

Thilo Weichert

Privacy and Data Protection in federal police cooperation

There has been cooperation for many years in the European Union concerning matters of «national security». In the intergovernmental third pillar of EU «Interior and Justice» a joint policy is strived for.

Table of contents

- I. Introduction
- II. The Free Flow of Statutory Basis
- III. The Free Flow of Data
 - 1. Classical Cooperation
 - 2. Electronic Cooperation
- IV. Consequences
 - 1. Legal Framework
 - 2. Data Subject Rights
 - 3. Development of Common Technical Standards
 - 4. Evaluation
 - 5. Supervision

I. Introduction

[Rz 1] There are first signs of common legal and organisational structures. This is particularly true for the law concerning aliens and asylum which has already been integrated into the first pillar of the European Union and most currently for the setting up of Eurojust.

[Rz 2] Under aspects of data and privacy protection the **police sector** is most interesting and currently subject to major changes. The non-EU-institutional cooperation of Schengen group members has been taken into communityship. The Schengen Information System (SIS) is enlarging. The European police authority Europol being under a rather enigmatic data protection regime, leads a rather peripheral existence in the EU. There is a discussion ongoing concerning a number of European instruments of criminal investigation that are already established in national laws such as joint finger print and DNA databases or provisions for a legal basis on European database searches (Rasterfahndung). It is planned to connect national registers of judicial antecedents. The attempt to vest the police with authority to restrict basic rights (Eingriffsbefugnisse) on an intensive level has been put forward not very sensitively as the current endeavours towards a broad European commitment to store telecommunication data for criminal investigation purposes show. In establishing due processes concerning protection, politics seem to be more scrupulous and reluctant.

[Rz 3] This is reason enough to choose the matter of police cooperation as a central theme from the **point of data and privacy protection**. Experiences by the supervisory bodies responsible for monitoring the Schengen Information System and Europol already exist. Their perspective – quasi from above – must be completed by a perspective from the bottom – a national perspective. So far there are only a few insights; yet, the reports of national supervisory bodies responsible for monitoring hint at several problematic fields that are still left unexploited.

[Rz 4] It makes sense to make existing experiences in **police cooperation of a federal state** useful to draw conclusions regarding cooperation in Europe. Germany is a good example, because its federal structure most of all in the police are parallel to those in Europe: competencies in legislation and public administration used to be allocated solely as competencies of the single federal states. At the same time there is a strong tendency to centralization which just reached a new peak as the «Bundesgrenzschutz» (Federal Border Guard) was renamed to «Bundespolizei» (Federal Police). The Data Protection Commissioners of the Federation and of the individual states have great experiences in cooperation between federal and state bodies that are mostly transferable to the European situation.

II. The Free Flow of Statutory Basis

[Rz 5] Law enforcement activities by the police are usually connected with **intrusions on privacy rights** that according to national as well as European law may only be executed pursuant to a law (restrictions of Art. 2 par. 1 in connection with 1 par. 1 German Basic Law, Art. 8 Charter of Fundamental Rights of the European Union). The legal requirements for such actions differ between the states (Laender) and the Federation regarding the relevant definitional elements as well as the protective regulations of the procedural law. In Germany parallel regulations exist in criminal procedure law of the Federation (Code of Criminal Procedure, Strafprozessordnung, StPO) as well as in the police codes of the Laender concerning restrictions of the right to informational self-determination; some regulations are even duplicated by secret and intelligent service law of the Federation and the Laender.

[Rz 6] Experiences show that security authorities tend to make use of those laws that afford the lowest requirements (competence-shopping). There is a general tendency to give preference to police law rather than criminal procedure law because actions according to the former are not subject of (a rather painful) **supervision** by the public prosecutor's office. On the other hand, it sometimes is quite comfortable for the police to pass responsibility to the prosecutor's office for specific actions. In recourse of criminal procedure law it is also possible to prevent an action to be controlled by an administrative court. In order to withdraw an action completely from public control, it may also happen in singular cases that it is carried out in the course of an informal cooperation by a secret service.

[Rz 7] A good example for competence-shopping are **database searches** (Rasterfahndung) executed after the incidents of September 11, 2001 throughout the federal states. Most of all the Federal Office of Criminal Investigation (Bundeskriminalamt) (!) obviously insisted on conducting the investigation according to the laws of the individual German states (!) even though there was a federal regulation in the Code of Criminal Procedure and the incidents of September 11 being the only connecting factor for investigations and no other substantiated risk detectable. It was obvious that the judiciary was not willing to support database searches as demanded by the Ministers of Interiors. Two states that did not have a statutory basis for database searches especially adopted such a bill: obviously it was easier to convince a state parliament of the necessity for such a desirable measure rather than the judiciary. The aim to omit a judicial decision may also give way to make use of state police law. According to German law, many restrictions based on criminal procedure law executed by the police depend on the judgement of a court (Richtervorbehalt) which is not the case or not to this extent for their counterpart in police law.

