Boston College International and Comparative Law Review

Volume 6 | Issue 1 Article 8

12-1-1983

The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?

J Lee Riccardi

The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?

I. INTRODUCTION

Information, access to information, and the flow of data play a central and increasing role in modern societies.[1] The need for information is without parallel, and, at the same time, the advent of computers[2] and other technological advances[3] has greatly increased our capacity for processing and distributing it.[4] "Information is the basis for almost all activity, both in the public and private spheres."[5] Information gathering thus touches almost every aspect of modern life, and automated data processing is indispensable if government and business are to deal with the mass of available material.[6]

---

* All translations are by the author unless otherwise noted.

1. H. ORDEMANN & R. SCHOMERUS, BUNDESDATENSCHUTZGESETZ 31-32 (2d ed. 1978) [hereinafter cited as ORDEMANN]. Dr. Hans Joachim Ordemann is a ministerial director in the German Federal Ministry of the Interior.

> The state needs [information] as the basis for decision-making in the planning of schools, kindergartens and transportation systems, for estimating tax income, and fighting crime. . . . Industry can only develop market strategies . . . or plan investments on the basis of careful information gathering. Success at business is no longer merely the result of personal experience, but far more of the ability to follow the developments in one's own line of business and control the mass of available information.

Id.

2. Computers involve "machine aided manipulation of information." J. ADAMS & D. HADEN, SOCIAL EFFECTS OF COMPUTER USE AND MISUSE 23 (1976) [hereinafter cited as ADAMS]. The first business use of an electronic computer was in 1964. *Id.* at 35. Since then, both technological progress and growth in numbers have been steady. In 1966, 15,000 computers existed; by 1970, 80,000 were in use. *Id.* at 45. Of these, 70,000 were in use in the United States alone. A. WESTIN & M. BAKER, DATABANKS IN A FREE SOCIETY 29 (1972). New products, such as personal computers, are now making the technology available to practically everyone. *To Each His Own Computer,* NEWSWEEK, Feb. 22, 1982, at 50 [hereinafter cited as NEWSWEEK].

3. Such advances include remote sensing of the earth from outer space by satellite, for example. *See* Recent Development, *In Search of a Legal Framework for the Remote Sensing of the Earth from Outer Space,* 4 B.C. INT'L & COMP. L. REV. 453 (1981).

4. The capacity for information gathering and distribution continues to increase. The IBM 360 Model 30, introduced in the 1960's, could perform 33,000 additions per second at full speed. Some personal computers can now perform 700,000 per second. NEWSWEEK, *supra* note 2, at 52.

5. ORDEMANN, *supra* note 1, at 31.

> As a worker, as a student, as a patient, as a taxpayer, as a bank depositor, as the owner or driver of a car, as a welfare recipient, as one ticketed for even a minor traffic violation — it is practically impossible to avoid becoming the subject of a record. The same is true if one wants to make an airline reservation, stay in a hotel, have life insurance, or buy on credit.

UNITED STATES DEP'T OF HEALTH, EDUCATION AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS, REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, at i (1973) [hereinafter cited as SECRETARY'S REPORT].

6. Without automated data processing one would need days or even months to perform certain tasks; others would be literally impossible. *See generally* ADAMS, *supra* note 2, at 32.

Modern data processing technology has numerous advantages over slower and more cumbersome hand methods, but advanced technology has certain problems as well. Some of these problems, such as receipt of an erroneous bill, a dunning letter on a bill already paid or duplicate magazine subscriptions, are minor.[7] Other problems are potentially more serious. When speed or information is vital, a computer malfunction may endanger health, or even lives.[8] More important is the fact that data processing may threaten the individual's right to privacy.[9] Personal data are now "combinable and storable without limit [and] also accessible as never before."[10] Data processors can disseminate and manipulate information from every area of endeavor, most often without the knowledge of the person concerned.[11] The possibility that government or business can gather information on every citizen may, therefore, pose a danger to individual freedom.[12]

