Financial Privacy and Data Protection in Europe

Alfred Büllesbach

INTRODUCTION

This chapter provides a perspective on data protection in Europe, using German laws and the European Data Protection Directive as models for a pan-European financial-privacy and security regime. Section I introduces the principles of European data protection, recognizing the similarities and differences in legal regimes among European Union countries. Section II describes the relationship between data protection and bank secrecy, showing why the two do not conflict. The requirements for processing and using personal data in Germany are outlined in Section III. Section IV discusses the applicability of German law to financial-services providers, while Section V outlines the conditions imposed on financial institutions that collect, process, and use personal data. Section VI describes the conditions for transfers of personal data to third parties, including data exchanges within the credit-protection system. Section VII stresses the importance of the legal entity that conducts data processing on behalf of others. Section VIII discusses cross-border data flows and payment transactions. Additional obligations of financial institutions as data controllers and individuals' rights are covered in Section IX. Section X concerns the distribution of financial services via such new media as the Internet. The supervisory requirements for data-protection activities, and the role of the corporate data-protection officer, are described in Section XI. Finally, Section XII discusses data protection as a self-regulation task and a challenge for global companies.

I. PRINCIPLES OF DATA PROTECTION IN EUROPE

Despite differences among the different countries in Europe, generally, the concept of data protection in Europe: takes the form of a system of regulation governing the collection, processing,

and use of personal data; grants specific rights to individuals affected by data processing; and imposes obligations on individuals responsible for data processing. This approach is very different from that of the United States. The objective of European data protection is not the protection of data, but rather the protection of the personal rights of those whose data is being processed. The essential core of data protection in Europe is described in the German Federal Act on Data Protection (Bundesdatenschutzgesetz—BDSG) as follows: "The purpose of this law is to protect the personal rights of individuals from becoming infringed upon by the use of their personal data."

The development of Europe's approach to data protection stems from specific historical and political experiences with dictatorial systems of power in parts of Europe. But today, the progressive development in the area of information technology plays an important role.

The early phase of electronic data processing was influenced by the use of mainframe computer systems, which instigated the fear of citizens being watched by "Big Brother" during widespread data collection and processing. The progressive technical development in the information-technology area and especially the increasing interconnection of computers will continue to simplify the collection and gathering of information, and intensify its processing and use.

Attempts to regulate these developments resulted in the enactment of data-protection laws in the 1970s. The German province of Hesse adopted the first law in 1972, while Sweden was the first European country to enact a data-protection law, in 1973. In the population-census order of the Federal Constitutional Court in 1983, the highest German court developed the "right to informational self-determination" so that individuals could decide what others, especially the government, were allowed to know about them.

The right to informational self-determination acts as a right of the concerned party to defend himself against those who seek to collect and process data about him. When infringed, this legal construction creates compensation claims for misused informa-

tion, provisions for rectification, and damages. The law also includes other basic rights that protect the personality. For example, there are legal protections for securing telecommunication secrecy. Parallel to this, extensive data-protection legislation has developed that includes area-specific regulations for processing personal data.

In the past, area-specific regulations mainly addressed the public sector; but now there is a tendency to regulate the private sector, especially in the area of innovative information and communication technology. In this context, the Telecommunication Act is noteworthy, as section 11 codifies data-protection requirements in the telecommunication area. In addition, data-protection regulations in the Teleservices Data Protection Act (Teledienstedatenschutzgesetz—TDDSG) govern institutions that provide "telebanking." The TDDSG is part of the Information and Communication Services Act (Informations- und Kommunikationsdienstegesetzes—IuKDG) enacted in 1997. Credit institutions and financial-service providers must observe effective data-protection regulations when collecting, processing, and using personal data, and they must also provide their services so the right to informational self-determination of the parties affected by data processing is not infringed.

In Europe, the right to data protection is generally recognized as a human right, as described in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The establishment of data-protection requirements in the respective national legal systems can vary. In Denmark, for example, the data-protection law[1] that applies to the public sector differs from the data-protection law for private enterprise.[2] A general data-protection law with regulations for the public sector contained in a special paragraph exists in Luxembourg,[3] the Netherlands,[4] Austria,[5] Switzerland,[6] and Spain.[7]

In Germany, the BDSG provides specific regulations for the public sector while it also regulates the authorization of processing personal data by private corporations. The control of data protection at federal agencies is exercised by the Federal Data Protection Commissioner. Private corporations or institutions

processing personal data are supervised by the responsible authority according to national law. Owing to the federal structure of Germany, the individual Länder (states) also have extensive data-protection regulations, which are carried out by the Länder administrations.

There are no distinctions between the rules governing the public and private sector in Belgium,[8] Estonia,[9] Finland,[10] France,[11] Greece,[12] Great Britain,[13] Ireland,[14] Italy,[15] Norway,[16] Poland,[17] Portugal,[18] Russia,[19] Sweden,[20] the Slovak Republic,[21] the Czech Republic,[22] and Hungary.[23]

Besides regional and national data-protection regulations, international regulations also must be considered. These regulations are not represented in the form of directly-effective law for lack of direct domestic applicability to financial-service providers. In 1981, the Council of Europe passed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, which contains suggestions for the formulation of national data-protection laws. Following its ratification in 1985, this international agreement at first was enacted in only the following five countries: France, Norway, Sweden, Spain, and the Federal Republic of Germany.

On October 24, 1995, the Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data was enacted. Not all member states have carried out this directive, which was supposed to have been incorporated into the various countries' national laws by October 24, 1998. Parallel to the EU Data Protection Directive, the so-called Telecommunication Data Protection Directive[24] had to be implemented, a process that still has not been successful in Germany. The implementation will become relevant for financial-service providers with regard to Article 12, which regulates the authorization of unsolicited telephone calls.