[Rz 8] If, in individual cases, the **substantive requirements** for an informational action according to criminal procedure law are fulfilled rather than those of police law, it occurs that criminal procedure law is given priority: for example, for identification proceedings (erkennungsdienstliche Maßnahmen), collected as a matter of routine whenever specific offences are involved even without a probability of repetition being necessary.

[Rz 9] In spite of federal independence of individual states, it can be stated that far reaching jurisdiction to restriction of rights pursuant to the Criminal Procedure Code often tempt the police to call these in for their own concerns (e.g., telecommunications surveillance, acoustic residence surveillance, genetic fingerprint identification) even though these actions are rather unsuitable for purposes of hazard prevention (Gefahrenabwehr). Similar adaptive mechanisms can be detected in between different police laws: a police law providing for multiple restrictions meets - depending on the current political climate - easy approval in other states. Data and **privacy protective measures** (e.g., time limitation of acts, evaluation regulations, obligation to notify the data protection representative) on the other hand do not have such an exemplary nature.

[Rz 10] Security law in Germany is shaped by different **party politics**. One political side often uses participation in government offices to question security law on the other level (federation or individual state). If, for example, specific measures cannot be pushed through on the federal level, they are enforced in police law on state level even though they should be classified as criminal prosecution from the legal point of view: for example, the introduction of genetic fingerprinting for children in the state of Hesse which would not have found a majority on the federal level.

[Rz 11] Comparable mechanisms can already be detected in the relationship between member states and EU: for the

benefit of security politicians is – diverging from the federal structure in Germany – that there is no clear demarcation line between central (criminal procedure) and regional (hazard prevention) legislative competence. The German Minister of Interior tried to establish database searches against terrorist perpetrators on the European level after his national attempts turned out a total failure in order to push the national discussion using the **power of the European Council**. Similar efforts can be determined – by the European Council – for the Cyber Crime Convention. This procedure is much more obvious concerning stock of telecommunication traffic data; the German Minister of Interior switched to the European level after recognising that the Bundestag (Federal Parliament) would not be willing to support his political demands. The idea is to force the national legislator by European law to pass a national law that otherwise would not have been passed at all. Such procedures can be called «policy laundering».

[Rz 12] This tendency is encouraged by what seems a reduced **standard in fundamental rights** on the European level. The jurisdiction of the Federal Constitutional Court, (Bundesverfassungsgericht) that explicitly stresses basic constitutional rights, must not be taken directly into consideration by EU-bodies, especially the European Council, when reaching consent on intrusions on privacy rights.

III. The Free Flow of Data

[Rz 13] There are different **intensities in informational police cooperation**: from

1. occasional (anlassbezogen) to 2.
2. periodical exchange of information,
3. joint working groups,
4. joint databases up to
5. joint law enforcement or investigations.

[Rz 14] On the European level an informational cooperation developed from SIS to Europol and up to the 4th stage. The German police actually practices actions on the 5th stage. Here, a number of serious problems regarding privacy protection occur.

1. Classical Cooperation

[Rz 15] No problems are to be expected if information is **exchanged occasionally**. Responsibility for data processing is clearly defined. It does not make any difference whether information is exchanged electronically or conventionally. If responsibility is transferred, meaning transmission of data, lawfulness can be checked at either point of transmission. Within the limits of transmission specific requirements (earmarking, prohibition of transmission, prohibition of exploitation, obligation to notification) can be defined and adherence can be checked. If these requirements are not complied with, there is – at least theoretically – a stop of communication possible to effectively sanction non-compliance.

[Rz 16] In **periodical or regular information exchange** there is no strict necessity check in singular cases on the sender's side. Such procedures are widely spread for situation reports by the police. The electronic equivalent is an automated file that can only be read but not worked on. In Germany such automated provision of data (automatisierte Abrufverfahren) exist in the field of police in the central databases of the Bundeskriminalamt (Federal Criminal Police Office, abbreviated BKA) within the INPOL cooperation, the computerized information system of the police. INPOL moreover maintains integrated files (Verbunddateien) that can be processed and worked on by the individual states. On a European level the Schengen Information System (SIS) as well as the Fingerprint System Eurodac belong into this category.

