The effects of Europol and Schengen on data protection control over police data

The necessity of closer police co-operation in a Europe which is growing together is undisputed from the point of view of data protection law. Such co-operation requires the exchange of relevant information about people. Dr Hans-Hermann Schrader, Data Protection Commissioner for Hamburg, Germany, raises the question whether the 1995 Europol Convention actually makes possible this necessary police co-operation in a correct manner and whether the rights of citizens affected are sufficiently safeguarded. Is the 1990 Schengen Agreement's Information System a better model?

Europol centralises police records

The Europol Convention recognises only two institutions: the Europol Central Bureau and the national central bodies. But in Germany, which is a federal state, policing is not exercised centrally, but in the Länder, the federal states. There are also two police authorities at federal level, namely the Federal Criminal Investigation Agency and the Federal Border Police. The Border Police take charge of all police tasks on the borders of Germany and at travel facilities such as airports and the railways. The Federal Criminal Investigation Agency provides scientific expertise and special facilities for the support of the Länder police forces. The Federal Criminal Investigation Agency only rarely engages in police enquires itself, the exceptions being, for example, in internationally significant cases and in the area of terrorism.

In Germany, the Federal Criminal Investigation Agency is now designated as the national body - despite its limited competencies and the fact that it does not have background knowledge. The Länder police forces retain specialist competencies and also the knowledge which is of relevance for data protection law.

According to the Europol Convention, access by the Europol Central Bureau to information held by the police forces takes priority over all other aspects of national law including aspects of data protection law. It should no longer depend on whether the police responsible for a case consider passing on information to the national central body to be necessary and whether this transfer is permissible in national law. The responsible police authority is, indeed, not even asked. If the national law stands in the way, it must be changed. Only the informational requirement of Europol counts, and this requirement has to be satisfied by the national bodies.

Responsibilities under data protection law divided

This centralist point of departure for arrangements on the information flow between the police authorities and Europol gives rise to the fear that a substantial deterioration is taking place for the protection of the rights of persons who are affected by the information.

As the law has been up to now, the competent police authority decides which information on a case it stores in supra-regional police information systems. It has comprehensive knowledge of the case and is in possession of the documentation. It learns directly of decisions of the state prosecutor and the courts, which are of importance for erasure or correction of the stored data. The data stored in a supra-regional unitary system are inspected by the Data Protection Commissioners who are responsible for the police forces which have carried out the storage. Legal actions are admissible at the courts which are competent for the police authorities organising the storage. Therefore, the expert competence and the data protection responsibilities are aligned.

However, the Europol Convention separates the responsibility for data protection from the police competence. In cases of prosecution and preventing dangers, the relevant police forces remain responsible, as previously. On the other hand, the data input in the Europol information system is carried out only on the basis of what Europol holds to be necessary. This means that the connection is broken between the case which led to the data input and the actual storage.

The example in the box (on the next page) makes it clear that the implementation of data protection rights - here of the right for data to be erased - depends above all on the body which enters the first data records remaining responsible for all further steps up to and including erasure. The centralist approach of Europol neglects this

Mr. A is innocent but what about his police record?

On the occasion of a cash transfer to France, whose background seems dubious to the bank and also to the prosecuting authorities in Hamburg, Mr. A comes under suspicion of money laundering. Mr. A is recorded by the Hamburg police in the information system as a suspect in accordance with the regulations of the Europol Convention.

In the course of further investigations by the authorities in Hamburg, the suspicion of money laundering held against Mr. A is completely dispelled; his cash transfer was fully legal. The Hamburg police receive this result of the proceedings and immediately conscientiously erase the data about Mr. A both in the information system in Hamburg and in INPOL. It has then erased all the data input that it has made itself. The Federal Criminal Investigation Agency learns nothing of this result, nor does it notice the erasure because the erasure has been carried out by the police in Hamburg directly. The Federal Criminal Investigation Agency has also no cause to concern itself with the data record because only Hamburg had been responsible for the case.

