

Germany
The Federal Data Protection Commissioner

Annual Report 2003/2004
of the Federal Commissioner for Data Protection
(Excerpt)

1	Introduction - Overview and Outlook —	4
2	Legal framework for data protection	8
2.1	Further development of data protection law.....	8
2.4	Strengthening the position of data protection officers in public authorities	10
3.1	The increasing importance of European legal instruments and their impact on data protection	12
3.2	Priorities in the European discourse on data protection.....	14
3.2.1	The Article 29 Working Party provided for in the EU Data Protection Directive	14
3.2.4	Safe Harbour Review	15
3.2.5	Data protection in the Council of Europe.....	17
3.3	Intensifying law enforcement cooperation in Europe.....	18
3.3.1	Europol	18
3.3.2	Schengen.....	19
3.3.3	Customs File Identification Database (FIDE) of the EU Member States	24
3.3.4	Improving the exchange of information within the European Union to fight crime and terrorism.....	25
3.3.5	Council Directive on the obligation of carriers to communicate passenger data	27
3.3.6	Interpol: Creating a DNA database	28
6	Internal administration; statistics.....	31
6.1.4	Should data of nationals of a EU Member State be included in the Central Aliens Register?	31
6.1.5	Eurodac — a successful undertaking?.....	32
6.2	Biometrics in identity documents	34
6.2.1	EU Regulation on standards regarding passports and travel documents.....	36
6.2.2	New techniques employed by <i>Bundesdruckerei GmbH</i> for producing passports.....	38
6.2.3	Biometric features in visas and residence permits	39
7	The Judiciary.....	42
7.1.1	Federal Constitutional Court decision of 3 March 2004	42
7.3.2	Should genetic fingerprints be treated as equivalent to conventional fingerprints?	44
7.9	European Cooperation in Criminal Matters	47
	Eurojust.....	47
7.9.2	Latest developments	48
11	The Private Sector.....	51
11.4	The SCHUFA is expanding its field of activity	51

11.5	Scoring and rating methods – Star-gazing instead of hard facts?.....	53
11.5.1	How the SCHUFA determines credit ratings	54
11.5.2	Use of credit ratings by telecommunications companies and Article 6a of the Federal Data Protection Act	54
13	Telecommunications and teleservices	57
13.1.1	To retain or not to retain data for possible future use?.....	57
13.2	How telecommunications companies handle personal data.....	59
13.2.1	Saving text messages for billing purposes.....	59
13.2.2	Location-based services.....	60
13.2.3	Retention periods for traffic data under the German Fiscal Code	61
13.2.4	Not all customers are happy with “Happy Digits”	62
13.2.5	New service feature to block unwanted telephone calls.....	63
13.2.6	Access to customer data in Deutsche Telekom’s T-Punkt sales outlets.....	64
13.2.7	Making court judgements anonymous when used in a civil case	65
13.2.8	Extent of the right to information according to Article 34 of the Federal Data Protection Act.....	66
13.8	Spam without end?.....	69
13.9	Google’s new e-mail service and other business ideas	71
14.1	Data transmission abroad	73
14.1.1	US authorities demand prior transmission of parcel data.....	73
14.1.2	Item data in foreign accounting centres.....	74
22.2	The transparent passenger	76
27.3	The International Conference of Data Protection and Privacy Commissioners.....	78
27.4	Organization for Economic Cooperation and Development (OECD)	80
28.2	The Data Protection Commissioner on the Internet.....	81

1 Introduction - Overview and Outlook —

The search engine Google gives more than 30 million results for the German keyword "*Datenschutz*" while more than 430 million results are obtained for the English "*privacy*". Thus there would seem to be little doubt that protection of personal data has by now become established both in Germany and at the international level. Moreover, since the so-called Population Census Decision, pronounced by the Federal Constitutional Court (*Bundesverfassungsgericht, BVerG*) more than twenty years ago [in 1983], it has clearly emerged that data protection, as the individual's right to determine the use of his/her personal data, is one of the basic constitutional rights.

Nevertheless, it is sometimes suggested that data protection is a troublesome and bureaucratic perfunctory exercise hampering and preventing appropriate solutions. Time and again, the demand is put forward that the scope of data protection should be restricted in the interest of allegedly more important legal rights, such as security, freedom of science and research, and tax equity. In a number of areas, the focus has in fact shifted significantly from data protection to other areas, especially crime control and law enforcement and fiscal administration and the social system.

During the period covered by the report, it was again the Federal Constitutional Court which, in a number of decisions, strengthened the fundamental right to determine the use of one's personal data and thus provided an important new orientation in this context. A particular case in point is the Federal Constitutional Court Decision on Acoustic Surveillance of private homes (referring to the so-called "large-scale eavesdropping operation") of 3 March 2004, which calls for continued full protection of an inviolable core of the private against any surveillance whatsoever; this implies the exclusion also of considerations of usefulness as a reason warranting any such operations. As in the case of the "Census Decision" of 1983, a number of views expressed in the course of the related debates are obviously aimed at playing down the Court's decision on acoustic surveillance. Thus the argument is put forward that the decision only had implications regarding acoustic surveillance of private homes, but did not refer to other powers regarding covert data collection, e.g. for tapping telephone lines. However, another Federal Constitutional Court decision of the same date established that the principles laid

down in its Decision on Acoustic Surveillance shall also be complied with as regards the authorization of the Customs Criminologic Office (*Zollkriminalamt, ZKA*) to carry out preventive interception of communications. At an academic colloquy organized by my agency, the attending experts agreed that a "restricted solution" was not sufficient, i.e. that all other powers regarding covert data collection should be reviewed and tested as well (see No. 7.1 below).

As already envisaged during the legislative procedure, a review is also needed of the powers assigned to the public security organizations after the terrorist attacks of 11 September 2001. In this context, I consider it good practice that the criteria underlying the review and its findings be made available to the public in order to ensure that the forthcoming political debate will take place on the basis of substantiated and verified findings. This is of particular importance because a decision will have to be made on infringements of fundamental rights, which may be introduced or continued only in compliance with the constitutional principle of proportionality (see No. 5.5.4 of the German report).

Technological innovations, especially as regards location technology, data transmission and image recognition, have in the period under review advanced to such a point that the new services and techniques deriving from these innovations will soon be introduced and/or implemented on a large scale: mobile communication location techniques provide for location services which not only entail greater convenience and allow introduction of new business models, but also allow tracking and registration of the whereabouts and movements of persons. Biometrics can be applied both in the private and the public sectors for facilitating identification of persons. However, these techniques can also be used for covert surveillance of individuals. Regrettably, the development of technological instruments available to individuals for their personal protection against surveillance has not kept up with that of surveillance technologies. Consequently, even greater importance attaches to the need - already identified in the amended Federal Data Protection Act of 2001 - to include data protection aspects already in the stage of developing and designing new systems. Apparently, however, not all of those involved are yet aware of this need. Thus I found that, even for a large-scale project like the change-over from unemployment assistance and social assistance benefits to the combined system of so-called

"unemployment compensation II" (*Arbeitslosengeld II*), fundamental data protection requirements were not included in the system design (see No. 16.1 of the German report).

Also, the new findings obtained by human genome research and the resultant possible applications are of essential importance. A person's identity and parentage as well as information on personal traits and features and susceptibility to diseases can be established on the basis of DNA analysis. In this respect, the controversies concerning the use of DNA as the "fingerprint of the 21st century" and the admissibility of paternity tests obtained without the other parent's knowledge and consent only reflect the beginnings of the radical changes entailed by these new findings. The resultant issues reach far beyond codified data protection law. The developments and decisions to be expected in the years before us will show whether the right to personal privacy can be safeguarded in view of these qualitative innovations (see No. 7.3 below).

It is a regrettable fact that, during the period under review, little progress was made in data protection legislation. Drafting and/or adoption of the Data Protection Audit Act required for implementation of the 2001 Federal Data Protection Act, the Data Protection Act regarding Employees and Wage-Earners, which has long been requested by the German *Bundestag*, and the urgently needed Gene Diagnostics Act continue to be put off, and the announced basic modernization of data protection legislation has come to a halt. Encouraging results were obtained only in a number of special regulations — e.g. the data protection provisions relating to the health insurance chip card. Against this background, I welcome the announcements by the German *Bundestag* that it intended to initiate parliamentary action on important issues of data protection, as was already manifested in the case of the Freedom of Information Act which is closely related to data protection issues (see No. 2.7 of the German report).

There has been a marked increase in transnational data processing and, in particular, in data transfer operations among the present number of 25 EU Member States. While the EU Data Protection Directive has by now been enacted in national law by all Member States, this Directive does not apply to the processing of personal data in the security domain. If law enforcement authorities are to co-operate more intensively and are also to exchange personal data without regard to national borders, as was decided under the Hague Programme, data protection must be raised to a common European standard in this

area as well. This must be based on the fundamental data protection rights guaranteed under the EU Charter of Fundamental Rights and included, without modification, in the draft European Constitution (see No. 3.3 below).

The period under review covers about half of the term of office of my predecessor Dr. Joachim Jacob whom I once more thank for his excellent work. On 17 December 2003, I was appointed Federal Commissioner for Data Protection (*Bundesbeauftragter für den Datenschutz*). Of course I am fully responsible for the present annual progress report. It should be noted that the reported activities - notwithstanding the "first-person" presentation - were, for the major part, carried out by my staff. My thanks also go to these staff members for their great commitment and successful work. Finally, I wish to thank the delegates of all parliamentary groups of the German *Bundestag* who have taken a sustained interest in, and been fully committed to, data protection, and the representatives of public and private agencies, for whom data protection is a prerequisite for successful action.

Peter Schaar

2 Legal framework for data protection

Effective data protection requires a legal framework that clearly describes the extent and limits of all permissible data processing and defines the rights and obligations of all those involved. Due to rapid technological progress and the emergence of new problem areas, this must be understood as a dynamic process of continual change which demands constant adjustment of existing laws in order to keep up with new developments and insights and close any remaining or emerging regulatory gaps. This is not about excessive regulation, but rather about comprehensively modernizing data protection law in order to arrive at efficient and unbureaucratic solutions.

Held at the start of the 15th legislative term of the German Bundestag, the conference of federal and state (*Land*) data protection officials adopted a resolution making a number of demands of the Federal Government and federal lawmakers (see box to No. 2, annex 12) in order to point out the need for reform on data protection and to push for legislative action.

2.1 Further development of data protection law

The second phase of data protection reform has come to a standstill.

Already while preparing the amended Federal Data Protection Act of 2001, the Federal Government announced a second phase of data protection law reform intended to prepare the way for modern and innovative data protection. A comprehensive report commissioned for this purpose contained a large number of excellent recommendations and suggestions (see 19th Annual Report, No. 3.3). Although the Bundestag repeatedly indicated its support for this reform project (at times with an impressive majority) (Resolution on the 18th Annual Report, Bundestag printed paper 14/9490 No. 2; Decision *Umfassende Modernisierung des Datenschutzrechts voranbringen* (Advancing comprehensive modernization of data protection law), Bundestag printed paper 14/9709; Resolution on the 19th Annual Report, Bundestag printed paper 15/4597 No. 1, box to No. 2.1), and although the reform is also an item in the coalition agreement for the 15th legislative term, the Federal Government has not yet presented draft legislation to

this effect. It is therefore all the more important that action should now be taken with alacrity.

An important first step towards modernizing data protection law, and one also recommended by the report, would be compiling the almost overwhelming number of special regulations within a new, clearly structured and easy-to-understand data protection law. In addition, the growing number of large-scale data collections in private hands, the increasing links between them, and new technological developments are pushing existing data protection law to its limits and making new legislative action necessary.

For this reason, I find the delays in reforming data protection legislation extremely regrettable. Particularly in this area, constant development and adaptation to the rapidly changing situation are essential; correcting errors once they have occurred is possible only with great difficulty. And the longer the reform of data protection law is put off, the greater the legislative effort needed to accomplish it.

2.4 Strengthening the position of data protection officers in public authorities

Data protection officers in public authorities are often unable to perform their required duties optimally because they are not given enough time off from their regular duties.

The amended Federal Data Protection Act of 2001 requires every federal agency to designate a data protection officer (see the 19th Annual Report, No. 3.2.5); this officer has a number of important responsibilities to ensure comprehensive data protection in the interests of agency staff and the public. Officers' continuous activity is an especially important contribution to implementing data protection regulations and principles. This is why I continued to promote their efforts during the period covered by this report. In this regard, a central problem that comes up again and again is the fact that, unlike the legislation governing equal opportunity officers and members of staff councils, the Federal Data Protection Act makes no specific provision for freeing such officers from their regular duties. As a result, many data protection officers must perform the duties required of them by the Federal Data Protection Act in addition to their regular tasks, which does not leave them enough time to sufficiently fulfil all the requirements of this office. Lawmakers therefore need to remedy this situation immediately with an appropriate regulation. In a public agency with several hundred staff and extensive electronic data processing operations, either the position of data protection officer should be full-time, or the necessary support staff should be provided in accordance with Section 4f para. 5 first sentence of the Federal Data Protection Act. Despite the lack of such a regulation, I have noted recently that some federal ministries have undertaken efforts to this effect. It would also be desirable if the data protection officers in the supreme federal authorities could assume a kind of supervisory and coordinating function for their colleagues in the subordinate agencies. Here, too, some ministries have set a positive example, although it is unlikely that all other agencies will follow suit unless required to do so by law.

During the period covered by this report, I also continued the experience-sharing measures I initiated with data protection officers of the supreme federal authorities. We were able to discuss the situation of data protection officers within their various agencies, problems of data protection law, developments of general interest and specific individual

questions in greater detail at events held in March 2003 and January 2004 and at a special meeting on staff data protection held in summer 2004 (see No. 10.5). These forums focused on the following topics: a presentation of the “Datscha” software application for automated management of lists of data processing operations; issues related to basic and advanced training; security strategies and IT issues; the development of data protection law; private Internet and e-mail use at work; staff data protection.

These forums continue to enjoy enormous interest, which is an incentive for me to continue offering such opportunities to discuss common problems and unresolved legal issues, thereby actively supporting the data protection officers in their important work.

3.1 The increasing importance of European legal instruments and their impact on data protection

The planned European area of freedom, security and justice makes it essential to harmonize data protection also in the area of combating crime.

Creating an area of freedom, security and justice has become the top policy priority for the European Union. As part of this effort, one of the most important aims is ensuring the free flow of data within the third pillar, i.e. between Member States' law enforcement and criminal prosecution authorities. Harmonizing European data protection in this area has the same fundamental significance as the EU Data Protection Directive had for the first pillar, i.e. above all the private sector. This includes uniform legal principles, effective means of checking European information systems and a guarantee that the independent data protection authorities will be consulted when European lawmakers prepare legislation on this subject.