After complete implementation of the Data Protection Directive, a standardized legal data protection will be created in the member states. Data can then be transferred directly within the EU domestic market, facilitating the cross-border flow of

financial data within the EU. But transferring data to so-called third countries remains problematic under legal data-protection standards, and is only authorized when the third country shows an adequate level of data protection corresponding to the EU standard. In June of 2000, representatives of the United States and Europe reached an agreement on privacy principles that US companies operating in Europe could adopt to get a "safe harbor" from liability under EU law.

The Signatory Act[25] establishes general requirements for the secure use of digital signatures in legal and commercial transactions. On December 13, 1999, the Directive of the European Parliament and Council Regarding Common General Requirements for Electronic Signatures was adopted and was ultimately enacted on January 19, 2000. The objective of this directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. While implementing this objective, the guideline distinguishes between "electronic" and "advanced electronic" signatures. For advanced electronic signatures, technical and organizational requirements for "certified service providers" and for producing these signatures are formulated. The directive must be implemented into national law by July 19, 2001, and will result in changes in the signature law.

An additional EU directive regarding distance marketing of financial services is under development.[26] This is designed to provide a smoothly operating and secure domestic market for these services for consumers and financial-service providers. The directive does not affect those rights granted to consumers by community regulations regarding the protection of personal data and the private sphere.

In September, 1999, the European Commission presented an Amended Proposal for a Directive of the European Parliament and Council regarding specific aspects of electronic-payment transactions in the domestic market ("E-Commerce Directive"). The draft, in consideration reason (20), refers to the obligation of member states to create secure communication requirements for the consumer resulting from Community regulations ensuring the protection of personal data and the private sphere.

II. THE RELATIONSHIP BETWEEN DATA PROTECTION AND BANK SECRECY[27]

Under standard business conditions, banks are usually bound to secrecy regarding all customer-related facts and values. This bank secrecy is a product of the contractual relationship between bank and customer, while data protection is imposed by act of law, for example, by the BDSG. The contractual obligation to secrecy does not refer to any special official or professional. Nevertheless, bank secrecy is granted a special position,[28] as it is legally recognized in investigations conducted by the Internal Revenue Service (IRS). It may restrict the investigative authority of the IRS on the one hand and the bank's obligation to disclose information to the IRS on the other hand. The obligation to disclose information is required only in criminal tax proceedings and other exceptional cases found in Section 30 of the Tax Code. The IRS must pay particular consideration to the trust relationship between the credit institutions and their customers when investigating the facts of a case.

Data protection and bank secrecy represent two independent entities that do not oppose one another. Rather, they co-exist as long as they do not overlap. Before a bank discloses customer data to third parties, it must observe both sets of legal obligations, at least when its customers are natural persons, for the BDSG protects, unlike bank secrecy, only natural persons.[29] Unlike bank secrecy, predominately relevant only in connection to third parties, data protection also regulates the collection, storage, changing, or use of data (*e.g.* for marketing purposes) by the bank.

III. PRINCIPLES FOR PROCESSING PERSONAL DATA IN GERMANY

The following central principles must be observed under the BDSG when processing and using personal data:

- ensuring the existence of specific legal authorization or consent by the concerned individual;
- observing the principle that data should not be used for purposes for which it was not collected;

- binding employees to data secrecy;
- observing the rights of individuals with regard to notice, access to their files, the rectification of errors, the timely deletion of files, and objections to direct marketing;
- assuring technical data security.

Several principles of modern data-protection law are found in the new BDSG, such as prevention (the principle of processing as little data as possible) and economizing. Compliance with these principles is monitored. Internal data-protection control is the duty of the corporate data-protection officer. Externally, authorities appointed by national law must exercise supervision, control authority, and monitor compliance with registration obligations (to which specific data-processing centers, especially corporations that process data by order of others, are subject). All parties concerned, including individual consumers, can bring issues before these authorities. A monetary fine will be imposed for violations of the regulations, which could lead to the enforcement of claims for damages.

IV. APPLICABILITY OF GERMAN LAW TO FINANCIAL-SERVICE PROVIDERS

Sectors of Application

The general provisions of the BDSG, as well as specific regulations for the private sector (Sections 27-38), apply to financial-service providers under private law in the absence of special data-protection rights for this sector. The regulations for public institutions (Sections 12-26) apply to federal credit institutions operated under public law, such as the Deutsche Bundesbank. In addition, credit institutions of the Bundesländer organized under public law, the Land Banks, are subject to the data-protection laws of the ir respective Land. The following refers to financial-service providers as private enterprises.

Territorial Area of Application

Unless the data processing occurs within the national territory of the Federal Republic of Germany, the BDSG applies

according to the territorial principle. This remains true even if a phase of processing such as storage occurs domestically. The BDSG is also relevant when data are collected through an affiliate branch of a bank in a foreign country, but are stored by a domestic branch.

After the implementation of the EU Data Protection Directive, data collected through a domestic, independent subsidiary in Germany and processed in a foreign country will also be subject to the BDSG. The location of data processing will no longer generally determine which national data-protection right is effective but, rather, the location of the processing officer. A member country should allow the "export" of its citizens' usual data-protection rights within the commercial territory of the EU without being restricted by unfamiliar data-protection regulations of other countries. The BDSG draft[30] formulates this as follows:

> This law is not applicable if the responsible location situated in another Member State of the EU collects, processes or uses personal data domestically, in other words, this is carried out by a domestic establishment. This law is applicable as long as the responsible location situated outside the EU acquires, processes or uses data domestically.