The data record at Europol, therefore, remains intact, although its raison d'être - the suspicion against Mr. A - has ceased to exist. Europol has no reason to erase its record on Mr. A because it has no information about the case and its further development, apart from the original data record.

principle. It authorises the national bodies and, in particular, Europol itself to engage in far-reaching measures of data processing without assuming the corresponding responsibilities. This can be in the interests neither of European police co-operation nor of the citizens affected. And the problem does not exist only in federal states such as Germany, but in all Europol member states.

The competent police force does not have the possibility of examining and deciding which data it considers to be necessary for further analyses and correspondingly for data transmission. Neither can it check the analysis itself because it no longer receives access to the data once it has delivered this data to its national body. Consequently, it is precisely information about victims and witnesses, i.e. information relating to serious violations of the rights of those affected, which is removed in the most far-reaching manner from the legal scope of data protection. The evaluation is carried out by Europol alone.

Effectiveness of data protection control weakened

This structure of the informational relationships between the competent police authorities and Europol aggravates very seriously effective data protection control.

Working on the basis of the arrangements provided for in the Europol Convention, I cannot establish from the police in Hamburg which data from Hamburg has been transmitted to Europol and is kept there. For, contrary to the case of the federal-wide unitary files, the police in Hamburg do not enter the data itself; rather, the Federal Criminal Investigation Agency transfers data on the basis of its obligation (according to Article 4 Clause 4 Numbers 1 and 2). The Federal Data Protection Commissioner responsible for the Federal Criminal Investigation Agency can, if necessary, reconstruct the individual transmissions to Europol - provided that a record of these has been made at the Federal Criminal Investigation Agency. But the Commissioner does not have the necessary documents, and in particular does not have the documents to be able to establish whether the prerequisites, (for example, according to Article 8), have been complied with.

The same applies to the joint data protection control authority according to Article 24. This organisation can, if necessary, inspect the individual data in the Europol Information System, but does not have any detailed information on the cases because this information is stored only with the police forces responsible for the investigations.

Alternative proposal that improves data protection

As I draw attention to these inadequacies of the Europol Convention, I should like to sketch at once an alternative which does justice to data protection and which would not involve any disadvantages for necessary police co-operation.

In this scenario, the responsible state (Land) police authority would decide itself whether, in accordance with the Europol Convention, it would transmit certain information to Europol. This could take the form that within a specific pool of information it would assign a particular code for all cases which were designated for storage with

Europol. The data would be automatically transmitted from this information pool to Europol. As corrections and erasures became necessary, the same procedure would apply: the police force with a duty to erase would give an erasure command into the national file, which would be transmitted automatically to Europol.

The responsibility of the competent police force in data protection law would thereby remain fully maintained. The responsible police authority could also judge fully when information was updated whether data records still existed at Europol. If the data record also affected other member states, agreement with the other police authorities would be both necessary and possible.

This model corresponds in essentials to the Schengen information system procedure. It is achievable. It should be striven for because the arrangements of the Schengen Agreement which are positive for data protection law are, in terms of end results, also achieved for the Europol procedure.

Despite the weaknesses of the convention, I hope that domestic safeguards are still possible which would enable an approach that does justice to the requirements of data protection law. The fear is that the Länder police forces will be able to obtain data from the Europol Information System but have no responsibility under data protection law for data records, corrections and erasures.

At present, then, it is not possible for the point of view of data protection law to give a positive judgement on Europol. Instead, the Data Protection Commissioners of the Federal Government and of the Länder in Germany must still apply massive pressure for improvements.

This report by Dr Hans-Hermann Schrader, Hamburg's Data Protection Commissioner, is based on his presentation at the Privacy Laws & Business Data Protection Authorities' workshop, *Data Protection and the Police,* held in Copenhagen, Denmark, September 5th, last year.