thirdly, the rules on data transfers to third countries must not make it practically impossible to publish information on the Internet. In its judgment in the Lindqvist case, the European Court of Justice had to answer the question, among others, whether rules on data transfers to third countries apply to information published on the Internet. Because Ms Lindqvist's website, which mainly published information intended for confirmation candidates, can in practice be accessed from every country of the world, applying third-country rules would have meant that information published on the Internet regularly resulted in unlawful transfers to third countries without the appropriate level of data protection and would therefore have to be prohibited. The European Court of Justice rejected this argument on the grounds that such prohibition could not be the desired result, and that the creators of the Data Protection Directive (95/46/EC) could not have intended such a result, as the Community legislature would not have been able to foresee the future Internet applications at the time the Directive was passed. The Court found that, given the structure of the Internet, which allows uploaded data to be accessed anywhere in the world, the special regime for third-country data transfers would necessarily become a general regime applicable to all data transfer on the Internet. According to the Court, this could result in a significant, and possibly total, restriction of information published on the Internet, which would also lead to a massive restriction of the freedom of expression. When determining whether data are transferred to a third country, it is necessary first to determine which location is relevant: If the location of the e-mail provider is the determining factor, then the additional conditions of the third-country rules would apply to all e-mail providers not established in any Member State.

5. Big Data and profiling

We would like to further improve the ability of the General Data Protection Regulation to deal with the Internet with regard to cloud computing, social networks, wearables and the Internet of things. Big Data refers to data processing which offers enormous opportunities for society (for example in the area of health, education and environmental protection). An important use of Big Data is creating individualized profiles. However, profiles are created not only using Big Data applications, but also by evalu-

ating data which an individual service provider collects on the people using its services. Large quantities of data make it possible to create individual profiles and score values, for example, and to make statements of probability about individual behaviour. Profiles are now being created with non-personal data and with personal data published by data subjects themselves. Requirements to inform data subjects and obtain consent can reduce these dangers. But they reach their limits when informing data subjects depends on identifying them, which creates a further problem of data protection. For this reason and due to the massive amounts of data and the large number of data subjects concerned, scientists and practitioners around the world are working to develop additional protective mechanisms. I am therefore in favour of strengthening tried and tested instruments such as consent and providing for additional innovative protection mechanisms if necessary. In addition, data subjects must have effective entitlement to information in order to understand the implications of decisions based on profiles, such as evaluations of creditworthiness.

6. Freedom of expression and freedom of information

With regard to the judgment of the European Court of Justice in the matter of Google v. the Spanish data protection agency (file number C-131/12), we should address at an upcoming Council what implications this judgment may have for privacy protection and for the freedom of expression, information and the press. The public debate focuses in particular on how search engine operators can be sure of making appropriate decisions which not only protect privacy but also pay sufficient attention to freedom of expression. Some have demanded independent arbitration services; very different solutions for establishing and running such services are conceivable.