These provisions are not effective if foreign locations have domestic establishments.[31] In such cases, they are required to comply with German data-protection laws. They are also not effective in cases in which data collection, processing, and use are carried out within the EU by financial-service providers with headquarters outside the EU, to avoid making a data-protection standard lower than the EU's available to the regulated parties. In these cases, the territorial principle applies once again.

Pertinent Concepts and Definitions

Only "personal data," defined as "detailed information about personal or factual relationships of a specific or definable natural person," are affected. Information about deceased or legal persons is not covered by the BDSG, but could be covered by other

laws, such as those describing general personality rights. The BDSG does not protect aggregated or anonymous data. A person is "definable" when data that does not refer to a person by name can be combined with additional information to supply a personal reference. The account number of a customer, for example, is personal data, since it can assign a numerical sequence of events to an individual person based on its records.

In cashless payment transactions, it can be difficult to clarify the question of personal reference.[32] For example, a retailer participating in an electronic-cash-based procedure based on the promise of payment of a card-issuing institution cannot make any claims against this institution for the release of the name or the address of the card holder, if the data is not available due to an illegible signature or the use of a PIN.

The BDSG applies to specific activities relevant to data protection in the area of private enterprise, such as the collection, processing, and use of personal data, whether these activities proceed automatically or when the data are organized or evaluated in files. "Processing" represents a collective concept, covering storing, altering, transferring, blocking, and deleting.

The law designates as "data controller" each person or organization that stores personal data for its own purposes or has others store the data. The data controller is entirely responsible for the authorization of processing and is the contact partner for the enforcement of rights on behalf of concerned individuals. Consequently, the new BDSG will replace the term "data controller" with that of the "data processing responsible." A bank as a legal entity, for example, is responsible, not the individual employees or the legally independent data-processing agency.

When an employee or agency collects, processes, or uses data under instructions from the controller, these activities do not result in "transfers of data" to "third parties" in the sense of the BDSG (such transfers are only permitted under certain conditions). Since the law is consistent with corporate law, affiliate branches are assigned to the controller; under the BDSG, this will be applicable to domestic branches. Also, the BDSG does not recognize any so-called corporate privileges; associated cor-

porations in a corporate group are considered third parties in relation to one another under data-protection law.

V. CONDITIONS FOR PERMISSIBLY COLLECTING, PROCESSING, AND USING PERSONAL DATA BY FINANCIAL-SERVICE PROVIDERS

The processing and use of personal data is permitted only if a law permits, or when the concerned individual has consented. While the BDSG currently in effect does not subject data collection to this authorization provision, the amendment of the BDSG stipulates that this legal provision will cover all processing phases in the future.

Relevant Legal Regulations Outside the BDSG

The following regulations outside the BDSG are examples of laws that authorize financial institutions to process personal data under legal obligations related to the need for transactional documentation, notice, and information:

- Data collected under Section 31 of the Securities Trading Act about the financial situation of the client should be stored under Section 34 of that act, which regulates recording obligations.
- According to Sections 2 and 9 of the Money Laundering Act (MLA) in connection with Section 154 of the Tax Code, financial institutions must, under their identification obligations, store the acquired data of depositors of cash amounts over 30,000 DM. According to the MLA, this data can be used to fight money laundering, for corresponding criminal-prosecution measures, as well as for information in taxation procedures.
- General accounting or recording obligations (Section 256 of the Commercial Code, Section 319 of the Tax Code) can legitimize data-processing activities according to commercial and fiscal regulations.
- Special data-protection regulations of the Civil Action Code in Sections 915 ff. and the List of Insolvent Debtors Code must be observed when accessing data in the debtors' index at municipal courts and for their further use by credit-information

systems in the credit industry. The SCHUFA,[33] as one of the most important German credit-information systems, is authorized to transfer data from these indexes to establish and manage a private index. The authorized storage duration of such data is restricted.

- The German Banking Act (GBA) requires specific loans, such as large-scale loans of the Deutsche Bundesbank, to be disclosed. Registration obligations under corporate law set out by the GBA may also be relevant.
- In the case of a deceased bank customer, transmission obligations of the bank are applicable to the IRS according to the Inheritance Tax Law (ITL).
- According to Section 45 of the ITL, a credit institution also has informational obligations related to the need for control of investment income-tax payments. The institution also must respect official inspection rights of the GBA and other regulations that impose information obligations in taxation procedures, public-investigation procedures, and criminal proceedings.
- Employment offices have information rights under a means test (Section 315 of the Social Security Code Vol. III) before they agree to pay out unemployment benefits.
- Finally, an institution that acts as an employer towards Social Security carriers also has information-collecting obligations.

In all of these cases, the data must not be used for purposes for which is was not collected. For example, the use of this data for advertising purposes would not be authorized.

Legitimation under the BDSG

Section 28 of the BDSG concerns data processing for an entity's own corporate purposes. Data processing on behalf of other entities and offered as a service, such as credit-information systems or directory distributors, is regulated by Section 29.

Data processing to fulfill a contract with a client. According to Section 28, storing, changing, transferring, and using personal data under contractual obligation to the con-

cerned customer is permitted. The financial-service provider is authorized to process and use all data required to carry out the services requested by the client. The decisive contractual relationship for the purpose of the requirement may be seen not only in individual contracts, such as processing an electronic-payment transfer or a credit-card transaction, but also in an invested long-term business connection.