[Rz 17] For regular data transmission attention needs to be paid that there is no data transmission just for the good of it, meaning that the data provided always needs to be necessary for the tasks assigned. On a first level a **general evaluation** can take place, but must be reviewable and revisable in singular cases.

[Rz 18] Regular data transmission relies on the receiving party only to retrieve and store data that are necessary for

their own tasks. Therefore, a high level of **confidence into the lawfulness** of data processing by the agencies involved must be given. This may already be problematic in the national context because even in Germany different privacy protection cultures are pursued. A lesser problem in so far are partly diverting national regulations. There are only minor differences in the legal standards in privacy protection laws in Germany. The framework legislation as well as the jurisdiction of the Federal Constitutional Court has a unifying impact.

[Rz 19] On the European level only a limited amount of such security nets exist: Even though there is a – still not binding – Fundamental Rights Charta, the European Court of Justice is guided by a **common standard of fundamental rights** in its jurisdiction. Yet, especially in the field of police we are far away from a joint legal culture. So far there are neither common overall privacy protection principles in the police sector nor a European criminal procedure code with uniform guidelines according to the rule of law. And there are only first small signs of coordination and cooperation among the data protection authorities.

[Rz 20] From the privacy protection point of view **joint working groups** among the police forces have the advantage that no direct electronic communication takes place, which basically means that no extensive electronic data stocks are exchanged. At the same time the members of the single police forces usually have comprehensive access to the data of their own agency. These information can then be shared with the colleagues from other security and intelligence agencies at the round table. Which data are exchanged often withdraws from any control especially if the exchange occurs on demand or taking shortcuts from the official channel route.

[Rz 21] Such working groups exist where joint investigations are conducted by different prosecuting authorities. An up to date example forms the establishment of so-called **information boards** (Lagezentren) of the German police authorities and intelligence services in Berlin just recently to fight terrorism. Such information boards are typical in the field of international cooperation among security authorities. A more institutionalized form of international cooperation includes cooperation with the European Police Office EUROPOL, where Europol officers and liaison officers work together.

[Rz 22] As working in joint committees naturally is a more informal cooperation, supervision as regards data protection is practically impossible. It is not ensured that personal data transmissions are put down in a protocol being checked. Therefore, it is usually impossible to find out the point of origin of specific information, whether it was obtained lawfully and how its utilisation is limited. In this context one can even talk about «**data laundering facility**»: data obtained unlawfully can be passed «across the table» and be processed without complaints by the receiver in a now cleaned form and can thereupon be passed back.

[Rz 23] Not only cooperation but also non-cooperation within the scope of the German federal security structure is a problem of data protection: since legal competence of the Federal Police and the intelligence services has been broadened, there are more and more areas in which not only the state police is the competent authority but further security authorities are competent for the same case, resulting in parallel investigations at different bodies concerning the same case. This may lead to **multiple intrusions on privacy rights**. From the privacy protection perspective, there is even more that is unwanted. It is almost a classical problem of German Security politics that security authorities mutually obstruct their own work and manipulate the results of investigations due to opposing influence. This problem can only be solved by a clear legal separation between duties and coordination.

2. Electronic Cooperation

[Rz 24] Basically there are no other problems in electronic than in conventional data exchange. This is at least true for single transmissions on occasional demand or by ones own initiative and for retrieval of data from a database. The establishment of a joint electronic **police information system** (known as INPOL) in the beginning of the 70ties in Germany caused even more confusion. It comprises a bundle of so-called «Verbunddateien», integrated files shared by the police forces of the Federation (Federal Police, customs authorities, BKA) and the individual states. The Bundeskriminalamt (BKA) serves as the central information and communication office of the German police within the INPOL system: the BKA is active in three specific roles: 1. storage and provision of own data, 2. coordination of a network between the Federation and the police forces of the individual German states, and 3. processing data on behalf of the individual German states. It also partly processes data for which the Federation and a single or some states have joint responsibility. A physical division between data of the Federation and data of the

individual states does not take place in the classical shared INPOL files.

[Rz 25] This leads to a merging of **responsibilities** for data processing which is mostly true for the data stocks of the individual states: here, responsibility remains completely with the states. Yet, since factual availability lies with the BKA, the states often do not perform their duties. This can result in disregarding control and review deadlines, «forgetting» data processed on behalf while deleting own data, not deleting or correcting data even though ordered by the states, or wrong information of the data subjects about the existence of data.