The German Federal Data Protection Act of 1977 (BDSG)[13] represents an attempt by the Legislature of West Germany to deal with that danger. This Comment discusses the provisions of the Act, and analyzes the success of the Act in protecting privacy. The author first briefly examines the meaning of privacy in German law and the protections German law accorded privacy before the enactment of the BDSG. After discussing the background and development of the BDSG, the author focuses on the specific provisions of the Act, and on some of the difficulties and interpretive problems these provisions have created. Although this Comment deals primarily with the protections the BDSG accords privacy, the Act has important business ramifications for data processors, as well. The BDSG's restrictions will affect all organizations which operate or participate in the German market. Since multinational corporations will be subject not only to German data laws but also to potentially conflicting data processing laws in other countries, the impact on such companies may be great. The precise nature and extent of that impact are, as yet, unclear.[14]

---

7. SECRETARY'S REPORT, *supra* note 5, at 13.

8. In 1973, the computer facility of the French National Family Allotment System broke down over changes made in certain allotment rates. Some suffering undoubtedly occurred, since the system served 700,000 people and disbursed $600 million annually. The facility had to use a manual system to restore order. *Id.* at 14, *citing* N.Y. Times, Jan. 26, 1973, at 4, col. 1.

9. *See generally* SECRETARY'S REPORT, *supra* note 5, at 23-29.

10. S. SIMITIS, U. DAMMANN, O. MALLMANN & H. REH, KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ 51 (2d ed. 1979) [hereinafter cited as SIMITIS, BDSG]. Spiros Simitis is Hessian Data Protection Commissioner and Professor of Civil and Labor Law at the University of Frankfurt/M.

11. ORDEMANN, *supra* note 1, at 32.

12. Speech of Bundespräsident Scheel on the 65th anniversary of the Max-Planck-Gesellschaft, *quoted in* ORDEMANN, *supra* note 1, at 31.

13. Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz — BDSG) of 27 January, 1977, BUNDESGESETZBLATT [BGBl] I 201 (W. Ger.) [Law on Protection Against the Misuse of Personal Data in Data Processing (Federal Data Protection Act — BDSG)].

14. GESETZ ZUM SCHUTZ VOR MIßBRAUCH PERSONENBEZOGENER DATEN BEI DER DATENVERARBEITUNG/ LAW ON PROTECTION AGAINST THE MISUSE OF PERSONAL DATA IN DATA PROCESSING 7 (Unofficial

II. BACKGROUND AND DEVELOPMENT OF THE BDSG

A. *The Right of Privacy Before the BDSG*

The BDSG is not the first German law to protect privacy. Articles 1 and 2 of the *Grundgesetz*[15] guarantee the "dignity of the individual,"[16] and the right to the "free development" of one's personality.[17] The Constitutional Court[18] has held that the right to free development of the personality is the "highest constitutional value,"[19] and has defined the right of privacy as an "untouchable sphere of private life withdrawn from the influence of state power."[20] The basic German formulation of the right to privacy is thus similar to that expressed in the United States by Justice Brandeis: "The makers of our constitution conferred, as against the government, the right to be let alone."[21]

In addition to these fundamental constitutional rights, at least 130 other laws regulated the handling of personal data before the enactment of the BDSG.[22]

---

translation on the basis of a translation provided by the Commission of the European Communities — Directorate — General [sic] for Industrial and Technical Affairs — Group of Experts on Data Processing and Privacy, Brussels, AZ: III/1125/76-E) (Gesellschaft für Datenschutz und Datensicherung e.V., eds., revised by Ursula Gliss 1977). All quotations from the BDSG are from this translation unless otherwise indicated.

15. The *Grundgesetz* [GG] or Basic Law functions as a constitution for West Germany until such time as the entire German people approve a constitution (*i.e.*, after reunification). *See* 1 I. VON MÜNCH, GRUNDGESETZ KOMMENTAR 24 (1974) [hereinafter cited as VON MÜNCH].