Looser contractual-promise relationships are equivalent to contracts, provided a concrete contract initiation is discussed. For example, a financial institution's one-sided appeals or advertisements for new customers would not be relevant. Under a current account agreement (for, say, a checking account), the following information would be relevant in addition to the basic data of the customer such as name and address: credit line, conditions, securities, credit standing, as well as marital status, income, assets, liabilities, and prior convictions. Should the customer only be interested in accumulating assets in a savings account, relevant credit-standing data cannot be retrieved by the financial institution in the absence of the possibility of an overdraft.

The gathering of customer data common in the credit-card industry for the purpose of producing user profiles should be included under specific requirements of credit-card contracts. This gathering is supported by the fact that unusual transactions are quickly recognized, cards are blocked earlier, and the liability risk of the customer is minimized. Based on the earmarking principle, other uses such as a targeted customer appeal in the form of special personalized offers would be excluded; these uses would no longer be covered by the original contract. The disclosure of bank-customer data to third parties for advertising and marketing purposes would also be unauthorized, unless the customer consents to this disclosure and the bank is no longer bound by bank secrecy.

Data processing and use without contract or when exceeding contract. If neither a contractual relationship nor a similar contractual-promise relationship exists, or if personal data is used beyond what the contractual relationship permits,

for example, for advertising purposes, data use is permitted according to Section 28 of the BDSG. Such use is allowed when it is required to preserve the justified interests of the financial institution and there is no reason to assume that the protection-worthy interest of the concerned individual regarding the exclusion of data processing or data use predominates.

Justified interest of the financial-service provider not only is considered in the case of legal concern, but also when it concerns a purpose carried out according to the general sense of justice according to economic, social, or cultural needs. This is especially true for the economically-important area of marketing.

The establishment of a noncustomer file for expansion purposes, to enable offering target-group-oriented products or services based on these data, would be permitted if the data were legally acquired from another location such as a directory distributor, or when the data originate from generally accessible resources (*e.g.* address and telephone books) and the use does predominate over the protection-worthy interests of the concerned party.

In practice, the balancing of interests required by law is predominately handled in summary. One can simply assert that the processing and use of data for advertising purposes are authorized so long as the opposing interests of the concerned individual do not obviously predominate, as they would if the customer made use of his objection right according to Section 28, Paragraph 3 of the BDSG. Implementing the EU Data Protection Directive will intensify these obligations, as concerned parties must be informed by the time of the first contact[34] about the origin of their data and their right to object to the data being used for the purposes of advertising, marketing, or public-opinion survey.

The use of customer data from a contractual relationship to produce behavioral or personality profiles for general advertising purposes may often represent an excessive encroachment on the informational right to self-determination of the customer. This authorization barrier must be especially observed in view of data-warehouse and data-mining concepts for advertising pur-

poses.[35] A detailed evaluation of personal data that causes the client to become a "transparent" target of advertising measures need not be tolerated.

Credit scoring and "Automated Individual Decisions" under the EU Data Protection Directive. In the current version of the BDSG, the use of personal data by computer-supported decision processes is not specifically regulated. During a scoring procedure, a score value is generated from a database by mathematical and statistical procedures that give the probability of a specific event occurring. The question of how relevant this procedure is to data protection is controversial.

The banking industry holds the belief that the prognosis summarized in a score value does not represent an appraisal of the credit standing of a concrete customer.[36] But the data-protection supervisory authorities argue that by establishing a score value, the data of the concerned party would be expanded by a value. This value would be based merely on the experiences with credit histories of other customers, and would provide a comparison with other customers by assigning a position within a reference group to the concerned customer.[37]

Article 15 of the EU Data Protection Directive will be included in the German act, which regulates the authorization of "automated individual decisions." Each person will have the right

> not to be subjected to a decision having legal consequences or one that would cause considerable infringement, which is exclusively issued based on an automated processing of data for the purpose of evaluating individual aspects of a person, such as career capabilities, credit standing, reliability or behavior.

While one may argue the scoring procedure is merely a decision tool of loan officers, whose personal evaluation of the overall situation determines the final outcome, the future BDSG explicitly stipulates that credit scoring should be regarded as an automated individual decision. The banking industry will have

to adjust to this, perhaps by granting internal complaint possibilities to concerned parties.

The Importance of Consent

The permission standards within and outside of the BDSG are equivalent to a consent by the customer. Customer consent is frequently used to legitimate data processing, especially in the banking area, even when the processing of the customer's data without explicit consent would be legitimized because of the contractual relationship. In such cases, the consent is of declarational importance, especially when it is connected to relevant legal regulations as well as to the type and extent of processing.

The extent of the authorized processing can be expanded with written consent. Verbal consent over the phone or a "mouse click" is not sufficient. An exception allowing "electronic" consent in the area of home banking and only applicable when using digital signatures is contained in Section 3 of the Teleservices Data Protection Act.

Pre-formulated consent statements are usually a component of a contractual agreement and are subject accordingly to content control under the Act on General Commercial Requirements (AGBG). A violation of the AGBG occurs when the pre-formulated consent is too generalized, when consent should be asked for each processing of all data, or if nothing is said in regard to the purpose of processing.

In addition, the customer can be disadvantaged in connection with the use of the consent. For example, when an application to open an account includes a pre-formulated statement saying the customer agrees to the transfer of his data to cooperation partners of the bank in the corporate group (so-called corporate group clause), a violation against the AGBG has occurred in most cases. Since the BDSG does not recognize corporate privileges, but rather considers each legally-independent corporation as an independent data controller, such a generic corporate clause would lead to a situation where the group of those able to use his data would not be clear to the customer.

A clause is considered legal when it clearly reveals that the granting of an approval is optional and that the opening of an account is not dependent on whether the customer decides to release his data throughout the corporation. In this connection the "corporate clauses" or the "exclusive financial clauses" developed by the Central Loan Committee in cooperation with the Data Protection Supervisory Authority of the German Bundesländer represented in the "Düsseldorf Group" are an example.