[Rz 26] Currently, the conversion of the old INPOL system, basically deriving from the 70ties, to a new system is prepared in Germany; technically it functions like a big **data warehouse**. Already today there are quiet many police data stocks that are available for complex analysis. Data warehouse solutions open up a lot of possibilities of technical data protection using differentiated responsibilities, purposes, access regulations, protocol and analysis on the one hand. At the same time risks in privacy protection are greatly enlarged: basically any datum can be processed for any purpose by any participant. Under certain circumstances these utilisations of data are unlawful und must be excluded by complex technical and organisational measures. Data warehouses with multiple responsibility rise new problems in data protection control; the later must be granted to every supervising authority being competent for an admitted participant and must be granted for the whole system.

[Rz 27] A terrific example for problems connected with shared files is the German discussion on building a joint **database file on terrorist and Islamic extremists** by the police forces and the intelligence services of the Federation and the states in Germany. It is sought to mutually provide information on Islamic terrorism collected by the respective security authorities. Two different approaches are discussed: 1. a reference file (Index-, Hinweisdatei) or 2. an information file (Erkenntnisdatei). A reference file only indicates names and objects and the authority that is in possession of information on either and the respective reference number of the authority that can be contacted and can provide their information in accordance with legal provisions. An information file provides investigative results and can be accessed as clear text from almost all terminals of participating authorities. An information based file causes rather more privacy and practical problems than it provides solutions: as legal competencies and jurisdiction differ greatly among the participating bodies, especially between the police authorities and the secret services, information is disclosed to agencies that are neither competent nor eligible to gain knowledge. As the information is detached from its original context, preliminary information is often interpreted as objective knowledge. The biggest problem from the point of the security authorities is the disclosure of conspiratorial information simultaneously endangering their sources. A solution to these problems is not yet found.

[Rz 28] Integrated solutions foster organised irresponsibility: since there is only partial responsibility encumbered on the individual participating authority, nobody feels competent for privacy protection; neither for single file stocks nor for the whole system. A prime example have been the **database searches** in the aftermath of September 11th, 2001 in Germany: the state police forces collected data and provided them on their own behalf for BKA comparative searches. At the same time, the BKA collected data on its own which were also incorporated. From the legal point of view, the state data should have been processed strictly in accordance with the orders of the states. De facto BKA data is not under control of the states, but subject to BKA analysis and considerations.

[Rz 29] Ambiguity concerning responsibility prolongs into conflicts concerning **control of privacy protection**: Even though BKA processes data on behalf of the individual states and therefore is obliged to process the data strictly in accordance with the orders of the respective states, it withdraws from supervision to be executed by the respective state commissioners arguing that it is an obstacle to basic principles concerning distribution of federal competence. Even the Federal Data Protection Commissioner is, due to legal obstacles, not the competent supervising authority because lawfulness of data processing is solely subject to state law.

[Rz 30] The amalgamation of federal and state data with diverging responsibilities results in a stock of data to which **different regulations** apply: this is true for the substantial requirements of storage and transmission, time limits of control and erasure, the procedural requirements (for example for obligations to participation, notification, and instruction), and for performance of the rights of the data subject. Yet, due to a broad homogeneity in the law of data processing by the police in Germany no significant consequences result

[Rz 31] On the **European level** there are already a number of integrated files within the field of police which are of

varying quality; for example, at Europol and in SIS. France, Germany and Spain have made an agreement to allow mutual access to the databases of the public prosecutor's office. In Germany the problems arising from diverting law often lead to unbridgeable gaps. It may, though, cause less problems to agree on a mutual standard for data formats that can be used with a mask in the respective mother language. Language skills may even make it possible to use free text in mutual data in a way understandable by the respective police officers. Anyhow, it is downright impossible to provide the respective laws to be applied in a comprehensible form. Such centralized legal information do not exist to my knowledge; at least not in a language known to all participants. The differences of the respective national cultures and legal interpretation of statutes can definitely not be comprehended. The consequences are at hand: in the best case, a police officer takes the domestic law as a basis even though not applicable. More probable though is that no legal check is taking place at all hoping or speculating that the respective national law applicable to the data permits its specific utilization.

[Rz 32] The diverging legal frameworks have serious consequences for **supervision by the data protection authorities**, but also by **courts** and **parliaments**. This shows during the further development of the Schengen Information System (SIS II). The system, to which the EU countries as well as Norway, Iceland, and henceforth Switzerland belong, is subject to EU parliament (EP) approval only concerning the granting of visa belonging to the first pillar of the EU. In further areas – in the classical fields of the judiciary and law enforcement – merely a consultation of the EP takes place. Accordingly, the rapporteur of the EP complaint about an «impossible situation»: «we cannot vote for a part of the new database without checking its other functions.»