16. Grundgesetz für die Bundesrepublik Deutschland of May 23, 1949. Article 1(I) provides: "The dignity of the individual is untouchable. It is the duty of all governmental power to heed it and protect it." *Id.*

17. Article 2(I) GG provides: "Every person has the right to free development of his own personality, in so far as he does no damage to the rights of others, to the constitutional order, or the moral law." *Id.* The right to free development of the personality means, in the broadest sense, the right to act freely. Judgment of Jan. 16, 1957 6 Bundesverfassungsgericht [BVerfG] 32, 36. *See also* G. LEIBHOLZ & H. RINCK, GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND — KOMMENTAR 48-49 (3d ed. 1968). "The freedom to develop one's personality is not exhausted in the general right to act freely, but in our [constitutional] order includes the basic requirement that the power of the state impose no detriment on a citizen not grounded in that constitutional order." *Id.* at 49.

18. The Constitutional Court (*Bundesverfassungsgericht*) is the "guardian of the constitution." *See* T. MAUNZ, DEUTSCHES STAATSRECHT 302 (16th ed. 1968). The Court's full jurisdiction appears in Article 93, GG. Anyone who "believes that his fundamental rights or other specifically mentioned in the Basic Law have been violated by public authorities" may invoke the guardianship of the Constitutional Court. Art. 93(IV)(a) GG.

19. Judgment of Nov. 6, 1958, 7 BVerfG 377, 405.

20. *See, e.g.*, Judgment of June 16, 1969, 27 BVerfG 1, 6; Judgment of May 6, 1973, 35 BVerfG 202, 221; Judgment of June 15, 1970, 27 BVerfG 344, 350.

21. Olmstead v. United States, 277 U.S. 438, 478 (1927).

22. These laws existed according to a study by the Gesellschaft für Mathematik und Datenverarbeitung (Society for Mathematics and Data-Processing), *cited in* ORDEMANN, *supra* note 1, at 34. Court decisions construing these laws also protected privacy. The *Bundesgerichtshof*, the highest of the German regular courts, *see* A. VON MEHREN, THE CIVIL LAW SYSTEM 130-33 (2d. ed. 1977), had ruled that unauthorized publication of a person's picture was an offense against the right of self-expression. *See* Judgment of Feb. 14, 1958, 26 Bundesgerichtshof in Zivilsachen [BGHZ] 349, 355. The BGHZ had also held that the "right to one's personality" constituted "another right" within the meaning of the Civil Code (Bürgerliches Gesetzbuch [BGB]), section 823 which provides: "Whoever unlawfully violates the

But the German Legislature had passed no comprehensive law to deal with data protection and the right to privacy, and some critics noted a possibility of conflict between the fundamental right to inform oneself from public sources guaranteed by Article 5[23] of the *Grundgesetz,* and the fundamental freedoms of Articles 1 and 2. Before the enactment of the BDSG some commentators[24] had urged that Article 5 prohibited individuals from *hindering* access to personal information.[25] The BDSG effectively closes this line of argument by denying access to personal data to data processors in many situations.[26]

B. *Legislative History of the BDSG*

During the greater part of the 1960's, both the public and private sectors considered the gains in efficiency attained through automatic data processing more important than any privacy problems the new technology might create.[27] As the decade progressed, however, various nations focused more attention on the possible dangers latent in the technology, dangers both for the individual citizen and for society as a whole.[28] Several countries planned or promul-

---

person, health, liberty, property or other right of another person, whether deliberately or negligently, is bound to make good the damages that arise therefrom." BGB § 823. Violation of the right could lead to an action for damages. *See, e.g.*, Judgment of May 25, 1954, 13 BGHZ 334; Judgment of Mar. 20, 1968, 50 BGHZ 133, 143; *see also* Herdemerten in VON MÜNCH, *supra* note 15, at 43, and Niemöhlmann, in VON MÜNCH, *supra* note 15, at 80. The *Grundgesetz* guarantees this right both against the state and against individuals. *See* Judgment of Apr. 2, 1957, 24 BGHZ 72, 76; Judgment of May 20, 1958, 27 BGHZ 284, 286. Laws also protected private secrets and made revealing them punishable. *See* Einführungsgesetz zum Strafgesetzbuch, 1974 BGBl I 469, 487 (amending § 203 (II) Strafgesetzbuch).