Already at the time when data protection within the first pillar was harmonized, the European aspect of data protection praxis took on a new quality. Key decisions can no longer be made without considering the European dimension. In future, the necessary and continuous process of adapting data protection to constantly developing information technology will largely be determined by developments at the European level.

Happily, the IT industry is increasingly willing to engage in dialogue about new products and applications already during their development, thus integrating data protection from the very beginning. I am committed to making sure this trend continues. Because the IT industry is internationally active, this discussion must also be conducted at the international level for data protection to be effective. The Art. 29 Working Party is the IT industry's most important European contact for data protection issues.

Given this background, I was happy to assume the chairmanship of the Art. 29 Working Party only a few weeks after taking up my duties as Federal Commissioner for Data Protection. Serving in this capacity brings with it enormous possibilities and great responsibility as well as significant burdens, not only for the office holder, but also for the office. During my two-year term as chair, I am responsible for achieving agreement

among 25 Member States which sometimes have very different ideas, for determining strategic-programmatic priorities and for representing European data protection within and beyond the European Union. After my first year in office, I can say that the proportion of office business related to Europe has expanded significantly in terms of both quality and quantity.

3.2 Priorities in the European discourse on data protection

3.2.1 The Article 29 Working Party provided for in the EU Data Protection Directive

The harmonization of European data protection is to be driven by a coordinated European strategy of supervision.

In a unanimous vote on 11 February 2004, the European data protection officials who work together in Brussels according to the terms of Article 29 of the EU Data Protection Directive elected me to serve as their chair. The group named Prof. José Luis Piñar Manas, head of the Spanish data protection authority, to serve as my deputy. The Art. 29 Working Party is made up of the data protection officers of the EU Member States and the European Data Protection Supervisor (see No. 3.2.3); the European Commission is also a non-voting member.

Also during the period covered by the current report, the Working Party dealt with a broad spectrum of topics and adopted 30 opinions (see box to No. 3.2.1). One major issue was the transfer of passenger name data to the US (see No. 22.2), Canada and Australia. The Working Party also gave great attention to the processing of biometric and genetic data for purposes of internal security and criminal prosecution. Communications data processing, e-government and video surveillance were also on the agenda, as were spam (see No. 13.8) and online authentication systems.

Apart from advising the Commission, one of the Working Party's key responsibilities is promoting the harmonization of data protection within the European Union. For example, it adopted an opinion on the obligation of data processors to provide information; another opinion specifies how airline passengers in the US are to be informed of their rights.

Further, in a working paper the Art. 29 Working Party agreed to do a better job of enforcing data protection regulations in certain areas using targeted checks. For example, sectors in which especially sensitive personal data are processed and those with a particularly high rate of complaints are to be inspected. Such Europe-wide inspections are also intended to increase responsible authorities' familiarity with the applicable regulations and data subjects' awareness of their rights. Through coordinated control

mechanisms, harmonization is likely to significantly improve enforcement of national law and the prosecution of violations.

The outstanding event during the reporting period was the entry of ten new Member States on 1 May 2004. Prior to that, the new members already had the option of attending the meetings of the Art. 29 Working Party as observers. EU enlargement provided a reason for the group to clarify its mission. It produced a strategy paper defining its future areas of concentration and describing its relationship to its various contacts in society. Not least, the strategy paper aimed to make the Working Party's activities more transparent and invite all interested parties to engage in a dialogue (Doc. 11648/04 of 29 September 2004, WP 98; see box to No. 3.2.1).

The Working Party usually has two-day meetings in Brussels five times a year; its work is supported by subgroups. During the reporting period, subgroups were active in the following areas: the Internet, passenger name data and binding guidelines for companies.

3.2.4 Safe Harbour Review

The European Commission found shortcomings in compliance with the Safe Harbour principles. The impact of legislation passed in the wake of the Sept. 11, 2001, attacks on the Safe Harbour framework has not yet been assessed.

Initiated by the United States (for more on the US, see No. 27.2 below), the special agreement with the EU to ensure an appropriate level of privacy for data transmitted from the EU to the US ("safe harbour") went into effect on 1 November 2000 following the decision of the European Commission on 26 July of the same year (see the 18th Annual Report, No. 2.2.2; see box to No. 3.2.4 for more on how Safe Harbour functions). Before that, in its resolution of 5 July 2000, the European Parliament had called on the Member States and the Commission "to review [its future] decision in good time in the light of experience and of any legislative developments". As a result, the Commission inserted a clause to this effect (Art. 4 para. 1) in its decision – to the great satisfaction of the Art. 29 Working Party (see No. 3.2.1). The Commission's initial assessment of the Safe Harbour arrangement in early 2002 found problems with the response of the US private sector and a widespread lack of transparency (see the 19th Annual Report, No. 3.7).

To fulfil the European Parliament's demand to review the Safe Harbour agreement within three years of its entry into force, in autumn 2003 the Commission charged an international team of experts to conduct a study of its implementation during the period from 1 November 2000 to 1 November 2003, which would serve as the basis for the Commission's Safe Harbour review. The team presented its comprehensive study – nearly 300 pages including annexes – to the Commission on 19 April 2004, which based its evaluation on this study, along with its own experience and research. The Commission presented its evaluation on 20 October 2004 in the Commission Staff Working Document: The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (SEC (2004) 1323).

The main conclusions of the Commission's review were as follows:

Although the number of American companies participating in the Safe Harbour programme is quite small, it has been steadily increasing: from 300 companies in 2002 and 400 in 2003 to 600 by the time the review went to press.

Many of the companies which self-certified to join the Safe Harbour programme have either not published a privacy policy or have published a policy that is not compliant with the Safe Harbour principles. This caused the Commission to make a number of suggestions to the US Department of Commerce and the Federal Trade Commission (FTC). Because interested companies may join the programme through self-certification without further verification, the Commission called on the Department of Commerce and the FTC to be more active in examining and monitoring compliance in order to detect and exclude participants whose privacy policies are insufficient.

Although the Commission was aware of no complaints that the companies concerned had not addressed to the satisfaction of the affected parties (see the 19th Annual Report, No. 3.7), which may be regarded as a positive sign, neither companies nor data subjects have yet contacted the EU Panel.

An important task will be to assess the impact of the US Patriot Act and other US legislation passed in the wake of the attacks of Sept. 11, 2001, on the Safe Harbour arrangement and to determine whether they affect the level of data protection.

The Safe Harbour Decision Implementation Study is available at the Commission's website: http://europa.eu.int/comm/internal_market/privacy/index_en.htm.

3.2.5 Data protection in the Council of Europe

The Council of Europe Data Protection Convention has now been ratified by 25 countries.

Following the entry of Monaco and Serbia-Montenegro, the Council of Europe now has 46 members. Twenty-five countries have now ratified the Council of Europe Convention 108, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 1981.

An additional protocol obligates parties to the Convention to improve the possibilities for applying the Convention's principles using two substantially new mechanisms. First, parties to the Convention are required to set up independent supervisory authorities with powers of investigation and intervention, as well as the power to engage in legal proceedings or bring violations to the attention of the competent judicial authorities. Second, the protocol introduces regulations modelled on the EU Data Protection Directive regarding transborder data flows with countries that are not signatories to the Convention. After ratifying legislation went into effect in Germany (Federal Law Gazette II 2000 p. 1882) and five other countries on 1 July 2004, thus providing the necessary quorum of at least five ratifications, the additional protocol also entered into force on this date.

The Data Protection Convention and related recommendations and reports are available in English and French at http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/.

3.3 Intensifying law enforcement cooperation in Europe

3.3.1 Europol

3.3.1.1 Amending the Europol Convention

The Danish initiative to amend the Europol Convention has not yet entered into force.

In my 19th Annual Report, I reported on a Danish initiative calling on the Council to draft a protocol amending the Europol Convention (see No. 16.1). From its advisory and supervisory activities, the Joint Supervisory Body is aware how important such an amendment would be for Europol's future activities. Nonetheless, the Council has made only one basic policy decision on accepting the Danish initiative, which reservations on the part of national parliaments prevented from entering into force. The Federal Ministry of the Interior has so far only drafted a proposal for ratifying legislation.

3.3.1.2 Activities of Europol's Joint Supervisory Body

The Joint Supervisory Body published its first Annual Report covering the period October 1998 to October 2002.

In its initial phase starting in 1999, the Joint Supervisory Body (JSB) dealt primarily with issues of application and interpretation; in the meantime, its supervisory activities have increasingly come to the fore. For example, the JSB carried out a number of site visits of Europol in which representatives of my agency also participated. During the first of these visits, the emphasis was on advising and supporting Europol in building its information and communications system. This system is very complex, as Europol is responsible not only for carrying out its own in-house analytical activities (see Art. 10 of the convention), but also for operating a European Information System (EIS) on behalf of the Member States, in accordance with Art. 8 of the Convention. As Europol's case analysis has intensified, the JSB's supervisory activities have increasingly expanded to include this area. Its results show that although the Member States are providing Europol with more data for analysis, they are sending this material largely without preliminary analysis by the national agencies which deliver it. In the interest of efficient analysis, however,

information and its sources to be examined should be checked first for authenticity, reliability, etc. in order to avoid collecting useless data.

The ten new Member States that entered the EU on 1 May 2004 will also be contracting parties of Europol as soon as they have ratified the Europol Convention. As appropriate data protection in the area of law enforcement is a prerequisite for joining the Convention (see Art. 14 of the Convention), the JSB used a questionnaire and follow-up discussions to inform itself regarding the status of data protection in the new Member States. In the meantime, most Member States have ratified the Europol Convention. Enlargement presents a new organizational challenge to the JSB, now that as many as 50 representatives attend its meetings.

During the period covered by this report, the committee responsible for dealing with complaints was able to resolve two more legal proceedings (see the 19th Annual Report, No. 16.1). Especially significant is the decision that Europol must respond to a data subject's request for information in accordance with Art. 19 of the Convention in the language of the request, if this is one of the EU's official languages. Prior to that, Europol had conducted all its correspondence in English; for petitioners who do not speak English, this was tantamount to being excluded from the possibility of legal recourse.

3.3.2 Schengen

3.3.2.1 SIS II — Will the Schengen Information System continue to be simply a file for wanted notices?

Key data protection issues concerning the expansion of the Schengen Information System remain unresolved in the wake of European Union enlargement.

One example of the apparently mostly uncoordinated efforts in creating cross-border communications networks among security authorities is the development of a second-generation Schengen Information System (SIS II) (see the 19th Annual Report, No. 16.2.1).

The original SIS has a maximum capacity of 18 participating countries; this capacity will be reached with the planned partial inclusion of the UK and Ireland and the association

with Switzerland in 2006. The ten new Member States are also required to join SIS. The possible entry of Romania and Bulgaria would bring the number of SIS participants up to 30 in the near future; this is more than the current system can handle.

However, increasing the capacity of this Europe-wide database of missing and wanted persons, containing more than 12 million data records, is only one issue. Another is updating the system, which was first developed 15 years ago. Further, the already-approved European Arrest Warrant (see No. 7.9.2) is to be integrated into the SIS technology. And implementing law enforcement demands (especially since Sept. 11, 2001) for new functionalities such as biometric features and expanded access would be problematic in terms of data protection law, because doing so would change the nature of the system: It would no longer be a law enforcement database in which officers can search for responses to their queries, but a comprehensive system of law enforcement information that the JSB and the national data supervisory authorities would have a hard time overseeing due to its complexity. Further, the question of responsibility for such a Europe-wide database would also have to be resolved.

The Council took an initial step in this direction with its Regulation (EC) No 871/2004 of 29 April 2004 (Official Journal of the EU, L 162, p. 29), which among other things creates the legal prerequisites for giving Europol and the national members of Eurojust limited access to SIS. However, the regulation cannot be applied due to reservations on the part of one national parliament, which had not yet been dealt with at the time this report went to press.

Like the European Parliament, the JSB became involved in the preparations for SIS II at an early stage. On 6 October 2003, the responsible EP committee held a symposium at which the responsible EU Commissioner and respected data protection experts presented their views on a future SIS. In a detailed opinion, the JSB, which has been consulted on the development of the SIS only sporadically, pointed out the possible threat to civil liberties posed by gradually expanding the existing SIS into a Europe-wide law enforcement information and search system. In particular, the JSB criticized the fact that the Commission was pushing ahead with development in the absence of a fundamental policy consensus on the tasks and purpose of the SIS II, creating facts on the ground in terms of information technology before European lawmakers could create the necessary

legal basis with an amendment to the Convention Implementing the Schengen Agreement. Another problem is the general lack of sufficient data protection within the EU's "third pillar". I have forwarded this document, which was produced for the European institutions, to the responsible committees of the German Bundestag and the Federal Government.

I expect the Federal Government to work at the European level to ensure that further development of the SIS strictly complies with data protection law and that the necessary legal framework is amended with the aim of strengthening civil liberties.

The recommendations can be found at www.bfd.bund.de (in German only; keywords "Europa/Internationales").

3.3.2.2 Supervising compliance with Art. 96 of the Convention Implementing the Schengen Agreement

Alerts regarding third-country nationals for the purpose of refusing entry make up the largest share of SIS alerts regarding persons. The JSB carried out a joint inspection of these alerts in the Member States.

Due to reports of possibly impermissible alerts, the JSB and the contracting parties to the Convention agreed to check alerts under Art. 96 of the Convention. As a first step, Member States were asked to complete a questionnaire on the use of Art. 96 alerts in their country.

For Germany, the Federal Ministry of the Interior's response provided the following picture: At the time of the survey in late summer 2003, out of a total of 800,000 alerts entered by Germany in the SIS, 270,000 were Art. 96 alerts. Germany thus issued the second-largest number of such alerts after Italy. By far the largest proportion of Art. 96 alerts were those issued under para. 3, that is, refusal of entry by the responsible foreigners authorities of the German states (*Länder*). A small proportion was issued (usually by the Federal Border Police) under para. 2, i.e. based on a threat to public policy or public security or to national security. At the time of the survey, the Federal Ministry of the Interior asked me to postpone the actual check until after EU enlargement on 1 May

2004, because roughly 60,000 alerts regarding third-country nationals would be deleted on that date, as these persons would then be EU citizens.

The second step began with the random selection of Federal Criminal Police (BKA) data files to be examined. The state commissioner for data protection then examined the roughly 400 files selected (approximately every 500th file) either in paper form or on site at the foreigners authorities. Only nine files concerned alerts according to Art. 96 para. 2 issued by the Federal Border Police. One result can be summarized as follows: The decision required by Art. 96 of the Convention was usually documented in the file.

All the files examined dealt with third-country nationals. Data of persons from the new EU Member States were immediately deleted.

In most of the cases examined, the alert was based on an unappealable expulsion or deportation order; in as many as 20% of cases, however, persons had been entered into the SIS only for the purpose of determining their current whereabouts, which does not justify an alert.