[Rz 33] To clarify responsibility for police data in the European information systems renders more complicate because most of the data do not derive from the national police forces but from independent police agencies, which is especially the case in federal states such as Germany. These police agencies are **independent from their national central police** forces as regards their operational, legal and hierarchical organisation. This may lead to a situation in which the law applicable to these agencies (e.g., the respective state police law in Germany) stays applicable even on a European level.

IV. Consequences

1. Legal Framework

[Rz 34] The simplest and most obvious consequence would be to create a uniform **common legal basis** for joint police data processing. As obvious as this step may be, as unrealistic it has been so far. The single legal basis for privacy protection in the field of police work is a recommendation of the European council as regards data processing by the police from the year 1987. The substantive regulations of the Europol Convention are restricted to a less specific standard, because its central or even single requirement for lawfulness often is the necessity to fulfil the assigned tasks. Serious endeavours to create a uniform legal framework in the sense of a standard protecting the data subjects cannot be detected. To give way to police enforcement jurisdiction for European or international cooperation often comes as a political reflex on international crime, may this be offences related to terrorism, organised crime, or sexual offences.

[Rz 35] The necessity for a **common development of data and privacy protection** may result from a privacy protection scandal in exceptional cases if it actually gains publicity. Generally, a high common standard can only be reached by a joint political awareness of politicians concerning the importance of privacy protection. Insofar, parliamentarians play an important role. In the past they have safeguarded their assignment to secure basic rights repeatedly in a responsible way. Another role could be played by lobbying of organised administrations. Unfortunately the EU has disintegrated privacy protection from the directorate-general Single European Market and made it part of security administration and therefore asked for trouble. Anyhow, the supervising data protection authorities and the civil rights organisations still further the cause of privacy protection and their influence must be strengthened.

2. Data Subject Rights

[Rz 36] Concerning data subject rights the Schengen treaty constitutes the best theoretical solution: it is upon the data

subjects to choose the country in which they would like to claim their rights. Applicable is the national law of the country chosen. This enables the data subjects to have recourse to privacy protection law «at home». There is even some kind of **most favoured nation treatment**: the data subject can choose the law most favourable to his or her case. The distress of the supervising authority or court having jurisdiction to assess the foreign subject matter is dealt with far easier than that of the data subject who would be urged to claim his or her rights in a foreign country under foreign law.

[Rz 37] This approach was not pursued further on the European level concerning what later became integrated files because ambiguity in competence matters can arise. No infringements of rights of the data subjects occur if a solution is chosen as practiced in Germany for years: if more than one body is engaged in data processing, the data subject can turn to any one of them. It is then obliged to **forward the issue** to the competent body. The regulations of data subject rights for Eurodac are guided by this approach.

[Rz 38] In comparison to this, data subject rights are regulated quite unsatisfactory for Europol being close to a **most discriminating procedure**: a refusal to give information can be expressed by any of the participating state according to the respective national law. Remedial actions can only be taken by a complicated procedure involving the common supervisory authority. The rights to deletion and correction solely depend on the vague regulations of the Europol Convention and not at all on the national law of the country providing the data.

[Rz 39] In the performance of data subject rights there are two comparably sensible and sufficient regulating approaches: for data having a clear national responsibility, it is most sensible to treat data subjects' rights according to the respective national law. If data are in the possession of several bodies, a **uniform privacy protection law** should be applicable. It goes without saying that these rights must not go below currently established standards. For the elaboration of such standards – that are still to be expected –, the respective highest standard of national regulations should be the guideline concerning data subjects rights.

3. Development of Common Technical Standards

[Rz 40] German federalism led to multiple technical solutions for processing personal data among the individual states and the Federation. This resulted in a development of 17 more or less diverging infrastructures of police data processing. Establishing INPOL, a somewhat harmonizing effect occurred because uniform interfaces were defined. However, it did not change anything as regards **fragmentation of it-infrastructure**.

[Rz 41] The attempts to standardize this particularism for a new conception of INPOL have not been really successful in the beginning because a **maximum functionality** was envisaged and privacy protection issues have not found consideration right from the start. The consequences are not only in view of privacy protection, but also in general concerning the functionality of procedure greatly unsatisfactory.