The SCHUFA clause, in which the customer would agree that the financial-service provider may transfer to the Credit Protection Organization data the customer already released by filling out specific applications (for example, for opening an account or granting financing aid), has come under review by Germany's highest court. It was noted in criticism that the consent regarding the transfer of "data of the borrower when processing a loan" disregarded the determination order. The banking industry requires that clauses be distinctly formulated and include a notation regarding the extent of the data transfer.

Still unclear is the question whether this ruling concerns a pre-formulated statement subject to content control according to the AGBG, when the financial institution requests that the customer state whether he agrees to be informed by phone about new products and services by checking either "yes" or "no." Since a high-court decision has not yet been issued regarding this question, the banking industry has refrained from including such a telephone-advertising clause in the General Commercial Requirements.

VI. CONDITIONS FOR TRANSFERRING PERSONAL DATA TO THIRD PARTIES OR DATA EXCHANGE WITH CREDIT-PROTECTION SYSTEMS

The transfer of customer data to a credit-protection organization is not regularly supported by a contract with the customer. Consequently, this requires the balancing of justified interests between the institution, a third party, or the general public,[38] and the protection-worthy interests of the customer. Bank secrecy is not an indication of an opposing interest of the customer, since

the customer has released the credit institution by the signature of the SCHUFA clause.

The basic interest of the credit institutions connected to a credit information or protection system is to transfer data regarding the nature, number, and extent of current liabilities, to facilitate the evaluation of the credit standing of a customer interested in obtaining credit. For this purpose, the regional SCHUFA organizations have been established. According to the principle of mutuality, these organizations provide credit information on the condition that corporations requesting their services are obligated to contribute and update necessary data on behalf of the system.

The transfer of data from the database of the SCHUFA organizations is based on the justified interest of associated corporations in the sense of Section 29, Paragraph 2 of the BDSG. Not every economic risk would be a reason for data to be retrieved. While a contractual partnership with SCHUFA is now restricted to corporations granting money and product loans (with an exception for cellular phone providers, whose credit risk is considered comparable), the group of contract partners will be wider in the future due to the development of a new system.[39]

In connection with the cooperation regarding a credit-protection system, the purpose-binding principle must be considered, according to which the receiver of data is allowed to use such data only for immanent system purposes.

Despite the basically justified interests of the institutions connected to the system, it remains necessary to balance others' interests in each incidence. In view of the consequences that the transfer of specific data can have for credit applicants, a distinction must be made between the "hard" and "soft" credit-standing data. Hard credit-standing data, such as the opening of a bankruptcy proceeding or the affidavit of the debtor according to Section 807 of the ZPO by which his insolvency is known to the court, can be transferred. But the transfer of soft credit-standing data from or to the credit-protection system must be preceded by a concrete individual-case inspection. A situation where soft data is used is when a lender has cancelled a standing credit and is

involved in a lawsuit with the borrower regarding the right of credit cancellation.

Also, the SCHUFA is obligated to document all retrievals from their database. If the data transfer occurs in an automated procedure, the retrieving location (the financial institution) must carry out the recording obligation.

VII. THE LEGAL ENTITY DOING "DATA PROCESSING ON BEHALF OF OTHERS"

When personal data is transferred from one data controller to another, this represents a data transfer according to Section 3 of the BDSG. This processing stage, like others, is subject to authorization conditions. An exception is granted when data is given to an entity such as a service center with the order to process or use such data for the controller, who remains responsible for obtaining legal authorization, especially in the case of information from an external concerned party. Section 3 clarifies that the contractor is not a "third party" in relation to the customer. The following criteria are prerequisites for authorized data processing on behalf of others:

The controller must carefully select the contractor to carry out the order according to instructions. The placing of an order must follow in writing. The individual processing phases must originate with the order; so must technical organizational measures with which the contractor must ensure the requirement to maintain data security is carried out. Furthermore, the controller must make sure the contractor complies with his registration obligation to the supervisory authority.

The contractor must also ensure that his employees adhere to confidentiality obligations when handling data and must appoint a data-protection officer. In addition to technical and organizational operation of data-processing centers, typical services of a contractor can also include carrying out market analysis with data prepared by the customer or creating technical requirements for home banking.

When complete corporate functions are outsourced, the legal framework for data processing on behalf of others is no longer

applicable. If the contracted corporation acts as the responsible party, taking over the payroll or salary accounting and bookkeeping duties, such a service is no longer designated as a supporting (technical) help function. The necessary data-transfer rules relevant to a *de facto* transfer are then subject to the requirements according to Sections 4 and 28 of the BDSG.

When outsourcing, the Banking Act must be observed, under which the financial institution must obtain the legally-required instructional authority on a contractual basis and incorporate the transferred areas of responsibility under control procedures.

Under Section 3 of the BDSG, foreign contractors are handled as third parties. After the implementation of the EU Data Protection Directive, the treatment of foreign contractors must be differentiated from that of domestic contractors as follows: Service providers located in an EU member state are treated like domestic contractors[40] based on the achieved reconciliation of privacy-protection standards. For contractors outside the EU, the general regulations as well as the requirements concerning data transfers in third countries apply.

VIII. CROSS-BORDER DATA AND PAYMENT TRANSACTIONS

So far, the BDSG includes no special regulations governing the transmission of personal data to nonofficial bodies abroad. However, ultimately, the same conditions apply to cross-border as to domestic transmission of data.[41] The person affected by the transfer must give his consent if the transmission has not been legitimized by a legal provision under the BDSG or otherwise.