In many cases, there was no record of a review as mandated by Art. 112 para. 1 of the Convention to determine the need for continued storage of personal data, which could therefore not be checked. The documentation often consisted only of a BKA notice of extended storage without an independent decision by the person responsible for handling the case.

Due to a lack of documentation, it was often impossible to determine how long an alert had been in effect; this is a serious shortcoming. When first issued, an alert may remain in effect for a maximum of three years but may be renewed if the purpose for which it was issued remains in effect. In some cases, alerts had remained in effect for up to nine years.

In nearly 50% of cases, the time limit for the alert in the SIS was linked to a permanent national ban on entry according to Section 8 para. 2 of the Foreigners Act; in the remaining cases, the alert was issued for a limited period of time in accordance with Art. 112 of the Convention.

Deleting the alert in the SIS did not always entail deleting the records on which it was based. In many cases, these were kept on file to document the Inpol alert.

Overall, this check at the national level revealed some – in some cases serious – shortcomings with an adverse effect on the rights of the persons concerned. The security task force of the federal and state commissioners for data protection has founded a working group to deal with the results of this study.

Once the national-level checks have been completed, the JSB will assess the results from all the Schengen countries and decide on further measures as needed. At the time this report went to press, the JSB had not yet finished its assessment.

3.3.2.3 Multilateral convention on law enforcement cooperation with Austria and the Benelux countries

Germany, Austria and the Benelux countries are planning a broad convention on law enforcement cooperation.

Since 2003, Austria, Germany and the Benelux countries have been conducting negotiations on a convention to increase law enforcement cooperation, particularly with regard to terrorism, cross-border crime and illegal immigration (Schengen III). Even the first draft treaty contained far-reaching regulations governing cross-border cooperation. I became involved in the negotiations around the end of 2004.

By that point, the original draft had already been watered down considerably. For example, the plan was then to limit mutual access to fingerprint and DNA data to showing only whether such data were on file in what is known as a hit/no-hit inquiry: Fingerprint or DNA data is checked against the database to see whether any matching records exist. If a match is found, the next step is to determine in the process of mutual assistance whether providing additional information on the subject is permissible. Here I recommended that access to DNA and fingerprint data should be allowed only for the purpose of identifying evidence; otherwise, if partner countries had access to data files containing subjects' personal information, they would already have this information before it was possible to determine in the process of mutual assistance whether providing such information was

permissible. Access to the above-mentioned databases should remain limited to designated national contact points.

In view of its scope, I find the draft convention's new provision on comprehensive mutual access to records of motor vehicle registration to be unreasonable, because it is to be used among other things for prosecuting traffic violations. I also have serious reservations about a so-called release clause in the draft which allows access to read and modify records to be extended to other suitable data collections. I see no need for this, because in addition to the draft convention's planned links between fingerprint and DNA databases, we already have the SIS for EU-wide alerts and the European Information System (EIS) which is currently being built up as a Europe-wide database of criminal records based at Europol. As a result, additional Europe-wide data collections do not seem necessary for law enforcement cooperation. On the other hand, I am pleased that the draft convention contains a data protection clause which explicitly treats the inalienable rights of data subjects, comprehensive record-keeping and data protection supervision.

Negotiations on the convention were still under way at the time this report went to press.

3.3.3 Customs File Identification Database (FIDE) of the EU Member States

So far, the national customs authorities make only limited use of the Customs Information System (CIS). Germany is the only EU Member State to have ratified the FIDE Protocol.

The EU **Customs Information System (CIS)** consists of two databases, one falling within the framework of European Community actions, and the other falling under inter-governmental action; both have been in operation since 24 March 2003 (see box to No. 3.3.3, see also the 18th Annual Report, No. 7.9, 13.4). Both databases, which are logically separated from each other, are managed by the European Anti-Fraud Office of the European Commission. During the reporting period, Commission representatives were available to provide further information to the Joint Supervisory Authority responsible for ensuring compliance with data protection law. Although the CIS is currently in operation, it is rarely used by the national customs authorities. For example, as of early December 2004, only about 135 alerts had been registered in the system. The Commission attributes this low take-up to the large number of existing databases for customs purposes. The

Commission has started a campaign to inform potential users about the system and its advantages. I also see this as an indication that constantly creating new tools, authorities and databases with sometimes overlapping tasks does not necessarily result in greater security or more efficient job performance.

Germany joined the CIS Convention on 30 April 2004, after the CIS implementing legislation, to which I had raised no objections, went into force on 1 April 2004.

The Customs File Identification Database **FIDE** (see the 19th Annual Report, No. 16.3.1) is intended to complement the CIS, which is purely a system for issuing and disseminating alerts. FIDE offers the national customs authorities additional data categories and the capacity to conduct customs and criminal investigations. Its legal basis is a protocol in accordance with Art. 34 of the Treaty on European Union amending the Convention on the use of information technology for customs purposes. Germany is so far the only EU Member State to have ratified the FIDE Protocol. The necessary technology for FIDE is still being developed. In 2004, the Commission asked the Member States to inform it of their specific needs; the Federal Ministry of Finance formulated the German response. The Commission plans to expand FIDE to the area covered by the European Community database. However, it should be noted that the EU agencies have no authority to prosecute customs-related crimes. Further, expanding the application of FIDE as planned still requires a legal basis. The Commission has not yet specified a date for when FIDE is to go into operation. I will monitor further developments carefully.

The Joint Supervisory Authority had planned an initial check of CIS compliance with data protection law in November 2004, but this had to be postponed due to unresolved organizational issues.

3.3.4 Improving the exchange of information within the European Union to fight crime and terrorism

Improving the exchange of information between Member States' law enforcement authorities is tenable only if data protection is guaranteed.

To aid Europe's progress towards becoming an "area of freedom, security and justice" (Art. 29 para. 1 of the EU Treaty), new initiatives were started in 2004 with the aim of

intensifying the exchange of information between security authorities in the Union, raising considerable issues of data protection. The most important of these initiatives were the following:

a Draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, in particular as regards serious offences including terrorist acts (known as the Swedish Initiative, Council Doc. 10 215/04 CRIMORG 46); and

a Commission proposal for a Council Decision on the exchange of information and cooperation concerning terrorist offences (Doc. 8200/04 JHA 109).

The Federal Government asked me to participate in preparing the German response to the draft proposals. I pointed out that more was at stake than simply creating individual legislation regarding the exchange of information; rather, what is needed is a comprehensive data protection strategy for the EU's third pillar (law enforcement and judiciary cooperation in the EU).

In November 2004, I was given the opportunity to testify before a sub-committee of the European Parliament Committee for Civil Liberties, Justice and Home Affairs (LIBE). I concentrated on the Swedish Initiative in particular; in my view, a major problem is maintaining a distinction between this project and other EU legal instruments, among them the EU Convention on Mutual Assistance in Criminal Matters. Further, I pointed out the ramifications of such a framework decision for constitutional law issues. In particular, the demands of public security must be kept in reasonable relation to civil liberties, which the Member States' constitutions and the draft European constitution are supposed to protect. Finally, I stated that, in my view, creating uniform data protection regulations in the third pillar promises significantly greater chances of success than a multiplicity of individual regulations such as the draft framework decision based on the Swedish Initiative.

I recommended evaluating existing regulations to fight terrorism before making a decision on the Commission's proposal for a Council Decision on the exchange of information and

cooperation concerning terrorist offences. Further, any regulation must lay greater stress on the principle of proportionality.

Consultations on these two initiatives are to be completed by June 2005 at the latest. I will monitor further developments carefully.

3.3.5 Council Directive on the obligation of carriers to communicate passenger data

Supplementary to the Convention Implementing the Schengen Agreement, carriers are required to transmit in advance certain passenger data to the border control authorities of the relevant Member State. In contrast to the system used by the United States (Advance Passenger Information System) and the passenger data required in that context, the transfer of data within the EU is subject to much stricter regulations.

Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (Official Journal L 261 of 6 August 2004, pp. 24 ff.), which went into force in May 2004, aims at improving border controls and combating illegal immigration. To achieve these aims, the Directive requires air carriers to transmit advance information concerning passengers to be transported across the EU's external borders to the Member States' authorities responsible for border control at the request of these authorities.

During the consultations on the draft Directive, in which the Art. 29 Working Party of EU Member State data protection officials took part, it was possible to make sure that the Directive largely complied with data protection requirements: The transmission of passenger data is permissible only for the purpose of border controls and the prevention of illegal immigration. The type of passenger data to be transmitted is limited to the essential and strictly oriented to the purpose of the Directive. The length of time these data may be retained by carriers and border control authorities is also limited. Finally, carriers are required to inform passengers in accordance with the provisions of the European Data Protection Directive 95/46/EC. From a data protection perspective, the draft is thus an improvement over the procedure used by the US (see No. 22.2).

However, I would have preferred different provisions on a number of individual issues. In order to limit the number of passengers affected by data transmission to the minimum necessary, I recommended applying the Directive only to problem routes and obligating the national authorities to request data from carriers only on the basis of need as determined by a risk assessment. In my view, such restriction would have been important also because the Directive applies to EU citizens. Given the fact that the Directive is aimed at improving border controls and combating illegal immigration, it is my view that it is not necessary, and therefore not permissible, for border control authorities to process and use data of EU citizens. Further, the Directive does not take into account the fact that, under the Convention Implementing the Schengen Agreement, citizens of EU Member States are subject to a different regimen of border controls when entering the EU than third-country nationals. In my view, it would have sufficed to transmit data after completing the boarding check, which would ensure that only data of passengers actually travelling would be transmitted to the border crossing points. Further, I had reservations regarding the freedom of the Member States to retain or introduce additional obligations for air carriers, including information or data in relation to return tickets, as provided in the recitals to the Directive. Extending the data transmission obligation also to passengers' biometric data, as provided in the recitals, would also constitute a much greater intrusion into passengers' rights and one for which I currently see no need.

Against this background, the further development of passenger data transmission within the EU remains to be seen. This applies particularly to the Directive's implementation in German law.

3.3.6 Interpol: Creating a DNA database

DNA technology is increasingly used at the international level to fight crime. Interpol has also initiated DNA-related projects.

The Interpol General Secretariat is preparing to process and use DNA profiles in data form to combat crime. To this end, since March 2000 it has been developing a pilot project to launch an international DNA database. The legal basis for this data collection is the Interpol charter "Internet DNA Gateway" which lists the conditions for storing and using Interpol DNA data. According to this document, DNA data obtained from

suspected/convicted offenders, from crime scene evidence, missing persons and unidentified bodies may be stored in connection with suspected international crimes.

The database is to contain DNA profiles in the categories listed above, without identifying information such as names or addresses; the profiles must contain certain features from the non-coding area of the genome. This means that no data regarding specific genetic dispositions may be stored. The database is to be operated from one stand-alone PC at Interpol headquarters; authorized member countries, who are solely responsible for the upkeep of the data they have entered, will be able to conduct automated database searches. If a match is found in the database, Interpol notifies the country requesting the search so that it can contact the country which possesses the information. Only then is the data subject identified by name.

In July 2003, Interpol sent requests for suitable data profiles to more than 100 member countries, including the Federal Criminal Police Office as the National Central Bureau for Germany. After this request at the national level had been discussed with the responsible agencies at state level – among others as the holders of the relevant data – in May 2004 the Federal Ministry of the Interior asked for my opinion with regard to data protection issues.

In my opinion, I expressed my view that the data in Interpol's collection have a personal character, because they can be attributed to individuals through recourse to the responsible holders of the data; indeed, this is the express purpose of the database. Due to the personal nature of this data, Section 14 of the Act on the Bundeskriminalamt and the Cooperation between Federal and State Authorities in Criminal Police Matters (BKA Act) applies to any data supplied by Germany. Based on this fact, I stated that only member countries with comparable standards of data protection should be able to access DNA profiles supplied by Germany (see Section 14 para. 7 of the BKA Act). Interpol must make sure this is the case. Further, in order to uphold the principle of proportionality, I stressed that only those DNA profiles of offenders or evidence should be supplied to Interpol for which there were specific indications of transnational relevance. Further, in view of the sensitive nature of DNA data, I insisted on an effective check of data protection compliance at Interpol; given the lack of an independent data protection supervisory authority for Interpol, this is problematic.

After receiving my opinion, the Federal Ministry of the Interior forwarded me among other things a report of the Federal Criminal Police Office on the creation of an international DNA database at Interpol; this report stressed that German participation was permissible in terms of data protection law. The report also noted, however, that certain additions to the relevant orders opening a file were still needed, in particular with regard to the Federal Criminal Police Office DNA database and its file of missing persons and unidentified bodies. This report was approved by Task Force II of the Conference of Interior Ministers in autumn 2004. The Federal Ministry of the Interior shared my view that the DNA profiles requested by Interpol constitute personal data which the Ministry regarded as pseudonymous. On the other hand, the Ministry did not share my reservations concerning the “transnational relevance” of profiles on practical grounds alone, arguing that in many cases, such transnational relevance became apparent only after finding a match in the Interpol database.

At the hearing on the revised orders opening a file in accordance with Section 34 of the BKA Act, I will advocate upholding the principle of proportionality when entering data into the Interpol database and ensuring the transnational relevance of the data entered. DNA profiles which are not needed in combating international crime should not be transmitted to Interpol. Another concern is to ensure that only Interpol member countries with comparable levels of data protection may have access to DNA data supplied by Germany.

6 Internal administration; statistics

6.1.4 Should data of nationals of a EU Member State be included in the Central Aliens Register?

The current practice is to store the data referring to nationals of an EU Member State, who have their residence in the Federal Republic of Germany, in the Central Aliens Register [Ausländerzentralregister - AZR]. In my view, this contravenes European data protection law.

A definitive answer to the question of whether data of nationals of an EU Member State who have their residence in the Federal Republic of Germany may be stored in the Central Aliens Register (AZR) is still outstanding. At the end of 2000, every fourth foreign resident whose data were stored in the AZR came from an EU Member State. Following the EU enlargement on 1 May 2004, the number of this category has continued to rise.

Already in 1999, the European Parliament forwarded a petition to this effect for my comments (see the 18th Annual Progress Report, No. 5.1.1). My conclusion was that general storage of such data contravenes the European Data Protection Directive (Directive 95/46/EC). Storage can be allowed only in individual cases, i.e. when decisions on issues under foreigners law, such as expulsion or deportation, are to be registered. In response to my comments, the Federal Ministry of the Interior informed me that it was looking into the question of the possible inclusion of an amendment to the Act on the Central Aliens Register [*Gesetz über das Ausländerzentralregister - AZRG*] in the legislative procedure regarding the draft Act to Control and Restrict Immigration and to Regulate the Residence and Integration of EU Citizens and Foreigners [short title: "Immigration Act"]; an amendment to this effect would cancel the storage of data on EU nationals (see the 19th Annual Progress Report, No. 34 no. 6). This, however, was not done (see also No. 6.1.1 of the German report).

