Dear Madam/Sir,

The German Federal DPA answers to the questions raised in section 3 of the above mentioned questionnaire as follows:

3. A
Supervisory authorities are regarding the Directive 95/46/EC the German Federal Commissioner for Data Protection and Freedom of Information (BfDI) as Federal DPA and the “Länder”-DPAs (eg. The DPA of Berlin). Regarding the Directives 2002/58/EC and 2006/24/EC the responsible supervisory authorities are the BfDI and the Federal Network Agency for Telecommunications (Bundesnetzagentur) as the regulatory authority for the telecommunications sector.

3. A. 1
The BfDI as well as the Bundesnetzagentur have investigative powers vis-à-vis providers. In case of complaints against a provider both authorities are able to launch an investigation, which can be limited to an official correspondence but as well lead to an on-site-inspection. In
regard to the Data Retention Directive the BfDI visited a few providers to be informed about the practical implementation of the national law implementing the directive.

3.A.2
The BfDI and the “Länder”-DPAs have investigative powers vis-à-vis law enforcement authorities. On the federal level, these investigative powers have not been made use of with respect to the implementation of the Data Retention Directive. Therefore, there haven’t been any cases to be reported about.

As described in 3.A.1 the BfDI has investigative powers, which also include in-situ audits. Being part of the Article-29-WP’s subgroup on data retention, the BfDI participates in an evaluation of the implementation of data retention by the telecommunication providers. Therefore a questionnaire focusing on 10 areas that are relevant for the retention and the security of traffic data (e.g. IT security, logical protection, physical protection, and back-up and disaster recovery procedures) was sent out to a few providers chosen to represent the German telecommunication market. Upon return and evaluation of the answers to this questionnaire the BfDI audited the providers based upon their answers.

Concerning the logical and physical protection all of the providers could be attested a high standard of security. The retained data are generally stored separate from operationally used data. In all cases the access to the data was limited to a small number of specially educated employees, which had to use workplaces password protected with specially registered IP-addresses.

However, also critical points were identified during the audits. The logging of the access to the retained data, for example, could not be considered sufficient in most cases, if there was logging at all. Also in some cases more data is stored than required by the German law implementing the Data Retention Directive (e.g. IP-traffic volume, cell IDs a mobile phone used for data transfer during mobile internet access, technical information concerning telephone switches). This surplus retention mostly is due to the subject of the German law not being precise enough in stating what data to store or not matching the factual technical circumstances. Sometimes the providers just do not comply with the regulations.

3.A.5
The BfDI has no experience concerning the matter of centrally stored data.

3.A.6
An action against the national law implementing the Data Retention Directive has been filed with the Federal Constitutional Court. There will be a hearing on December 15th, 2009 and a decision by the court is to be expected within the first half of the year 2010. In 2008 the Fed-
eral Constitutional Court already issued two preliminary rulings restricting the use of the retained data until the court has reached its final decision.

There are also proceedings currently under way concerning the question of whether providers are obliged to carry the costs of the data retention (especially the asset costs for the systems needed to retain the data as required by law), as well as regarding the question whether the providers are obliged to inform a telecommunication user about the data retained to his person.

3.B
Section 111 of the German Telecommunications Act requires telecommunication providers to collect data (name, address, phone number, etc) i.a. of all the persons getting a prepaid SIM card. However the data provided by the customer has not to be verified by crosschecking any official identification. Therefore a general traceability of a prepaid SIM card can be achieved, though there is no guarantee, that the data linked to the prepaid SIM card is referring to a real person or, even if so, that this person is actually the one using this SIM card.

Best regards
By order

Hensel