One law that falls within this category and is particularly important to financial institutions is Section 44a of the Act Regulating Banking and Credit Business (Kreditwesengesetz—KWG).[42] Under this requirement, institutions with at least 20 percent of their shares held by a company domiciled abroad must pass on to this company all data required for fulfilling the provisions in the recipient country relating to bank supervision.[43] In addition to global figures, this may include data on borrowers, for example, notification of individual loans of one million or more Deutschmarks. Otherwise, the persons involved must give

their consent if transmission is not legitimized. In international data transactions, however, this will often be the case, since executing a transfer or other noncash transaction is part of the purpose of the contract with the customer, so that reference can be made to Section 28, Paragraph 1, Number 1 of the BDSG.

Within the European payments system these transactions will be processed by Gesellschaft für Zahlungssysteme (GZS) (Eurocheques, Euro/Mastercard and Visacard). To the best of my knowledge, there is no special data-protection or data-security policy for either this organization or for the SWIFT system; if data transfer is needed in order to fulfill the terms of a contract, additional admissibility conditions do not need to be observed.

However, the situation is different if the data transfer is only indirectly linked to the customer, for instance, if a bank uses a service center in another country. Although the cost savings that can be achieved through this may be of indirect benefit to the customer, ultimately the bank is acting here in its own interests and is required under Section 28 of the BDSG to weigh these interests against the affected customer's need for protection. This may mean a reasonable standard of protection needs to be defined at the outset.

Although a uniform internal market will have been created once the EU Directive on Data Protection has been implemented, the situation will remain unchanged as far as nonmember states are concerned. In other words, providers of financial services may only transfer data to countries demonstrating a reasonable level of protection. In the absence of such a level of protection, an exception will be needed. The same questions arise here as for all companies participating in international data transactions.[44] For this reason I will not enter into any greater detail here on the "third countries discussion."[45]

IX. ADDITIONAL OBLIGATIONS OF FINANCIAL INSTITUTIONS AS DATA CONTROLLERS, AND THE RIGHTS OF INDIVIDUALS

In addition to the requirements discussed, all data controllers must require employees involved in processing personal data to

observe data secrecy, that is, to ensure confidentiality. Moreover, the clearly-specified requirements of data security set out by the BDSG must be guaranteed by both the controller and the contractor by deploying suitable technical and organizational measures.

In the interests of effective data protection, the BDSG guarantees affected individuals various rights. Individuals' rights to access gives them the right to find out about data stored regarding them. If the data are incorrect or outdated, the individual may require correction under Section 35 of the BDSG. If storage of individuals' data is impermissible or no longer permissible,[46] or if there is a dispute about the data's accuracy, individuals may require deletion or blocking. Attention has already been drawn to the right to object to direct marketing.

Asserting these individual rights assumes the affected party is aware of the use of data in question. For this reason the law requires notification of affected parties in cases where the individual does not know his data were being processed. In the loans business, for instance, notification may be unnecessary since processing of data can be regarded as normal practice in the industry.

Access to data must be requested by the person affected, and this person is required by law to specify what his request applies to. The right to access does not have the same scope as the right of freedom of information. The right to access affects the following information: the purpose of storage, the origin of data, and, possibly, the recipient of data, if regular transmissions are made to this recipient. If the right of access is used in a malevolent or troublemaking fashion, it may in exceptional cases be refused.[47] Information is provided free of charge. If the information is not provided within a reasonable period of time or not provided accurately, the claim may be asserted in a civil court.

In the event of contraventions of data-protection obligations, the BDSG provides for criminal penalties and fines, and eases requirements on the provision of evidence for affected parties when they assert their compensation claims in court.

A number of new requirements will be included in the new BDSG. In this respect, the new provisions on mobile storage

media (chip cards) will be particularly relevant to banks. According to the EU Directive on Data Protection, chip cards must be submitted to prior data-protection checks by the corporate data-protection officer. In addition, the supervision of premises open to the public using optical-electronic installations will also be regulated by law for the first time.[48]

X. DISTRIBUTION OF FINANCIAL SERVICES VIA NEW MEDIA

Financial institutions are turning increasingly to new media to rationalize existing business processes and open up new financial-services markets. The legal conditions under which this may be done are governed in Germany by the IuKDG.[49] A significant element in this act is the Teleservices Act (Teledienstegesetz—TDG), covering, in particular, the issue of freedom of entry, providers' obligation to identify clients' and providers' responsibilities, as well as defining the concept of teleservices. The data-protection requirements imposed upon providers of teleservices are laid down in the TDDSG, whose provisions take precedence over the more general BDSG. Finally, the Digital Signature Act (Signaturgesetz) should be mentioned. This creates the conditions that ensure safe use of digital signatures in legal and business transactions. It is worth noting that the opportunities opened up by the law have been little used to date.

The relevance of these relatively new laws is not limited to home banking in its narrow sense, extending to all financial services offered through the Internet, as long as they are "teleservices." With respect to financial-service providers, the TDG defines as teleservices information and communications opportunities offered by financial institutions in which digital data can be used by consumers in electronic online dialogue with the aid of their computers.[50]

The main requirements laid down in the Teleservices Data Protection Act are as follows:

- legal authorization or consent is needed;
- the purpose-binding principle, that information not be used for

purposes other than those for which it was collected, must be respected;
- the principle of user autonomy must be respected;
- the principle of data thrift must be respected;
- the principle of notification before consent must respected;
- electronic consent is introduced.