While the draft Act to amend the Act on the Residence, Economic Activity and Integration of Foreigners in the Federal Territory [Act to amend the Residence Act] and Other Acts (*Bundestag* printed paper no. 15/3784) also envisaged extensive changes to the Act on the Central Aliens Register (AZRG), my request - repeatedly put forward during

interdepartmental discussion of this draft Act - that general storage of the data of EU nationals should be excluded from the Central Aliens Register was not complied with.

On 7 July 2004, the European Commission initiated an infringement procedure against the Federal Republic of Germany. The Commission took the view that general processing of personal data of EU nationals in a central register (of foreigners) is not needed in view of Art. 7 lit. (e) of the European Data Protection Directive. Also, processing of such data in a separate register covering foreigners was in contradiction with the principle of banning discrimination based on nationality with regard to those persons who exercise their right as EU nationals to reside, without restriction, on the territory of a Member State, and thus contravened Articles 12, 17 and 18 of the EC Treaty. Therefore, in the Commission's view, the AZR Act in these respects was not consistent with the EC Treaty and the European Data Protection Directive.

I share this view and will follow the infringement procedure just as closely as the administrative proceedings (at present suspended on account of the infringement procedure) under which the petitioner requests erasure of his data from the Central Aliens Register (AZR).

6.1.5 Eurodac — a successful undertaking?

Eurodac has been in operation since 15 January 2003.

The **European dactyloscopic** system EURODAC started operations - on schedule - on 15 January 2003; I reported on the system's provisions already earlier (see the 17th Annual Progress Report, No. 5,7, and the 19th Annual Report, No. 7.1.1).

The system's start prompted me to obtain information on the various working processes from the agencies responsible for implementing the EURODAC Regulation [Regulation (EC) No. 2725/2000] at the national level. For this purpose, I visited the central office of the Federal Office for Migration and Refugees [*Bundesamtes für Migration und Flüchtlinge - BAMF*] (formerly: *Bundesamt für die Anerkennung ausländischer Flüchtlinge* - Federal Office for the Recognition of Foreign Refugees) and one of its branch offices and the Federal Criminal Police Office (BKA). There are no objections to the working processes for establishing, compiling and transmitting so-called Eurodac hits [i.e. matches; results of

comparison]. The Luxembourg-based central database is controlled by the European Data Protection Supervisor (see No. 3.2.3 of the German report).

Experience shows that a database of this type kindles greediness. Thus, Germany already in autumn 2001 suggested that the data stored in the central Eurodac database might also be used for police purposes. It was argued that inclusion of the Eurodac data holdings would make it easier to match police intelligence with the fingerprints of persons staying as asylum seekers in other Member States. This in turn would significantly facilitate criminal prosecution and would also make it possible to identify risks to security already in advance.

Given the strictly limited applicability of the EURODAC Regulation [Regulation (EC) No. 2725/2000] to uses under the Dublin Convention, the relevant data cannot be used in such a way for police purposes. The data may only be used for determining the Member State responsible for examining applications for asylum, or for actual examination of such applications. For any envisaged uses going beyond this scope, the EURODAC Regulation would have to be amended.

I will continue to follow developments in this area.

6.2 Biometrics in identity documents

It is planned to integrate biometrics in identity documents - notwithstanding considerable doubts about the reliability of the envisaged technology.

Photos have always been an integral part of identity documents. Introduction of digital photographs will make it possible to search a database for the person shown in the photo. In other countries, fingerprints were included in identity documents already in the past (see the 19th Annual Progress Report, Nos. 2.2.3, 2.3.4).

Added security is given as the main reason for calling for the introduction of biometric features that can be utilized and analyzed electronically:

protection of such documents against forgery would be increased;

use of counterfeit or stolen documents would be prevented;

controlling of vulnerable areas, e.g. airports, would be speeded up.

In view of the findings obtained so far, I doubt whether such biometrics-supported travel documents will ultimately provide the promised added security, because

protection of German passports and identity cards against forgery is already ensured to a very large extent (see the 19th Annual Progress Report, No. 7.2);

where biometrics-supported passports are issued in countries without a regulated civil registration system, it is not possible to prevent that biometrics-supported documents might be made out in the name of other persons;

in view of the high error rates obtained in automated data evaluation processes, a large number of individual items are likely to require checking and reworking.

On the basis of the Act to Fight International Terrorism (*Terrorismusbekämpfungsgesetz*) of 9 January 2002 (Federal Law Gazette I, p. 361), the Passport Act (*Passgesetz - PassG*) (Section 4 paras. 3 and 4) and the Act on Identity Cards (*Personalausweisgesetz - PersAuswG*) (Section 1 paras. 4 and 5) now include provisions under which biometric features may generally be included in identity documents. At its 63rd meeting in March 2003, the Conference of the Federal and *Land* Data Protection Commissioners discussed

this issue and adopted a resolution stipulating certain conditions for the inclusion of biometric features in identity documents (see box to No. 6.2 [German report]).

Subsequently, both at the national and international levels, many activities were aimed at introducing biometric features in identity documents. These efforts are significantly advanced by the International Civil Aviation Organization (ICAO), a United Nations (UN) specialized agency which for years already has studied the scope for introducing biometrics in identity documents. Since September 2000, ICAO has been advocating the facial recognition approach. After September 11th, 2001, the related activities have been stepped up significantly. ICAO and the International Organization for Standardization (ISO), which was entrusted with this task by ICAO, are supported by other (national) standardization organizations, such as *Deutsches Institut für Normung e.V.* Both the European Commission and the European Council as well as the Federal Government base their provisions on the objectives and requirements stipulated by ICAO - both with regard to the selection of biometric identifiers to be included in identity documents, and as regards use of specific techniques. Consequently, ICAO's specifications - while not being internationally binding rules - constitute a *de facto* international standard for the introduction of biometric features and techniques.

As regards the practical usefulness of biometric identifiers - both in terms of verification and identification - attention must be drawn to the large number of technological problems which, for the major part, are not yet solved. The report submitted by the parliamentary Office of Technology Assessment (*Büro für Technikfolgenabschätzung - TAB*) to the German *Bundestag* pointed out that for the generally well investigated biometric applications of digitized hand and palm recognition and iris recognition, the respective recognition rate has not yet been tested on a large scale. But also in the case of fingerprint and facial recognition techniques, which have been studied and tested in greater detail, it must be noted that mass application of these techniques continues to yield a high error rate as regards the number of persons falsely recognized. For example, it is not possible in all cases to take fingerprints (e.g. if the persons concerned have lost fingers, or their fingerprints have been damaged).

A high rate of false recognition or false acceptance in a biometric system would, in terms of security, disqualify the system for use, i.e. these techniques would be unsuitable for

mass application. On the other hand, false rejections would have discriminatory effects for the affected persons and would result in poor acceptance of the technique by users. Moreover, the problems posed by false rejection cannot be resolved by combining various biometric features, e.g. fingerprint and facial recognition; rather, a person might in this case be refused admission for the mere reason that there is no match for just one of the biometric features. This might ultimately result in a further increase in the false-rejection rate.

The TAB's report also drew attention to the considerable costs involved in introducing biometrics.

Reference: "*Zweiter Sachstandbericht — Biometrie und Ausweisdokumente*" (Second TAB Report - Biometrics and Identity Documents), *Bundestag* printed paper 15/4000, www.tab.fzk.de/de/projekt/zusammenfassung/ab93.pdf

6.2.1 EU Regulation on standards regarding passports and travel documents

In future, EU citizens' passports are planned to contain an RFID chip that also stores biometric features.

On 13 December 2004, the Council of the European Union (European Council of Ministers) adopted the "Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States" (Official Journal L 385, 29/10/2004 pp. 0001 - 0006). This regulation serves the purpose of further harmonizing the passport format in the European Union Member States. The adopted EU standards regulation aims at establishing harmonized standards for security features and integrating biometric identifiers in EU citizens' passports.

During the discussions on the introduction of biometric features in EU citizens' passports, the EU Member States were agreed on the the inclusion of a digitized photo as a biometric identifier. However, their views differed with regard to the form in which photo data should be included in a chip embedded in the passport: only as a digital face recognition template - i.e. only in the form of an electronic reference pattern of the photo — or as raw

data (source data). Since the ICAO specifications are to be adopted at the European level to the greatest extent possible, it was decided to opt for storage of the raw data record.

Discussions on a second biometric feature soon centred on digital fingerprints. Views differed, however, on the question of whether inclusion of this second biometric feature should be obligatory or remain optional. In summer 2004, the motion proposed by a number of Member States for obligatory inclusion of the second biometric feature was rejected; however, following internal deliberations of the so-called "G5" Group (Germany, France, Italy, Spain, United Kingdom), the Council of Ministers for Justice and Home Affairs (JHA Council), at its meeting on 25 October 2004, amended the proposed draft Regulation, which then was already before the European Parliament (EP) for consultation, without giving any reasons for this amendment which provided for obligatory inclusion of digitized fingerprints as an additional biometric identifier. Therefore, it was only a few days before the adoption of the EP opinion on the original draft, that a revised draft Regulation was transmitted to the European Parliament. The latter noted this new proposal but delivered its opinion on the previous draft which only envisaged optional inclusion of digitized fingerprints.

Another legal problem in a data protection context was addressed only marginally in the preambular paragraphs of the draft Regulation. The "long-term perspectives" Recital referred to the creation of a European Passport Register, i.e. a European central file containing data on all passports issued in EU Member States. Objections to this plan were expressed by the Article 29 Working Party in its letter of 18 August 2004 to the Chair of the Council of the European Union, the President of the European Commission, the President of the European Parliament (EP) and other European agencies. These objections were shared by the EP which, in their Opinion of 2 December 2004, expressly declared themselves against a central database of passports and travel documents.

On 13 December 2004, the European Council of Ministers adopted the EU Regulation on standards regarding passports and travel documents - Council Regulation (EC) No 2252/2004 - without taking account of substantial arguments put forward in the EP Opinion. The Article 29 Working Party supports the EP position and requests that an explicit ban on establishing a central database be included in the Regulation;

biometric data may only be used for verification of the document's authenticity and the holder's identity on the basis of directly available comparable features if presentation of the passport is prescribed by law;

no data other than those permitted by law be stored in the passport;

the purpose for which passport data are read, stored, modified or deleted should be laid down just as specifically as the designated government agencies authorized to read, store, modify or delete such data.

Moreover, all supervisory data protection bodies of the EU Member States consider it desirable to have appointed representatives of the Article 29 Working Party advise the committee to be established under the EU passport regulation - Council Regulation (EC) No 2252/2004 - in its deliberations preceding the decision-making process so as to ensure that the envisaged technical specifications will, from the start, meet the requirements of data protection law.

6.2.2 New techniques employed by *Bundesdruckerei GmbH* for producing passports

At my request, the Federal Printing Office (Bundesdruckerei GmbH) provided information about the technical means that can be employed for integrating biometric identifiers in passports and other identity documents.

On the basis of the provisions of Council Regulation (EC) No 2252/2004 regarding inclusion of biometric identifiers in passports (see Nr. 6.2.1 above), it is planned to introduce new technology in the production of travel documents. It remains doubtful, however, whether introduction of biometric features will indeed enhance the protection of travel documents against forgery. Any gains in security protection of travel documents that might be anticipated are likely to stem from the introduction of a specific type of chip technology rather than from biometrics. In any case, it should also be noted in this context that for German passports and national identity cards, a very high technical standard has already been achieved as regards anti-forgery safeguards.

On several occasions I visited the Federal Printing Office to obtain information on the technical possibilities for embedding a chip in passports. I was informed that, under the

pertinent ICAO specifications, the only options regarding inclusion of biometric features in identity documents were a 2D bar code or a so-called RFID chip (Radio Frequency Identification-Chip; see No. 4.2.1 of the German report). It is planned to use 2D bar code technology for the international identification documents for seafarers (see No. 6.2.5 of the German report), while RFID chips are to be used under the provisions of Council Regulation (EC) No 2252/2004.

6.2.3 Biometric features in visas and residence permits

Under the European Union's common policy on visas, biometrics are to be integrated in the procedures for issuing visas and in residence permits for non-EU nationals.

Already before September 11th, 2001, the Federal Foreign Office and the Federal Ministry of the Interior initiated the inclusion of a photograph in the visa sticker. In its Regulation (EC) No 334/2002 of 18 February 2002 amending Regulation (EC) No 1683/95 laying down a uniform format for visas (Official Journal L 053, 23/02/2002, p. 7), the Council stipulated that "a photograph produced according to high security standards" be integrated in visa stickers.

On 24 September 2003, the Commission submitted a draft Regulation to introduce biometric features (digital photo, two digital images of the holder's fingerprints taken with the fingers flat) in visas and residence permits for third-country nationals and, in addition, to establish a nationally and Community-operated database (VIS = Visa Information System) containing alphanumerical data (e.g. name, address, date and place of birth), biometric data (digital photograph, fingerprints) and other scanned-in documents (possibly to include passports, birth certificates, etc.) of visa applicants.

In the wake of the Madrid terrorist attacks of 11 March 2004, the Council called on the European Commission to submit proposals for enhanced interoperability between European databases and, in addition, to explore the creation of synergies between existing and future information systems (SIS II, VIS and EURODAC) in the prevention of, and fight against, terrorism.

Following the Council's funding decision of 8 June 2004, preparations started on establishing this system. The Commission's aim in this respect is to provide an identical technical platform such as the new Schengen information system (SIS II — see No. 3.3.2.1 above).

All measures taken in this field will have a major impact on the fundamental rights of foreign nationals applying for visas for entering a so-called Schengen country. It is expected that, as of 2007, some 20 million visa applications per year will be filed for entry into countries of the enlarged European Union. Therefore, the current database cycle will affect up to 100 million persons.

The Article 29 Working Party, in its Opinion No 7/2004 of 11 August 2004 on the inclusion of biometric elements in residence permits and visas (see No. 3.2.1 above), made a critical assessment of the Commission's proposal. The Working Party stressed the need to maintain protection of fundamental rights - notwithstanding the understandable wish to combat "visa shopping" and "identity fraud". It expressed the concern that the principle of proportionality might be neglected in creating a central database containing biometric data on all foreign nationals applying for a visa. Moreover, the Working Party urgently called for precise rules regarding a clear definition of specified, explicit and legitimate purposes. Strict security specifications were formulated, in particular, for the chip originally planned to be embedded in visas. In view of possible recognition errors (false rejections) in biometrics-based border checks, the persons in question must be informed of the reasons for the rejection. Also, they must be provided the means by which they may assert their own point of view before any decision is taken (Article 15 of Directive 95/46/EC - European Data Protection Directive - on automatic decisions).

