Dr. Sommer, Landesbeauftragter für Datenschutz und Informationsfreiheit, Bremen/Germany

Press Release: Conference of data protection commissioners says that intelligence services constitute a massive threat to data traffic between Germany and countries outside Europe

In response to reports of extensive surveillance by foreign intelligence services, in particular the U.S. National Security Agency (NSA), in the absence of specific suspicion of wrongdoing, the Conference of Federal and State Data Protection Commissioners calls to mind the powers given by the Federal Data Protection Act and the EU's Data Protection Directive to the data protection supervisory authorities with regard to international data traffic between companies in Germany and countries that are not members of the European Union.

In a number of decisions, the European Commission has defined "Safe Harbour" principles for data transfer to the U.S. (2000) and standard contractual clauses for data transfer to countries outside the European Union (2004 and 2010). These principles are intended to ensure that appropriate standards of data protection apply to personal data sent to the U.S. or other non-EU countries. However, the Commission has always stressed that the national supervisory authorities may suspend the transfer of data to such countries when there is a "substantial likelihood" that the Safe Harbour principles or standard contractual clauses are being violated.

This is now the case. There is a substantial likelihood that the principles in the Commission's decisions are being violated: According to current information, the NSA and other foreign intelligence services are accessing personal data sent from companies in Germany to offices in the U.S. and doing so on a large scale, without suspicion of wrongdoing and in disregard of the principles of need,proportionality and purpose limitation. The Safe Harbour agreement does contain a provision limiting adherence to the Safe Harbour principles when required by national security or if laws create such authorizations. In view of the aim of providing effective privacy protection, however, these powers of access are to be used only to the extent actually needed and not excessively. In a democracy, therefore, national security considerations cannot justify comprehensive access to personal data without reasonable suspicion. When transferring data to the U.S. on the basis of the standard contractual clauses, importers of data must state that, to the best of their knowledge, their countries have no laws that would seriously interfere with the guarantees in these clauses. Such a general authorization seems to exist in the U.S., as this is the only way to explain the substantial likelihood that the U.S. intelligence service routinely accesses personal data transferred on the basis of the standard agreements.

The Conference therefore calls on the Federal Government to provide a plausible explanation of how the unlimited access of foreign intelligence services to personal data of persons in Germany is effectively limited in line with the principles referred to. Until this is guaranteed, the data protection supervisory authorities will not issue any new permission for data transfer to non-EU countries (for example also for the

use of certain cloud services) and will examine whether such data transfers should be suspended on the basis of the Safe Harbour framework and the standard contractual clauses.

Lastly, the Conference calls on the European Commission to suspend its decisions on Safe Harbour and on the standard agreements until further notice in view of the excessive surveillance by foreign intelligence services.

The current chair of the Conference of Federal and State Data Protection Commissioners, Dr Imke Sommer, stated in this context: "Companies that send personal data to the U.S. bear the responsibility for these data. Like everyone in Germany, they must therefore have an interest in ensuring that personal data flows are not subject to large-scale surveillance by intelligence services."