[Rz 42] In a federal system it is very difficult to establish a **uniform it-system**. Yet, such uniformity always bears a chance to establish uniform high standards of privacy protection as well. At the same time though, there is the risk that privacy enhancing technology is not sufficiently deployed and therefore the whole system is not operated according to a due process of basic law. This can be prevented by an early incorporation of privacy protection which is, as a matter of fact, provided for by European law in the instrument of prior checking (Vorabkontrolle).

[Rz 43] Schleswig-Holstein provides further instruments to ensure the deployment of privacy enhancing technology: a data protection ordinance obliges to prepare a detailed specification as well as a **security and privacy protection concept** before launching a new system. Only after a test phase under consideration of privacy protecting requirements the controller in charge may release the product. A rather less strict procedure is provided for by federal law: the setting up of police systems requires a mandatory directive (Errichtungsanordnung) for which the substantive due process of law regarding the processing of data as well as precautionary measures of data security implementing sufficient technical and organisational measures are subject to review. In a complex procedure with many participant data and privacy protection requirements can only be realised by including representatives of data and privacy protection already in the concept phase.

[Rz 44] Extraordinarily enhancing for the development of privacy protection standards even in complex police

procedures are **privacy protection audit and seal of quality**. In an independent process by an independent body and after thorough legal and technical examination it is certified that an it-product or procedure is compatible with the provisions governing data protection. It is most probable that a procedure in which several countries are participating is most successful that meets the legal requirements best. This is exactly what audit and seal certify. Federalism can be utilized for issues of privacy protection comparing competing systems on the basis of legal requirements. Security and product profiles are developed within the procedure whose criteria are generally to be taken into account for it-products or procedures in specific areas of use. Up to now a formal audit and seal procedure only exist in Germany and exclusively in Schleswig-Holstein. Police procedures have not yet been subject of a certification. But it is possible, especially with those that are not only used by the domestic police forces but also offered to other police offices. An audit or privacy seal can be used to enhance dissemination of such programs.

4. Evaluation

[Rz 45] In Germany it is up-to-date to restrict data processing competencies of the police by limiting the period of validity of special processing rights and to evaluate their practical application. Insofar federal competition is fruitful: the intensity and depth as well as the executive distance of evaluation differ from state to state. Plurality of evaluation results renders feasible **critical questioning of evaluation** as well as of those regulations and their application that have been evaluated. Self evaluation always bears the risk of a purely affirmative evaluation. To ensure a critical examination it is necessary to commission evaluation to an independent body: for example, a scientific institution. Subject matter of evaluation are the data subjects rights, losses of effectiveness due to ambiguous competencies, and deficiencies in supervision.

5. Supervision

[Rz 46] In a police information system structured according to federal principles an effective supervision plays an important role. On the one hand it is necessary to prevent supervision-free zones; on the other hand a close **coordination and cooperation** is necessary because supervision often is spread among several supervising bodies. In Germany cooperation takes place at the conference of privacy commissioners of the Federation and the individual states. In its working group on national security, chaired by the Independent Centre of Privacy Protection Schleswig-Holstein, the necessary coordination between the Commissioner of the Federation and the state commissioners takes place. Legal competence of a privacy commissioner is distributed according to the police office that is responsible according to the provisions governing privacy protection. This kind of regulation is essential because police offices have a tendency to withdraw from effective control and do not hesitate to play supervising bodies off against each other.

[Rz 47] A specific problem of supervision in privacy protection on the European level in the field of police is the lack of competencies of the European Data Protection Supervisor; they are (still) distributed to **different supervising bodies**. Because an informational connection of European data processing is striven for, it is highly necessary to establish a uniform privacy protection control on the European level which also needs to have the competencies for supervising data processing by (European) police forces.

[Rz 48] Similar to the relationship between the Federation and the states in Germany, a working group should be established in which police experts and national data protection boards can exchange their experiences and opinions as well as coordinate their work. There are numerous **European working groups** of the police to coordinate and optimize their work. There is no reason why privacy protection should not follow this example. This is the way for privacy protection to achieve an effective federal supervision of police cooperation.

Dr. Thilo Weichert Head of the Independent Centre for Privacy Protection Schleswig-Holstein, Germany

Translation by Kirsten Bock

Rechtsgebiet: Datenschutz
Erschienen in: Jusletter 3. Oktober 2005
Zitiervorschlag: Thilo Weichert, Privacy and Data Protection in federal police cooperation, in: Jusletter 3. Oktober 2005
Internetadresse: <http://www.weblaw.ch/jusletter/Artikel.asp?ArticleNr=4271>