A new draft Regulation submitted by the Commission on 28 December 2004 takes account of a number of these requirements. The draft provides for storage, in the VIS, of alphanumerical and biometric data (digital photographs, fingerprints), but not of any other scanned-in documents. Instead, links to other applications are to be stored. A deletion period of five years is to apply to such data. On account of difficulties in applying RFID technology, the draft does not contain provisions on the storage of biometric features on visa stickers. The VIS is to be used for visa procedures and, in addition, for asylum procedures and the identification and return of illegal immigrants. The Article 29 Working

Party plans to submit its comments on the draft soon, thus helping to ensure that the forthcoming EP deliberations will also cover data protection issues.

7 The Judiciary

7.1.1 Federal Constitutional Court decision of 3 March 2004

The Federal Constitutional Court ruling on acoustic surveillance in private homes provides important orientation when balancing the demands of internal security against the rights of the individual.

In its landmark decision, the Federal Constitutional Court set clear limits on covert acoustic surveillance of private homes (see box to No. 7.1.1). A minority of the deciding senate regarded Art. 13 para. 3 of the Basic Law, which provides the constitutional basis for the surveillance of private homes, as “unconstitutional constitutional law”. The majority of the senate argued that Art. 13 para. 3 of the Basic Law must be interpreted restrictively and with regard for human dignity, ensuring that acoustic surveillance of private homes does not intrude on the inviolable core of the private sphere. In my view, the heart of the ruling concerns the further development of this concept, which is derived from the concept of human dignity and has been refined in constant judicial practice. Surveillance may not intrude on this core area, not even in the interest of criminal prosecution. This means that covert listening is not permitted when a person is alone at home or there with person(s) to whom he/she has a special, private relationship of trust and there is no specific reason to believe that their conversation will have a direct bearing on a criminal offence. This refers to family members and close personal friends. Protection of the private sphere thus prohibits round-the-clock surveillance of any kind, as well as continuous automated recording.

In any case, acoustic surveillance of private homes can only be justified in investigations of especially serious crimes. According to the court, the catalogue of offences introduced in Section 100c para. 1 (3) of the Code of Criminal Procedure (StPO) in 1998 goes well beyond the bounds of what is permissible. For example, the catalogue lists numerous minor offences, some of them without minimum penalties, as grounds for ordering acoustic surveillance of a private home. But for a crime to be regarded as especially serious, as referred to in Art. 13 para. 3 of the Basic Law, it must carry a maximum penalty of at least five years’ imprisonment.

Also welcome was the Federal Constitutional Court's explicit criticism of the law's failure to pay sufficient attention to the right of refusal to give evidence or testimony. Acoustic surveillance and recording of protected conversations must be prohibited by law. Section 100d para. 3 StPO is not sufficient for this purpose, as it does not provide for a general ban on surveillance of persons entitled to the right of refusal to give testimony, which includes in particular close relatives, but provides only for inadmissibility of evidence gained from their conversations; nor does it contain any restrictions on conversations with other close friends. Further, it does not stipulate that information acquired in this way must be destroyed.

It is also significant that the court requires that all persons affected by acoustic surveillance are to be informed after such surveillance has taken place, as this is the only way to ensure their right to court relief.

The decision on acoustic surveillance of private homes and the decision on interception of post and telecommunications according to the Foreign Trade and Payments Act (see No. 5.4.3), also announced on 3 March 2004, affect significant provisions of the StPO which govern telephone surveillance. For this reason, other powers of intervention need to be re-assessed, in particular covert information-gathering that necessarily intrudes on the private sphere, such as longer-term observation, the covert use of technical means, and the use of confidential informants and undercover investigators. This affects not only federal law, but also state laws governing the police and the authorities for the protection of the constitution. Even though these laws are not explicitly mentioned in the court's decision because they were not the subject of the proceedings, the values expressed in the decision and the court's argumentation also extend to these powers of intervention (see No. 5.1.2).

7.3.2 Should genetic fingerprints be treated as equivalent to conventional fingerprints?

There are widespread calls to use DNA testing as a standard law enforcement procedure for identifying and registering individuals, although it has the potential to provide far more information than that yielded by fingerprints, photographs and measurements.

Particularly in recent months, policy-makers have increasingly called for broader use of DNA testing. The Standing Conference of the Interior Ministers of the states (*Länder*) in the Federal Republic of Germany has called for making DNA analysis of non-coding areas of the genome the equivalent of other law enforcement measures for identifying and registering individuals within the framework of Section 81b of the Code of Criminal Procedure (StPO). The Conference of Justice Ministers charged their criminal law committee to examine whether and if so, to what extent constitutional law allows DNA testing to be used for the purpose of identification in future criminal proceedings, analogous to standard law enforcement procedures for identifying and registering individuals.

At an expert hearing by the CDU/CSU parliamentary group on 18 September 2003, a public expert discussion held by Alliance 90/The Greens on 1 March 2004, and in a discussion with the Federal Ministry of Justice on 15 June 2004 I stressed that DNA testing could not be regarded as equivalent to conventional fingerprinting simply due to the former's potential to provide far more information than the latter. Using current technology, it is already possible to draw conclusions regarding personal characteristics such as age, ethnicity and certain diseases even without examining the non-coding areas of the genome. One should also not overlook the fact that obtaining the material necessary for DNA analysis constitutes a bodily intrusion; according to Section 81a StPO, doing so requires a judge's authorization and may only be carried out by a physician. By contrast, according to Section 81b StPO, the police or public prosecutor's office may take photographs and fingerprints of persons even against their will.

There are other serious arguments against making DNA testing the equivalent of conventional fingerprinting: first of all, the potential risk inherent within the procedure for DNA analysis. Once the human cells needed for DNA analysis have arrived at the laboratory responsible for testing, there is a risk that the coding areas of DNA may

mistakenly be included in testing, resulting in information about personal characteristics and appearance. This risk remains until the DNA profile has been created and stored in the database of the Federal Criminal Police Office (BKA) and the original sample has been destroyed. For this reason, legislation specifying numerous steps to ensure security throughout the process has been passed, including Sections 81d and 81e StPO with their strict conditions for use; and, according to Section 81f para. 2 StPO, only certain trustworthy specialists may carry out the procedure. Further, according to Section 81f para. 2 StPO, the sample must be given to the specialist in anonymous form and must be destroyed immediately as soon as it is no longer needed for analysis (Sections 81a para. 3, 81g para. 2 StPO).

Another argument against making DNA testing a routine part of identifying and registering individuals is the fact that, according to the constitutional prohibition on the use of excessive means, such analysis is to be limited to exceptional cases. The Federal Constitutional Court (see No. 7.3.1 above) saw this limit as given under existing law, which states that DNA analysis may be performed only if the person concerned has already been convicted of a serious crime and if there is factual evidence that he or she is likely to re-offend in future. In the court's view, the need for a judge's authorization as specified in Sections 81g para. 3 and 81a para. 2 StPO takes into account the individual's special interest in effective protection of his/her basic rights. The Federal Constitutional Court also ruled that before a well-founded decision regarding intervention into the individual's right to informational self-determination could be made, a sufficient investigation of the situation was necessary, including in particular reference to the available criminal and prosecution records, probation officers' records and recent queries of the Federal Central Criminal Register; the grounds for the decision should also include an assessment of the significant circumstances, which requires deciding on a case-by-case basis.

In my view, judicial authorization and factual evidence of the likelihood of re-offending are absolutely required by constitutional law. The possibility of court relief after the fact cannot serve as a substitute for a judge's authorization for the simple reason that such authorization plays an important role in ensuring that the procedure adheres to the rules. Any concessions with regard to determining the likelihood of re-offending would be untenable due to the constitutional prohibition on the use of excessive means and the

resulting restriction of DNA testing to exceptional cases, as the Federal Constitutional Court has repeatedly emphasized.

Even for taking conventional fingerprints, Section 81b StPO requires an assessment of the likelihood of re-offending in that there must be some indication that the suspect could commit another similar or different offence and that an official law enforcement record of his/her identity would aid in subsequent investigations. However, this standard of assessment does not in any way fulfil the constitutional requirements for taking genetic fingerprints. This standard is significantly lower than the standard specified in Section 81g para. 1 StPO and in Sections 2 and 3 of the Act on establishing a person's identity by means of DNA analysis (DNS-IFG). Nor does Section 81b StPO provide for authorization by a judge. I do not see how the police or public prosecutor's office are supposed to be able to produce an assessment of the likelihood of re-offending that is sufficiently comprehensive to satisfy the demands of the Federal Constitutional Court.

On the other hand, I have repeatedly stated that I would not object to doing away with the requirement of judicial authorization for the analysis of unidentified trace evidence (see Bundestag document 15/4136), as there appears to be little sense in having a judge examine cases in which the DNA to be analysed is that of an unknown person.

7.9 European Cooperation in Criminal Matters

Eurojust

The Act on Eurojust, which created a national legal basis authorizing the transmission of information to Eurojust, could be improved.

Established by the Council Decision of 28 February 2002, Eurojust began operations in December of that year. The Council Decision also had to be implemented in Germany; although it is binding for all Member States, it is not directly effective at national level (see Art. 34 para. 2 second sentence (c) of the Treaty on European Union). In particular, it was necessary to create the necessary legal foundation for authorizing the transmission of data by national authorities to Eurojust (see the 19th Annual Report, No. 8.9). The Council Decision was transposed into national law by the Act on Eurojust, which entered into force on 18 May 2004 (Federal Law Gazette I p. 902 ff.). In addition to governing the transmission of information to Eurojust, the Act primarily contains provisions on the rights and obligations of the national Eurojust member.

During the consultations on the legislation, my concerns were only partly addressed. For example, I regard the provision on the transmission of information (Section 4 para. 1 of the Eurojust Act) as too indefinite. It fails to clarify sufficiently for the transmitting authorities in which specific cases data may be transmitted. Further, I pointed out that Section 7 para. 1 fourth sentence of the Eurojust Act does not sufficiently define the right of national contact offices to use information contained in work files. In my view, it is not enough to specify the necessary data protection regulations within a legal ordinance; I would have therefore preferred to see the data protection regulations, such as those regarding the maximum length of data retention and mandatory destruction of records, included in the law itself. As a result of my expressed concerns, only the following sentence was added to Section 7 para. 1 of the Eurojust Act during the parliamentary process: “Proper consideration shall be given to the protection of personal data.”

However, the ordinance on Eurojust contact offices of 17 December 2004 (Federal Law Gazette I p. 3520), which contains data protection provisions as well as designating the Federal Public Prosecutor as Eurojust’s national contact office for terrorism, does take into account some of my recommendations, for example with regard to the defined purpose of the file to be set up at the Federal Public Prosecutor’s office and with regard to

the obligation to keep this file separate from other files and registers using technical and organizational means.

7.9.2 Latest developments

The principle of the mutual recognition of decisions in criminal matters threatens the individual's right to protection.

EU legislation aimed at creating an area of freedom, security and justice in the area of criminal law is progressing rapidly. I welcome improvements in European cooperation on criminal matters but note with concern that these are threatening to take precedence over the individual's right to protection. The mutual recognition of decisions in criminal matters, which the Tampere European Council in 1999 declared the "cornerstone" of judicial cooperation, entails the risk that the strictest national criminal code will become the standard for the entire EU. For this reason, I consider it absolutely essential that this process take sufficient account of individual rights. As far as data protection is concerned, the so-called third pillar continues to demonstrate significant shortcomings. The interests of improved European judicial cooperation are equally served by ensuring shared high standards of data protection also in this area (see also No. 3.2.6).

One of the first measures having to do with the mutual recognition in criminal matters was the creation of the **European Arrest Warrant**, which was transposed into national law by the act of 21 July 2004 implementing the Framework Decision on the European arrest warrant and the surrender procedures between Member States (Federal Law Gazette I p. 1748). As early as 24 November 2004, the Federal Constitutional Court issued a provisional order suspending the first extradition requested on the basis of a European arrest warrant (File ref. 2 BvR 2236/04). It will be interesting to see whether the court's pending decision on the constitutional complaint which led to this action will have consequences for the European arrest warrant and possibly also other measures of mutual recognition.

The European Commission's proposal for a Framework Decision on the **European Evidence Warrant** for obtaining objects, documents and data for use in proceedings in criminal matters (COM (2003) 688 final; Council Doc. 15221/03) is also based on the principle of mutual recognition. This measure, which is aimed at quicker, more effective

judicial cooperation in criminal matters, is highly problematic, as I have pointed out to the Federal Ministry of Justice and the legal affairs committee of the Bundestag in joint comments with the state data protection commissioners. For example, the conditions on the use of personal data in Art. 10 para. 1 of the proposal are in part more broadly formulated than the provisions in German law. According to the Code of Criminal Procedure, for example, information acquired through certain types of covert surveillance may be used only in prosecuting certain specific criminal offences. By contrast, the proposal would allow such data obtained in the executing state to be used when prosecuting less serious offences and even civil violations in the requesting state, threatening to render meaningless national restrictions on the proper use of information in the judicial area. One may also question whether the right of refusal to give evidence and prohibitions against seizure are given sufficient attention. Lastly, a special cause for concern is the prospect of a joint instrument, as described in the rationale behind the proposal, that would apply to all types of evidence, including that which still must be secured. Such an instrument would be an even greater intrusion upon basic rights, as it would require a much lower burden of proof for telecommunications surveillance or DNA testing than that now required at the national level. For this reason, I am pleased that the Bundestag has also criticized the Commission's proposal in its comments to the Federal Government and has called for additional safeguards in the area of data protection, among others (Bundestag doc. 15/3831).

In reaction to the terrorist attacks in Madrid on 11 March 2004, the Commission considered establishing a **European criminal record** (COM(2004) 221 final; Council doc. 8200/04). I am extremely reluctant to endorse such a record, as it would hardly be possible to ensure the standard of data protection required by German law and data records would be likely to be duplicated. On the other hand, a suggestion by the Federal Ministry of Justice and the Council of EU Ministers of Justice and Home Affairs does appear to be acceptable: Rather than establishing a central, European register of criminal convictions, they call for linking the existing national criminal registers as far as possible while upholding the rights of those concerned. This is the aim of a project currently under way between Germany, France and Spain. In addition, the "Swedish Initiative", which I have discussed above in No. 3.3.4, also serves the purpose of improving the exchange of information between the criminal prosecution authorities of EU Member States.

Given the lack of uniform standards for procedural rights in the individual Member States, I welcome the Commission's intention to formulate another proposal for a Council Framework Decision on certain procedural rights in the European Union (COM(2004) 328 final; Council doc. 9318/04) in order to set common minimum standards. However, the proposal's provisions on audio and video recordings are extremely fragmentary in terms of data protection standards. In my view, such standards should at least take account of differences between types and seriousness of the crime of which the suspect is accused and of the recording's significance for the proceedings. Further, provisions specifying the maximum length of retention and use of information and prohibiting its reproduction need to be added. In consultation with the state data protection commissioners, I have pointed this out to the Federal Ministry of Justice; it and the Bundesrat (Bundesrat doc. 409/04) largely share my view.