Data-protection obligations on the part of teleservices providers to be stressed are:

- to facilitate anonymous use and use based on a pseudonym if economically reasonable;
- to secure data protection using information technology;
- not to create user profiles related to individuals;
- to observe regulation with regard to the use of contract, connecting, and billing data;
- to provide a right of access that can be electronically requested and granted.

The law formulates special data-protection regulations based on the specific features of teleservices. A key feature here is the ban on creating user profiles.

Irrespective of the requirements defined by law, increasing awareness of data protection and security matters amongst customers, especially with respect to use of the Internet, has created a customer need for safer financial services designed in a manner that complies better with data protection. In particular, plans for safeguarding authenticity, integrity, and confidentiality are essential, in view of the high potential losses linked with financial transactions, and the potential threats from the use of electronic and networked communications media. With this need in mind, the national industry-standard Home Banking Computer Interface (HBCI) was introduced under the leadership of the Central Credit Committee (Zentraler Kreditausschuss).[51] In this way, bank customers can communicate with the bank computer using their computers to obtain information or conduct transactions such as fund transfers. Security is achieved by encoding

the contents of the message and initialing it with the customer's personal code.

XI. DATA PROTECTION SUPERVISION AND THE CORPORATE DATA-PROTECTION OFFICER

Under the BDSG, compliance with the data-protection requirements by private industry is monitored by the supervisory authorities of the different Bundesländer. The field of telecommunications is an exception, falling within the jurisdiction of the Federal Commissioner for Data Protection. This federal commissioner also shall observe developments in the field of teleservices and comment on these in his report on his activities.

Government supervision distinguishes between supervision based on particular incidents (*e.g.* after a complaint has been received by a person affected) and official supervision. This has the following consequences: Private financial-services providers are checked if there is sufficient indication of an infringement against data-protection regulations. But enterprises that store personal data for the purpose of transmission as part of their operations, or that process them under contract, are officially monitored; in other words, a check can be carried out by the authority without the need for a specific incident. The same applies to the providers of teleservices. In implementing the EU Directive on Data Protection, the non-incident-related form of supervision will be introduced generally for all enterprises.[52] As part of its supervisory process, the authority may utilize its rights of inspection and examination, as well as its rights of direction and intervention.

A corporate data-protection officer must be appointed by all financial institutions with at least five employees constantly working on automated processing of personal data. This position is the interface between the company and data-protection supervision and may be described as a legally-legitimized organ of self-regulation. The law requires the data-protection commissioner to report directly to company management, that he can operate without instructions and can carry out his duties independently. To do so he should be allocated sufficient personnel

and resources. A person with the requisite professional knowledge and personal reliability may be appointed data-protection officer.

Independent companies within a group must appoint their own officers, although prevailing opinion holds that the same officer may be appointed for all or some of the companies if this does not give rise to any conflict of interest. At a minimum, the corporate data-protection officer must safeguard data-protection principles and data security in the enterprise, monitor data-processing programs by random sampling, and train staff involved in the processing of personal data.

XII. DATA PROTECTION AS A SELF-REGULATION TASK AND AS A CHALLENGE FOR GLOBAL COMPANIES

Because economic globalization is occurring in the context of different international legislative regimes in the field of data protection, global companies are likely to adopt self-regulation measures to establish unified data-protection policies, thereby creating or specifying an appropriate framework for their own business processes. The position of the corporate data-protection officer offers the opportunity to develop plans that go beyond the simple fulfillment of the legal requirements, taking in the business significance of data protection and data security as quality and competition features,[53] particularly in the field of financial services. Approaches of this kind are already available if we read the privacy statements issued by Citibank or American Express.

DaimlerChrysler has also begun developing a group-wide self-regulation plan that would set unified worldwide standards for relevant issues of data protection and data security. In order to define a data-protection standard that is as uniform as possible and can be implemented throughout the group, a Privacy Code of Conduct has been developed, and is now in the approval phase. Initially, this code is limited to customer and supplier data. The aim is to create a uniform philosophy with regard to the management and implementation of data protection and data security in customers' relationships with the group.

DaimlerChrysler has selected a mixture of centralized and decentralized elements for organizing its data protection. The Chief Corporate Data Protection Officer for the Group is empowered to issue guidelines and is supported by decentralized data-protection coordinators in the individual regions and companies of the group. In this respect the Chief Corporate Data Protection Officer for the Group and his staff function as the Competence Center. The independent position of the corporate data-protection officer is intended to guarantee compliance with the self-created system. A uniform Privacy Statement has already been implemented.

The increasing importance of the Internet as the infrastructure for eCommerce is making it necessary for a company like DaimlerChrysler to design its business-to-customer relationships as well as its business-to-business relationships in a data-protection-compliant manner. Privacy enhancing technologies (*e.g.* self-protection measures such as encoding) must be based on infrastructures that inspire trust to maintain or gain the confidence of customers and other communications partners. At the same time, internal processes—*e.g.* for data-warehouse and data-mining applications—need to be organized in a manner that secures optimal information processing with respect for the private sphere. Companies that have undertaken to provide their customers with first-class service must conceive their customer-relationship management in its full dimension as an essential element in the value-added chain to promote long-term acceptance for electronic commerce.

Notes

[1] Danish Public Authorities Registers Act.
[2] Danish Private Registers Act.
[3] Nominal Data (Automatic Processing) Act.
[4] Act providing rules for the Protection of Privacy in Connection with Personal Data Files.
[5] Federal Act on Personal Data.
[6] Federal Act on Protection of Personal Data with the Decree of June 14, 1993.