11 The Private Sector

11.4 The SCHUFA is expanding its field of activity

The SCHUFA credit reference agency is planning to expand its field of activity. From now on, sectors of the economy that are not “classic” partners of the credit industry are to be connected to its information system.

In the reporting period, the SCHUFA continued to pursue the goal of tapping into new fields of activity. Whereas in the past the SCHUFA’s contracting partners came exclusively from the credit industry (banks, telecommunications companies, mail order, retail), according to its own statements, the SCHUFA is now planning to allow all those companies “who grant loans in the broader sense to benefit from the SCHUFA data”. It is therefore increasingly entering sectors of the economy whose justified interest in the SCHUFA data is dubious. In the reporting period, these were specifically the housing industry, the insurance industry and the debt collecting industry. The SCHUFA planned to include these sectors by means of a so-called “B” process, i.e. the contracting partners report negative features to the data records that can then be called up by all other contracting partners. On the other hand, they would be entitled to receive negative features from the entire data records. I expressed major reservations about including these sectors in the SCHUFA data records.

As far as the housing industry is concerned, I refer to the deliberations in my 19th Annual Report (cf. 19th Annual Report No. 10.5.1; cf. No. 11.6). I believe that the intended inclusion of the insurance industry is unacceptable because there is not usually a credit risk for the insurance companies. If insurance premiums are not paid, insurance companies can terminate a policy, which then cancels the insurance cover. Furthermore, the SCHUFA has conceded that no link between a risk of damage to the insurance company and the creditworthiness of a client interested in insurance has been proven. I can only imagine the incorporation of debt collecting agencies in the SCHUFA in the extremely limited cases where the debt collecting agency is acting as the “extended arm” of another SCHUFA contracting partner. In my opinion, all other cases would be an impermissible extension on the part of the SCHUFA contracting partner in the absence of a justified interest.

The SCHUFA currently has data on over 60 million German citizens. Against this background, further expanding the number of contracting partners would mean an even broader distribution of the credit records of practically all working people in Germany, with all of the consequences (cf. No. 11.7). I will therefore continue to advocate that the group of members remains limited to those with a justified interest in the creditworthiness of affected parties.

11.5 Scoring and rating methods – Star-gazing instead of hard facts?

Credit scoring and rating methods are gaining importance for commercial decisions that affect the individual citizen. Legal framework conditions in this field would be helpful.

Methods of scoring and rating consumers as credit risks are increasingly being used for economic decision-making. These methods define risk classes on a mathematical and statistical foundation and assign loan applicants, potential customers, etc. to the various classes in order to produce a supposedly representative picture of their creditworthiness. These methods are designed to assess individuals' creditworthiness largely independently of their actual behaviour, even if there is no negative information about a person's past credit record. Nowadays hardly any economic decisions are taken without the use of such methods. If you order goods over the Internet, the scoring process is usually already working in the background while the address data are being collected; the merchant then uses the results of this process to decide whether to offer only cash-on-delivery or also the option of payment by invoice.

The increased use of such scoring methods is questionable in terms of both data protection law and social policy. Scoring methods rob individuals of the possibility to determine how they will be viewed in public and even of the ability to influence it through their own law-abiding behaviour.

For this reason, a clear legal framework is needed here in order to ensure a sound data foundation, in particular a restriction to relevant individual information regarding credit records, income and property details.

Moreover, the method must be transparent, i.e. the affected person must be informed about the data and features considered, their weighting in the calculation of the score and of the actual score. In my view, limiting the individual's right to information under data protection law by referring to a company's "operational and business confidentiality" is unacceptable.

11.5.1 How the SCHUFA determines credit ratings

To date the SCHUFA has not responded to demands for comprehensive transparency in its rating method. It is therefore to be feared that, without legislative intervention, individuals will not be able to find out on what basis an application for credit has been accepted or rejected.

For many years the data protection supervisory authorities have criticized the lack of transparency of the SCHUFA's credit rating system (cf. 18th Annual Report No. 31.1.1, 31.1.2; 19th Annual Report No. 34, No. 14 there). Although the SCHUFA has now stated its willingness to notify individuals of their current credit rating upon request, it will not tell them what credit rating it provided to contracting partners. In the interests of improved transparency, I believe individuals also need to know this information, which may have contributed to decisions affecting them – for example, the refusal of a loan application. In the reporting period, too, the supervisory authorities resolutely demanded that individuals be informed of their credit rating provided to contracting partners. The SCHUFA believes that this cannot be achieved before the end of 2006 due to a lack of technical facilities and has not made any promises in this respect for the future, either.

The SCHUFA continues to refer to business confidentiality in its refusal of the supervisory authorities' long-standing demand for information on the factors included in calculating credit ratings and their weighting. But without this knowledge, individuals have no way of understanding and, if necessary, influencing unfavourable ratings that result in negative decisions. This should be viewed against the background that no individual has a negative entry at the SCHUFA just on the basis of a poor score and should therefore be fundamentally viewed as a creditworthy, respectable person. But if individuals do not know that, for example, frequent house moves, etc. can have a negative impact on credit ratings, they cannot take the opportunity to explain the circumstances (e.g. fixed-term volunteer soldier, job changes, etc.) to the contracting partner.

11.5.2 Use of credit ratings by telecommunications companies and Article 6a of the Federal Data Protection Act

Telecommunications companies which use credit ratings to determine creditworthiness prior to approving service contracts do not usually rely on impermissible automated

decisions based on personal data. But I continue to view critically the use of rating methods which are largely opaque to the individual concerned.

In my 19th Annual Report (No. 10.5.2) I dealt with the question of when the use of credit ratings (cf. No. 11.5.1) to check a person's creditworthiness constitutes an impermissible automated decision within the meaning of Article 6a of the Federal Data Protection Act (cf. box to No. 11.5.2). The background to my deliberations then was the practice of credit institutes when deciding whether to grant a loan. I referred to the idea of protection in this regulation stating that an evaluation of personality features always requires an evaluation by a person and may not be based only on a standardized computer analysis.

In the current reporting period I examined how telecommunications companies conduct creditworthiness checks before approving a new customer's service contract and the extent to which pre-determined credit ratings are used in this process. I was especially interested in whether there is an individual check in every single case or whether automated decisions are taken that would violate Article 6a of the Federal Data Protection Act, in that such decisions would have legal consequences for the persons concerned or would otherwise constitute a significant hindrance. As creditworthiness checks are frequently used for mobile telecommunications in particular, I limited my survey to mobile telecommunications providers. This revealed that only some of the companies use credit ratings as part of their creditworthiness checks. Those providers who use such ratings as the basis for deciding whether to provide service stated that an application for mobile telecommunications service was everyday mass business that did not allow for individual checking. Nevertheless, the decision as to whether a manual or automatic check is made partly depends on an internally specified threshold. The mobile telecommunications providers were unanimously of the opinion that Article 6a of the Federal Data Protection Act was not relevant to creditworthiness checks in the telecommunications industry. They argued that rejecting an application for mobile telecommunications service did not entail any negative legal consequences for the affected party, and that a legal consequence within the meaning of Article 6a of the Federal Data Protection Act could only be a legal consequence decreed by a statutory regulation. But refusing to provide mobile telecommunications service is based on the principles of contractual freedom, they argued, adding that such refusal would also not constitute a "significant hindrance" for the affected party as required by the Act. The companies went

on to argue that, irrespective of whether lack of access to a mobile telecommunications network – unlike the fixed network – constitutes a hindrance, the affected party could use a pre-paid product from the same provider at any time, which is not subject to a creditworthiness check, and would not therefore be excluded from the option of mobile telephony.

Also taking account of this legal argument, I do not see any cause to revise my fundamentally critical attitude to the use of credit ratings (cf. No. 11.5.1; 19th Annual Report No. 34, No. 14 there).

13 Telecommunications and teleservices

13.1.1 To retain or not to retain data for possible future use?

The amended Telecommunications Act did not introduce any provisions requiring data retention for the purpose of preventing crime, nor is any requirement to retain telecommunications data to be introduced at the European level.

The previous law allowed telecommunications traffic data to be saved for up to six months with the final three digits deleted. This has changed with the new Telecommunications Act. As a rule, service providers may now save all traffic data in unabbreviated form for up to six months after customers have been billed for services. However, customers may still choose to have all their data deleted or abbreviated by three digits after the bill has been sent. In a decision, the federal and state data protection commissioners have opposed this amendment, which makes attaining the previous level of data protection dependent on the initiative of the affected party (cf. box to No. 13.1.1). During the legislative process, the Committee on Legal Affairs of the Bundesrat even demanded that a data retention requirement be introduced. This requirement was not included in the Telecommunications Act due to the constitutional reservations expressed by the data protection commissioners. A requirement of this kind would be constitutionally questionable in particular because mandatory data retention would primarily affect law-abiding users of telecommunications services and would thus disproportionately interfere with telecommunications secrecy and the right of individuals to determine the use of their personal data.

However, discussions continue on the introduction of a requirement to retain data. For example, at EU level France, Ireland, Sweden and the United Kingdom have submitted the “Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism”. A final decision on this has not yet been taken. As the Art. 29 Data Protection Working Party noted in its Opinion 9/2004 of 9 November 2004, the mandatory retention of all types of telecommunications traffic data for the purposes of public order would be

disproportionate and therefore not permitted under Article 8 of the European Convention on Human Rights (cf. box to No. 3.2.1).

13.2 How telecommunications companies handle personal data

13.2.1 Saving text messages for billing purposes

Saving the contents of text messages is against the law and violates telecommunications secrecy.

Various members of the public have written me to say that providers of so-called premium SMS services also save the contents of such text messages for long periods. They justify this practice by claiming that message contents are needed as evidence because mobile phone subscribers often dispute authorship of such text messages or cite technical faults on the part of the network operator to avoid having to pay for the service.

I discussed this problem with the Regulatory Authority for Telecommunications and Post (RegTP). We agreed that this practice violates telecommunications secrecy. Service providers may not monitor the content of telecommunications beyond the extent necessary to provide these services properly. This means that saving and monitoring message content is not necessary for operations in order to be able to prove that the contractual service has been provided, in particular because saving message content is not suitable proof of authorship of the text message as any details about the subscriber's identity can be easily falsified.

Preventing the sending of unlawful content, which is also used as a justification, should also be classed as impermissible monitoring as it is not necessary to provide the service. In this connection, I refer to Article 8 para. 2 sentence 1 Teleservices Act, which even exempts the providers of teleservices, i.e. content providers, from an obligation to monitor the information they transmit or save and states that the protection of telecommunications secrecy applies; this is even more the case for telecommunications services where the technical aspect of communication is even more to the fore than in teleservices and media services.

An implied waiver of telecommunications secrecy by the customer resulting from the use of the text service can be ruled out since monitoring the content of text messages violates the statutory requirements of data protection and telecommunications legislation and for

that reason alone does not meet the expectations of ordinary customers. Nor is it sufficient to include a note to this effect in the general terms and conditions of the service contract.

If message content has nevertheless been saved, the affected party may take legal action to demand that this data be deleted and to block the use of illegally saved text message content. Furthermore, the affected party can report the matter to the RegTP.

13.2.2 Location-based services

Mobile network operators and providers of location-based services must guarantee data protection for such services.

Locating mobile telecommunications subscribers is a sensitive issue (cf. 19th Annual Report No. 11.6, 11.10.4). During an advisory and inspection visit to a mobile network operator I came across a problem that is directly linked to the international division of labour in the telecommunications industry.

Mobile phone tracking takes place within the mobile telecommunications infrastructure of the network operator, which can be used by so-called platform providers. In turn, they make easy-to-use interfaces available to service providers, which are also used for other services, in particular for invoicing purposes. For example, if a mobile telecommunications customer wants information about nearby restaurants, the platform provider takes care of locating the customer with the network operator and charging for the service. The content provider supplies information about the restaurants near the stated coordinates. For this, the content provider receives a credit from the platform provider, but not the customer's telephone number because it is not necessary for this service. The content provider does not therefore process personal data; all of the data remain only with the platform provider (cf. figure to No. 13.2.2).

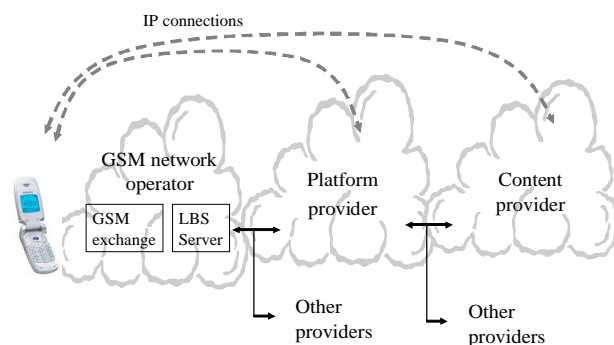


Figure to No. 13.2.2

Diagram of data processing

At the time of my advisory and inspection visit, the platform was offered by a company owned by the network operator but based in another EU country. As this company has to be assessed as a teleservice provider and has its headquarters abroad, I did not have the authority to check the data processing there. Based on information volunteered by the platform provider, however, it could be ascertained that it stores log files that also contain location information for too long – at least under German law. This problem is to be solved in the medium term by means of organizational changes.

13.2.3 Retention periods for traffic data under the German Fiscal Code

The long retention periods of the Fiscal Code do not apply to the retention of telecommunications traffic data.

According to Article 97 para. 3 of the Telecommunications Act (TKG), in principle traffic data must be deleted at the latest six months after sending the invoice. However, during checks I have repeatedly noticed that the itemized list of calls enclosed with telephone bills were stored for much longer. The companies referred to the retention periods specified by the Fiscal Code (AO): Under Article 147 of the Fiscal Code, documents relevant to taxation must be retained for six to ten years.

[Box]

At my instigation, agreement on this problem was reached with the Federal Ministry of Finance, the supreme financial authorities of the states (*Länder*) and the Federal Ministry of Justice. They agreed that network operators are in principle not required to retain traffic

data for tax purposes; retaining telephone invoices without listing individual phone calls is sufficient. However, if the invoice describes only the type of service and refers to the enclosed list of individual calls for their extent, these details become part of the invoice and must also be retained. I therefore suggested that invoices be designed so that the services provided are understandable without having to consult the list of individual calls.

A similar problem concerned employees' private use of employer-owned computers and telecommunications equipment. According to the recording and retention obligations of the Turnover Tax Act, first of all a distinction must be made as to whether employees are charged for their private use of such equipment. If the employer charges employees to use company computers or telecommunications equipment for private purposes, this is a taxable transaction: a non-gratuitous miscellaneous service. The basis for assessment is in principle the agreed or paid fee within the meaning of Article 10 of the Turnover Tax Act. In these cases, it can be assumed that the employees concerned have at least implicitly agreed to the recording of the data needed for invoicing, which is probably adequate for levying turnover taxes.

If employees are allowed to use company computers or telecommunications equipment for private purposes free of charge, the employer is in principle providing them with taxable goods and services granted free of charge within the meaning of Article 3 para. 9a of the Turnover Tax Act. The basis for assessment is all of the costs incurred for private use. Individualizing the data (recording the specific traffic data) is not necessary in terms of turnover tax law; it is sufficient to record the charges per employee for each invoicing period.

For employees, the benefits of being able to use company computers and telecommunications equipment have been tax-free since the year 2000 according to Article 3 No. 45 of the Income Tax Act. According to this, there is no need to retain traffic and usage data of privately used company computers.

13.2.4 Not all customers are happy with “Happy Digits”

Improper registration in a bonus programme blatantly violates customers' data protection rights.

We are all familiar with the question: “Have you got a loyalty card?” This is the good old trading stamp in new packaging. More and more companies in the modern business world are trying to increase their sales by using special customer loyalty programmes.

Telecommunications companies also use these marketing instruments.

Several members of the public wrote to inform me that customers of a large telecommunications service provider had repeatedly received mail from a company that manages the “Happy Digits” bonus programme welcoming them as new subscribers although they had not given any permission for this or had actually explicitly refused to join this programme.

My research revealed irregularities in the telecommunications service provider’s registration of new subscribers to the programme in mid-2003. Service provider employees had registered customers for “Happy Digits” without their consent. The company investigated and confirmed this suspicion. By doing so, these employees blatantly violated data protection provisions and infringed the rights of the customers concerned to determine the use of their personal data. Misconduct of this kind – however unpleasant it may be for the person affected – cannot always be completely avoided, unfortunately.

In the meantime, the company has deleted the data in all of the cases that have come to its attention. Since the company credibly assured me that there were no further cases of data transmissions without customer consent, nothing further needed to be done in these cases from the point of view of data protection. Irrespective of that, however, as part of my data protection supervision duties I have already generally discussed with the service provider what measures can be taken to ensure that the error rate is kept as low as possible in future. Efforts to further improve the procedure are continuing.

13.2.5 New service feature to block unwanted telephone calls

A new feature should enable telephone users to protect themselves against nuisance calls.

In the past, only call centres had the technical possibility of averting nuisance or malicious telephone calls (cf. 19th Annual Report No. 11.10.1; 18th Annual Report No. 10.14). In the reporting period, one telecommunications company began developing a new service

which allows individual customers to prevent nuisance calls from ringing. Using a specific combination of keys on the telephone, customers can enter telephone numbers on a list of numbers to be blocked. This can be done during or after a call has been received, whether the customer has answered it or not and whether the caller's number has been displayed or not. The list holds a maximum of ten numbers, after which they are overwritten. Customers may also delete the whole list themselves, but cannot view it and therefore cannot find out the telephone numbers that are not displayed on the customer's phone. The list of numbers blocked by the customer is saved at the exchange and can be viewed only by technicians responsible for the system technology.

This kind of call blocking is an alternative to call tracing. It should be considered a milder method in terms of data protection legislation because the customer who does not want to be pestered does not receive any personal data. From the point of view of data protection I have reservations that no automatic deletion deadline is specified for the telephone numbers that have been blocked. This means that a number can remain in the list of numbers to be rejected for a very long time if it is not overwritten. I have asked the company to introduce general, regular deletion deadlines as soon as this is technically possible.

13.2.6 Access to customer data in Deutsche Telekom's T-Punkt sales outlets

Employees in T-Punkt outlets should allow customers read-only access to account information and telephone records only after carefully checking their identification and authorization.

A Telekom customer who had visited a Deutsche Telekom AG sales outlet (T-Punkt) for advice on changing products wrote me to express surprise that the T-Punkt employee was able to view his most recent telephone bill just on the basis of his telephone number. The customer raised particular reservations concerning the possibilities of abuse, particularly due to the record of calls made, which was also visible. This letter led me to investigate the possibilities for internal access to customer data by T-Punkt employees with regard to data protection legislation.

Deutsche Telekom AG assured me that T-Punkt employees need general access to customers' billing data, including the record of calls made, to provide customer service. According to the company, although customers also had the option of calling a free telephone hotline to clarify questions about existing service contracts or to complain about a bill, customers with such concerns often visited the T-Punkt outlets instead. Deutsche Telekom said that employee access to billing data was, however, limited and did not include the ability to print out telephone bills or itemized lists of calls. The company went on to say that although the current review had revealed that a technical fault in some T-Punkt outlets meant that it had been possible to print out these data for a short time, this problem had now been remedied. Furthermore, due to my query, Deutsche Telekom AG has introduced a company regulation for all T-Punkt outlets that is designed to ensure that customer and billing data are released only to subscribers. To ensure proper identification or authorization, T-Punkt employees are now required to ask for the customer number, account number, invoice number, area code and telephone number, as well as the customer's name, address and date of birth. An existing rule already required third parties to present a statement of consent from the customer and their own identity card. Furthermore, individual access to customer account and billing data is recorded, which means that it is possible to conduct specific checks in the event of suspected misuse as well as regular random checks; under the Deutsche Telekom AG data protection strategy, such regular checks are also planned. I believe that these measures, which – as in the past – are associated with ongoing employee training on dealing with sensitive personal data, are appropriate and adequate.

13.2.7 Making court judgements anonymous when used in a civil case

When publishing court judgements, the privacy rights of those involved in the trial shall be maintained by blacking out their names.

A petitioner wrote to draw my attention to the fact that during a civil trial, a telecommunications company used court judgements from other trials where the names of those involved in the trials had not been deleted. The petitioner feared that a judgement reached in her own affairs could be used in this way and her personal data could be passed on to third parties in the operative provisions of a judgement without being made anonymous.

Publishing court judgements with the names of those involved in the trial is unacceptable according to Article 28 of the Federal Data Protection Act. Although the use of court judgements with legal force that have already been made is standard for the purposes of litigation, the names of those involved are not necessary in the operative provisions of a judgement. With regard to the principle of data protection legislation that personal data must be made anonymous as far as possible, personal data contained in judgements should be deleted before copies are released.

Since this is a general problem above and beyond the individual case, I informed the telecommunications company that the parties involved in conducting legal disputes have to respect the need to make copies of judgements anonymous before they are released to third parties. In response, its group data protection commissioner wrote to inform me that he shared my opinion and assured me that he would act accordingly in future.

13.2.8 Extent of the right to information according to Article 34 of the Federal Data Protection Act

Affected parties have a comprehensive right to information from telecommunications companies. This does not apply in certain exceptional cases.

For individuals, the right to know what personal information concerning them has been saved, as regulated in Article 19 and Article 34 of the Federal Data Protection Act, is a key instrument in asserting the right to determine the use of one's personal data. It is therefore hardly surprising that a number of people have complained to this office that telecommunications companies had not provided the information requested under Article 34 of the Federal Data Protection Act – or had provided only incomplete information. If information was not provided at all, the reason was often that the employees in the customer services department or complaints management had not recognized these requests as formal requests for information within the meaning of Article 34 of the Federal Data Protection Act and had therefore failed to forward them to the company's data protection officer or legal department. Only more intensive data protection training for the employees can bring improvement here, and I repeatedly draw attention to the need for this during inspections.

Another problem is presented by a customer's blanket request for comprehensive information about all personal data saved without giving more precise details about the nature of the data. To prevent unnecessary and excessive efforts on the part of companies storing the data, they must be able to ask affected parties to more precisely define what information they require, as stated in the wording of the law. On the other hand, the telecommunications company must not limit itself to generally cite just the type of data saved – as happened in one case. To enable affected parties to check the correctness of the saved data, they must be given specific information about these data.

In one case, I had to investigate whether a telecommunications company's refusal to notify a complainant of all the data stored about him or her was justified. The company explained its action by saying that these were data collected, saved and processed for business purposes. Under Article 34 para. 4 of the Federal Data Protection Act there is indeed no obligation to provide information if the affected party is not to be notified pursuant to Article 33 para. 2 sentence 1 Nos 2, 3 and 5 to 7 of the Federal Data Protection Act. In particular, this includes data that are used only to secure data or check data protection and where providing information would require excessive work. Furthermore, it concerns data that have to be kept secret by their very nature due to the overriding interest of a third party, as well as data saved for own purposes and where providing information would greatly hinder the business purposes unless the interest in notification outweighs the risk.

As the case that I investigated showed, it is difficult to assess which saved data are not legally subject to notification in a specific individual case. The question can only be answered by taking account of all the circumstances of the individual case and after careful consideration of the competing interests. There is no obligation to provide information if doing so would reveal company secrets and if the affected person's interest in the information cannot be considered greater than the company's interest in secrecy. In my opinion, the same applies if the data in question have to be kept secret due to the legal interest of a third party (e.g. an employee), for example, in the case of some recorded and saved telephone notes in a call centre. On the other hand, however, these may also contain notes about customer concerns that may affect an existing contractual relationship. In this respect, customers must have the opportunity to make sure their concerns are properly represented in order to be able to assert their right to correction, deletion or blocking. In

any case, it should be carefully considered whether the data in question should be deemed a company secret or employee data and how they should be assessed in relation to the affected party's interest in information. It is impossible to say in general which specific data are subject to the right of information and which are not.

13.8 Spam without end?

The UN organization ITU estimates that 75% to 85% of worldwide e-mail traffic is now spam. Resistance to this annoying irritant has resulted in numerous initiatives.

Everyone with an e-mail account is affected at one time or another. Sometimes a trustworthy e-mail service provider accidentally ends up on a “black list” of an anti-spam initiative, which means that e-mails sent via its service can no longer be delivered. And sometimes a spam attack brings the server of an e-mail service provider to its knees. In May 2004 one of the Federal Government’s e-mail servers was affected, which led to considerable delays in delivery of incoming and outgoing e-mails. And even if such problems can be overcome relatively quickly, they cost time and money. A corporate advisor therefore estimates the damage to German companies caused by spam at €300 million per year.

The tolerance of many users, companies and service providers has reached its limits. As a result, several governmental organizations, associations and international institutions have now come together in various initiatives, only a few of which can be mentioned here. In Germany, the eco association has formed an anti-spam task force; at EU level there is a working group of the national government offices responsible for investigating spam; and, internationally, the OECD has a task force to fight spam. Since they all have the same aim, the measures that have been planned or actually started are also similar: establishing a network of Internet providers, provider and international complaints management, positive lists of (legal) mass senders, “early warning systems”, awareness-raising among users, etc. These organizational measures are to be accompanied by technical and legislative measures.

In Germany a first step has been taken by transposing Directive 2002/58/EC on the protection of privacy in the electronic communications sector into German law. The Fair Trading Act amended on 1 April 2004 allows commercial e-mails to be sent only with the recipient’s consent and prohibits senders from disguising or concealing their identity so that recipients have the opportunity to take action against senders. However, these regulations disregard one thing: The majority of spam e-mails are sent via so-called zombie PCs, i.e. the computers of unsuspecting Internet users that professional hackers

from the spam services have taken over and linked together in so-called zombie networks. The spammers then operate using this computer's IP address and remain undetected themselves. Thus the "sender" of the spam e-mail – the unsuspecting Internet user – does not play a role. On the contrary, the one who benefits, i.e. the owner of the website advertised in a spam, must be made responsible for sending.

Even if it were possible to take legal action against the actual perpetrators, this is made more difficult, if not actually impossible, by a further circumstance: Operators of spam websites are increasingly moving to countries whose governments fail to take action against the plague of spam and whose service providers knowingly host and profit from spammers.

At the United Nations Anti-Spam Conference in July 2004, the ITU predicted that the spam problem could be overcome within two years by increasing cooperation to pursue spammers and by harmonizing laws. This is an ambitious goal which in my view can be achieved only if the various initiatives coordinate their efforts and all work together in future.

13.9 Google's new e-mail service and other business ideas

Google's announcement in April 2004 that it would shortly offer a free e-mail service aroused the interest not only of the relevant news media, but also of European data protection agencies.

Even before the official launch, civil rights activists and data protection specialists expressed their concerns, because everything that could be learned about the new **GMail** service from Google seemed to ignore all generally applicable rules to protect privacy. Google consequently took the bull by the horns and contacted the data protection agencies in several EU countries to present its new product and face critical questions from data protection specialists. In May 2004 talks took place with Google representatives in my agency. For the purposes of a common evaluation by all European data protection authorities I suggested that the Article 29 Working Party deal with the GMail issue (cf. No. 3.2.1).

GMail differs from other e-mail services mainly due to a feature that has not yet been imitated, possibly due to the implications under data protection law: The service automatically searches e-mails for specific key words and inserts context-related advertising. However, e-mails are not searched when they arrive on the Google server – as originally assumed – but just at the moment when users download e-mails from their mailbox. Then, while the e-mail content is displayed, the “matching” advertising is displayed on the side in the browser window. This is done dynamically, i.e. the advertising contents are not saved with the e-mail, but the whole process is repeated every time the e-mail message is read.

This automatic search procedure triggered lively discussions as to whether it required consent not only from GMail users, i.e. e-mail recipients, but also from e-mail senders. In terms of data protection law, this concerns the contents of communications whose confidentiality has to be guaranteed by the service provider during transmission. This automatically means that a deviation from this requires the consent of both correspondents. Currently, Europe's data protection experts are concerned with several more questions: Is this procedure a form of processing personal data? Is the automated scanning of e-mails a form of interception within the meaning of Directive 2002/58/EC on

privacy and electronic communications? Is the communications process completed when the e-mail arrives in the mailbox of the GMail user? Depending on the answers, the evaluation will come to a different conclusion: no consent is necessary, or just the consent of the GMail user or the consent of both correspondents.

At the time this report went to press, no definitive result had been achieved, but it is clear that Google will have to improve a few other aspects of its GMail e-mail service so that it complies with European data protection law. Google has already indicated its willingness to do so.

Another e-mail service, also launched on the market by a US provider, aroused comparatively little attention: Rampell's **Did-they-read-it**. This service, which is available by paid subscription, allows users to follow the course of e-mails they send. E-mail messages are sent via the provider's server, which tags them and tells the sender when the e-mail has been read, for how long, how often, whether it is forwarded and then also read. This information gained without the recipient's knowledge may be interesting to a few e-mail senders, but under data protection legislation a process of this kind is not permitted without the prior information and consent of the recipient.

Next year, the Article 29 Working Party will continue to concern itself with this and other e-mail services.