[7] Law on the Regulation of the Automatic Processing of Personal Data.
[8] Law concerning the Protection of Personal Privacy in Relation to the Processing of Personal Data.
[9] Personal Data Protection Act.
[10] Personal Data File Act and Personal Data File Decree.
[11] Law No. 78-17.
[12] Law on the Protection of Individuals with Regard to the Processing of Personal Data.
[13] Data Protection Act.
[14] Ibid.
[15] Protection of Individuals and other Subjects with Regard to the Processing of Personal Data.
[16] Act on Personal Data Registers.
[17] Law of August 29, 1997, on the Protection of Personal Data.
[18] Law for the Protection of Personal Data with Regard to Automatic Processing.
[19] Law of the Russian Federation on Information, Informatization and Information Protection, 1995.
[20] Data Act.
[21] Since February, 1998, a new data-protection law has been effective, which closely relies on the EU guideline.
[22] Law on the Protection of Personal Data in Information Systems of April 29, 1992.
[23] Law No. LXIII, 1992, on the Protection of Personal Data and Freedom of Information Act.
[24] Directive of the European Parliament and of the Council on the Processing of Personal Data and on the Protection of the Private Sphere in the Field of Telecommunication.
[25] Directive 1999/93/EG of the European Parliament and Council of December 13, 1999, Regarding Common General Requirements for Electronic Signatures.
[26] Amended Proposal for a Directive of the European Parliament and Council Regarding Distance Marketing of Financial Services to Consumers and the Amendment of Directives 97/7/EG and 98/27/EG, KOM 1999-385 endg. 98/0245—COD.
[27] In this connection, the Discussion Regarding the Effects of the European Data Protection Directive on Financial Services in the USA is being referenced, *e.g.* Peter Swire, "Effects of the European Privacy Directive on Financial Services," available at http://www.osu.edu/units/law/swire.htm.
[28] See Thorwald Hellner and Stephan Steuer, *Bankrecht und Bankpraxis*, vol. 6 (Köln: Bank-Verlag, 1999), Section 17. "Datenschutz," RN 14.
[29] This restriction is not required: The Austrian Data Protection Law includes legal persons (Section 4, Number 3 DS G2000). According to Italian Law (Article 26), data of legal persons are protected on a restricted basis.

[30] Reference Draft of the Federal Ministry of the Interior Regarding the New Draft of the BDSG.
[31] According to the reference draft, an establishment is presented when the financial-service provider constantly uses an established, continuous, or regularly recurrent space which is used by him for the operation of his business.
[32] See the exhaustive *Bankrecht und Bankpraxis*, vol. 6, 17/36.
[33] Schutzgemeinschaft für allgemeine Kreditsicherung.
[34] See Section 28, Paragraph 4 of the new BDSG draft (Federal Ministry, Stand 6, July 1999).
[35] See *Bankrecht und Bankpraxis*, vol. 6, 17/136. More detailed information in Alfred Büllesbach, "Datenschutz bie Data Warehouse und Data Mining," in *Computer und Recht* (2000), p. 11.
[36] See *Bankrecht und Bankpraxis*, vol. 6, 17/150.
[37] See the 17 Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (1997-98), p. 503 f.
[38] See Section 28, Paragraph 1, Record 1, Number 2 or Section 28, Paragraph 2, Record 1a of the BDSG.
[39] See the 17 Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (1997-98), p. 501 ff.
[40] Correspondingly formulated according to Section 3, Paragraph 8, Record 3 of the new BDSG draft: "Third parties are not the concerned party as well as those persons or locations, which acquire, process or use personal data domestically or in the area of application of legal regulations regarding the protection of personal data of the Member States of the EU."
[41] See Simitis in Simitis/Dammann/Geiger/Mallmann/Walz, BDSG, 4th ed. (April 1998), Section 28/8.1.
[42] Section 44a of the KWG is based on the EC Directive of June 13, 1983, on supervision of credit institutions on a consolidated basis (EC file no. L 193 dated July 18, 1983).
[43] See *Bankrecht und Bankpraxis*, vol. 6, 17/238.
[44] Barbara Wellbury, "The U.S. Side of Data Protection Policy," in Alfred Büllesbach, ed., *Datenverkehr ohne Datenschutz?—Eine globale Herausforderung* (Dr. Otto Schmidt Verlag, 1999).
[45] Schwartz/Reidenberg, *Data Privacy Law* (Michie Law Publishers, 1996) provides a summarised comparison of the EU requirements and US data-protection legislation, including aspects relating to the finance industry. An up-to-date worldwide comparison is given by EPIC and Privacy International, *Privacy & Human Rights, An International Survey of Privacy Laws and Developments*, 1999.
[46] For instance, a credit-protection organisation must observe the ban on utilisation contained in Section 51 of the Federal Central Register Act (Bundeszentralregistergesetz) or in Section 153, Paragraph 5 of the Trading Regulations (Gewerbeordnung), whereby data deleted from these registers on the basis of statutory deletion dates may not be kept in other legal handlings,

or used to the detriment of the affected party.
[47] *Bankrecht und Bankpraxis*, vol. 6, 17/280.
[48] See consideration (14) in the EU Directive on Data Protection.
[49] Information and Communication Services Act dated August 1, 1997, Federal Gazette (BGBl.) vol. 1.
[50] See *Bankrecht und Bankpraxis*, vol. 6, 17/390.
[51] The most important central associations in the German loans industry work together in the Central Credit Committee (Zentraler Kreditauschuß).
[52] See Section 38, Paragraph 1 of the draft amendment of the BDSG.
[53] For more details on this see Alfred Büllesbach, "Innovative and Technology-Shaping Data Protection—Social and Commercial Requirements," in *Multilateral Security in Communications*, vol. 3, Günter Müller, Kai Rannenberg (Addison-Wesley, 1999), p. 61.