14.1 Data transmission abroad

14.1.1 US authorities demand prior transmission of parcel data

To combat terrorism the US demands prior information about the addressees and senders of parcels to the United States. Whether this demand is compatible with data protection legislation needs clarification at European level.

“US demands advance data about parcel recipients” – in the summer of 2004 the news agencies used these and similar headlines to announce that the US authorities were demanding advance information from European postal companies about the recipients and senders of parcels destined for the United States. With serious doubts about the permissibility of transmitting such data I initially researched the background to these reports. Based on the Trade Act of 2002 that entered into force on 5 December 2003, US Customs & Border Protection requires the advance transmission of electronic cargo information for goods being sent to the US. This law is designed to take account of the American demand for more security in the traffic of people and goods. These include freight items sent by ship as well as airmail parcels sent to the US. Disregarding these provisions is punishable and can result in the seizure of the plane with the unregistered cargo.

Unlike the cargo sector, the previously practised transmission of data using the written single voucher on the CN 23 customs form used all over the world is still acceptable for goods sent by post.

I find this requirement extremely problematic; in particular, I doubt whether transmitting such data is permissible, as far as the data are subject to postal secrecy under German law. I am critical of the fact – as with the advance transmission of passenger data of air travellers (cf. No. 22.2) – that the US is trying to collect personal data outside its own sovereign territory also from transport companies. If fears are confirmed that data about the transmission of parcels, packets and letters subject to postal secrecy are also concerned, I will take up this issue in discussions with the data protection commissioners of the other EU member states.

14.1.2 Item data in foreign accounting centres

Nowadays, data processing frequently no longer takes place at a company's headquarters. This is problematic if no adequate data protection level is guaranteed in the country of data processing. However, the Federal Data Protection Act contains regulations to protect personal data abroad.

Thanks to quick traffic routes and technical facilities, many companies are globally active. They have their headquarters or subsidiaries in countries of the European Union, America or Asia. This means that ever more data, e.g. customer and employee data, are transmitted to other countries.

Whereas Article 4b para. 1 of the Federal Data Protection Act defines data transmission to EU countries as the equivalent of domestic transmission, transmission to third countries has the additional prerequisite that an adequate level of data protection must be ensured (Article 4b para. 2 Federal Data Protection Act). Otherwise, data transfer is permitted only in the case of the exceptions listed in the catalogue given in Article 4c para. 1 of the Federal Data Protection Act: Personal data may be transmitted even without an adequate level of protection to agencies other than those cited in Article 4b para. 1, in particular if the affected party has given his or her consent or if the transmission is necessary to fulfil a contract concluded between the affected party and the responsible agency or to carry out pre-contractual measures taken at the instigation of the affected party. If none of the exceptions applies, the company must apply for approval under Article 4c para. 2 of the Federal Data Protection Act. This approval is granted if the responsible agency provides adequate guarantees with regard to the protection of privacy and the exercise of the rights associated with it. In particular, the guarantees can result from contractual clauses or binding company regulations.

In the summer of 2002 United Parcel Service (UPS) informed me of its practice of transmitting personal data of customers and parcel recipients to be saved by the parent company in the United States. Because the US does not have adequate data protection laws, the data importer UPS had not agreed to comply with safe harbour regulations (cf. No. 3.2.4), and because no exceptions under the Federal Data Protection Act apply, I asked UPS to make its data transmission and processing conform with data protection by acquiring the consent of affected parties or applying binding guidelines pursuant to Article

4c para. 2 of the Federal Data Protection Act. UPS decided to compile internal company guidelines for data transfer based on the EU standard contract clauses of 27 December 2001 (EC Data Protection Directive 95/46/EC). After extensive negotiations, the company supplemented its regulations so that there was now proof of adequate guarantees. As a result, I approved data transmission pursuant to Article 4c para. 2 of the Federal Data Protection Act in the summer of 2003.

Article 4c para. 2 of the Federal Data Protection Act clearly assigns me the authority to approve of transmission of postal and telecommunications customer data. However, postal and telecommunications service providers gather personal data not only on customers, but also on employees. The responsibility for monitoring compliance with data protection law in connection with employee data lies with the relevant supervisory authority for the private sector. But in order not to delay the approval procedure and thus block the company's ability to act, I also approved the transfer of employee data in consultation with the states' (*Länder*) supervisory authorities in March 2004 after the company submitted another contract.

22.2 The transparent passenger

The last word about the agreement between the EU and the US on the processing and transfer of PNR data by air carriers to US Customs and Border Protection (2004/496/EC) has not yet been spoken.

On 17 May 2004 the European Union concluded an agreement with the US on the processing and transfer of PNR data by air carriers to US Customs and Border Protection (2004/496/EC). This had been preceded by the Commission's statement of 14 May 2004 following lengthy and difficult negotiations to the effect that the level of protection guaranteed by the competent agency, US Customs and Border Protection, was adequate.

The Agreement finally put the data transmission practised since March 2003 on a legal footing, but I have serious reservations with respect to the agreements reached and the type of data transmission practised. In a number of points the Agreement does not seem balanced to me because it takes insufficient account of the interests of affected parties under data protection law. Because of reservations of this kind, in June 2004 the European Parliament asked the European Court of Justice to review the Agreement. A decision is expected in 2005.

During the negotiations between the Commission and the US, the Article 29 Working Party (cf. No. 3.2.1) repeatedly expressed its opinion. Some of the Working Party's demands were then taken into account, but others were not. For example, the purpose of data transmission is still much too broadly defined in the Agreement. It now includes preventing and combating terrorism and other serious crimes, including organized crime, without defining these more precisely.

Nor do I agree with the extent of the data to be transmitted. Although the US has cut the list of data categories from the original 38 to 34, this is still much more than the 19 data categories that the Article 29 Working Party considers adequate for the stated purposes. There are also still problems with regard to sensitive data, such as information on race, health, political and religious beliefs that can be included in general data categories. Although the agreements require the US to filter out such sensitive data, the European data protection authorities are not yet convinced that this is being carried out fully.

At the urging of the Article 29 Working Party, the original retention period of 50 years was reduced to 3-½ years, but even this period is excessive.

The US authorities receive the passenger data in what is known as the “pull” method of transfer, i.e. by accessing the airlines’ booking systems. In the process they access the complete data record available for the individual passengers. In individual cases, this can actually be more than 34 data elements. From the outset the Article 29 Working Party therefore called upon the airlines to install filter software ensuring that only the 34 data elements agreed in the Agreement are transmitted using the “push” method and that sensitive data are filtered out at the same time.

The European data protection authorities have agreed on uniform information texts, so that all airline passengers travelling from Europe to the US are now comprehensively informed about how their data will be handled in the US and their rights, irrespective of their destination or nationality.

In the reporting period the Commission also conducted negotiations with Canada and Australia about agreements concerning the transmission of passenger data. The Article 29 Working Party is also carefully monitoring these negotiations.

27.3 The International Conference of Data Protection and Privacy Commissioners

The 25th and 26th International Conferences of Data Protection and Privacy Commissioners in Sydney and Wroclaw focused on a number of international issues and adopted more resolutions than in any previous reporting period.

The 25th and 26th International Conferences of Data Protection and Privacy Commissioners took place in Sydney from 10 to 12 September 2003 and in Wroclaw from 14 to 16 September 2004, respectively. As in previous years (cf. most recently 19th Annual Report No. 32.5), the conferences brought together representatives of data protection authorities from all over the world with representatives of international organizations and from academia, business and public administrations for a wide-ranging exchange of opinions.

The 25th International Conference in Sydney bore the motto “Practical Privacy for People, Government and Business” and adopted resolutions on the following subjects:

automatic software updates (cf. Annex 4),

transfer of passenger data (cf. Annex 5),

data protection and international organizations (cf. Annex 6),

improved communication of data protection and privacy information practices (cf. Annex 7), and

radio-frequency identification (cf. Annex 8).

The use of radio-frequency identification technology, its impact on citizens’ privacy and the resultant challenges for data protection was also one of the main issues at the 26th International Conference in Wroclaw (cf. No. 4.2.1). In addition, out of the large number of subjects dealt with, special mention should be made of the issue of balancing the needs of public security and the affected parties’ fundamental rights — in this connection a

representative from the US Department of Homeland Security spoke at first hand about the requirements of the US Patriot Act — and of the discussion of topical issues relating to the risks to privacy from print media and the Internet and from political marketing.

The Wroclaw International Conference passed resolutions

on a draft ISO Privacy Framework Standard (cf. Annex 9)

on amending the decision of the 2003 Conference on Automatic Software Updates (cf. Annex 10)

on accrediting further participants in the International Conference on Privacy and Personal Data Protection (Accreditation Resolution, cf. Annex 11).

The globalization of data processing and its consequences for data protection was an important topic. In view of all previous, regionally limited approaches, I described the need for effective, global data protection and explained that following the great success of European data protection, we now have to deal with the issue of global data protection which is binding under international law.

The next International Conference, which is scheduled to be held in Montreux, Switzerland, in September 2005 under the motto “The protection of personal data and privacy in a globalized world: A universal right respecting diversities” will give us the opportunity to do this.

27.4 Organization for Economic Cooperation and Development (OECD)

The OECD is showing great interest in cooperation with the Article 29 Working Party and the national supervisory authorities. The OECD supports the European data protection position on biometric data in travel documents.

During my meeting with representatives of the OECD in Paris in June 2004, I was gratified at their great interest in working more closely with the national data protection supervisory bodies and the Brussels Article 29 Group (cf. No. 3.2.1). As chairman of the Article 29 Working Party I was especially pleased about their proposal to hold informal consultations or meetings, perhaps in the form of workshops, on subjects of joint interest. Special attention should be given to the joint work of the OECD and the International Civil Aviation Organisation (ICAO) during the reporting period on draft guidelines for the use of biometric data in international travel documents (cf. No. 6.2 on biometric data in passports and visas). The OECD's main aim is to harmonize the objectives and results of the many international working projects on biometric data. In this connection, the OECD sets great store by agreement with the conclusions of the Article 29 Working Party in its Opinion No 7/2004 of 11 August 2004 (WP 96, cf. box to No. 3.2.1).

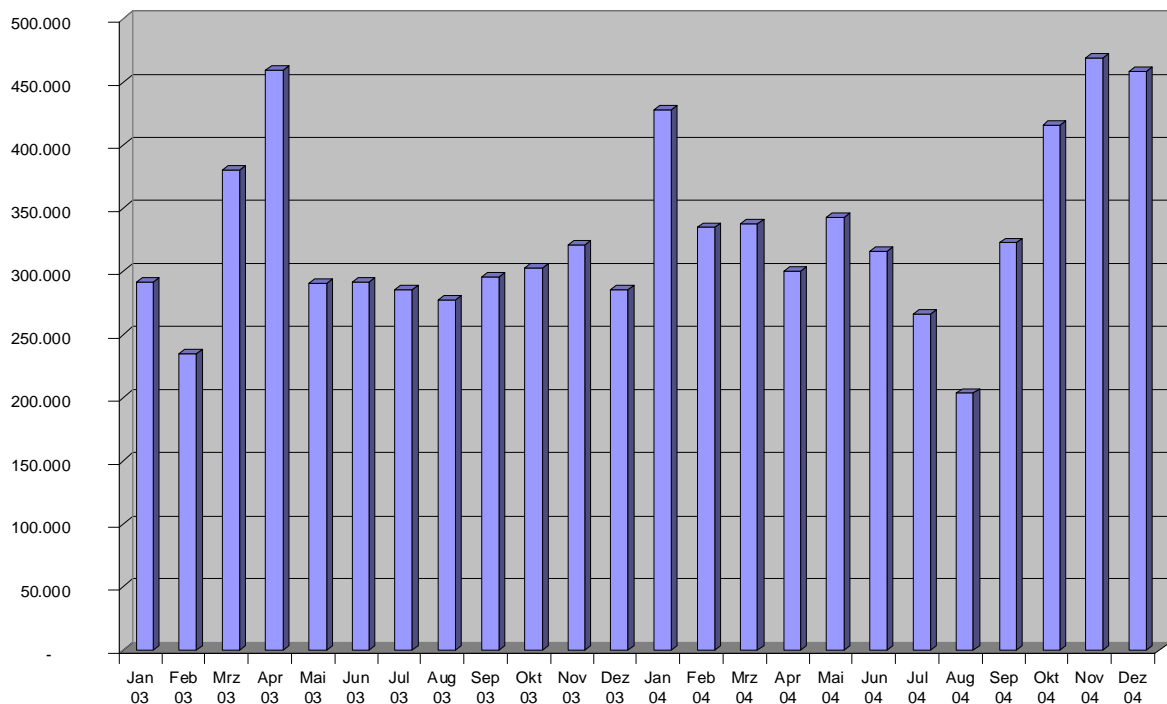
28.2 The Data Protection Commissioner on the Internet

The information offered by the Federal Commissioner for Data Protection on the Internet attracts a large number of users. The homepage of my office can be reached at the address www.bfd.bund.de or www.datenschutz.bund.de.

In addition to conventional means of public relations, the Internet is constantly gaining in importance as a general information and communications platform. This is why expanding my office's Internet presence has high priority for me.

The website of the Federal Commissioner for Data Protection already contains a wide variety of current information (in particular press releases, speeches, resolutions of the International Conference of Data Protection and Privacy Commissioners, and a calendar of events) and various fundamental texts (e.g. laws, guidelines for data security, annual reports from the Federal Commissioner for Data Protection and European data protection supervisory institutions).

In the reporting period approx. 7.9 million page views were recorded. That corresponds to an average of 10,800 page views per day.



Most visitors (approx. 75%) were recorded in the section containing documents on data protection, including annual reports, the five information brochures from the Federal Commissioner for Data Protection Info, resolutions from the data protection conferences and relevant laws and ordinances.

The website of the Federal Commissioner for Data Protection is constantly being updated to increase the information on offer and improve usability by adding new functions that make the diverse information easier to access. For example, in December 2003 a search engine was added, making it easier to find specific information.

An interactive form has been available since October 2004, allowing members of the public to send messages in protected form to me over the Internet. The application was developed in conjunction with the Federal College for Public Administration and ensures that sensitive message data are encrypted, protecting them against monitoring or alteration by unauthorized parties during transmission.

These measures and other planned improvements have been coordinated with the Federal Government's e-government project BundOnline 2005. In mid-2004 I set up a project group designed to further expand and optimize the BfD website, with particular emphasis on making it easier to access the available information.

The "Virtual Data Protection Office" also plays an increasing role in the public perception of data protection. This institution was initiated by Helmut Bäumler, the former data protection commissioner for the state of Schleswig-Holstein and, with my participation, continues to be operated by ULD Schleswig-Holstein (www.datenschutz.de). It is intended to improve cooperation between data protection authorities and is also a good starting point for Internet users interested in data protection.