23. Art. 5 GG. "Article 5 contains several fundamental rights . . . [including] . . . freedom of information . . . . The meaning of the fundamental rights of article 5, in particular those of freedom of expression and freedom of information, is evident in a democratic state," VON M;UNCH, *supra* note 15, at 196. Article 5 includes a right to information from all generally accessible sources. These sources include all possible holders of information, whether they pertain to public or private matters. *Id.* at 202. On the necessity for information as a formative principle of the "freedom of personality" guaranteed by the *Grundgesetz, see* Egloff, *Information und Grundrechte,* 7 DATENVERARBEITUNG IM RECHT [DVR] 115 (1978).

24. Simitis, *Bundesdatenschutzgesetz — Ende der Diskussion oder Neubeginn,* 30 NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 729, 731 (1977) [hereinafter cited as Simitis, NJW].

25. *Id.*

26. *Id.*

27. *Id.* at 729. "Attention was directed toward the perfection of information gathering, not, however, to the implications of such perfection." *Id.* As late as 1976, the Interior Committee of the Bundestag proposed giving each citizen a *Personenkennzeichen* or identification number for data-processing purposes. *Id.* The Legal Committee on the other hand, labeled the proposal "unacceptable." *Id.*

28. *See,* for example, Simitis, *Datenschutz — Notwendigkeit und Voraussetzungen einer gesetzlichen Regelung,* 2 DVR 138 (1973). The Secretary's Report also identified several problem areas: (1) a feeling of individual loss of control, SECRETARY'S REPORT *supra* note 5, at 29; (2) of distrust of computer systems in general, *id.* at 28-29; and (3) of "Big Brotherism," *id.* at 29.

> Another, potentially more serious consequence of putting record-keeping in the hands of a new class of data-processing specialists is that questions of record-keeping practice which involve issues of social policy are sometimes treated as if they were nothing more than questions of efficient technique. The pressure for establishing a simple, [sic] identification scheme for locating records in computer-based systems is a case in point.

SECRETARY'S REPORT, *supra* note 5, at 23. The parallel in the German experience is the *Personenkennzeichen. See* note 27 *supra.*

gated laws affecting data processing and privacy.[29] Yet, as late as 1971, the official position of the German federal government was that existing laws[30] sufficiently protected the right of privacy and that Germany needed no further regulation of data processing.[31]

The Bundestag[32] had, however, already declared its preference for general regulation of data processing,[33] and after a long delay the government stated that it would propose such a law.[34] Nonetheless, the government presented no proposals to the Parliament until 1973.[35] Despite the passage of time and the recognized need for regulation, the Bundestag was neither willing to approve the proposed draft nor satisfied with minor changes.[36] In view of the newness and complexity of the data processing field, the Bundestag returned the bill to Committee[37] for further study.[38] After making additional modifications,[39] the Bundestag approved the bill,[40] but the Bundesrat now requested changes. After the Joint Committee made further changes,[41] both legislative houses of Parlia-

---

29. The United States, for example, passed the Fair Credit Reporting act of 1979, 15 U.S.C. § 1681 (1976); *see also* Swedish Data Protection Law of May 11, 1973, *Datalagen* [1973] SVENSK FÖRFATTNINGSSAMLING 289. In West Germany, two of the lands, Hesse and Rhein-Pfalz, passed data protection acts before the federal government. *See* Hessian Data Protection Act of Oct. 7, 1970, GESETZ- UND VERORDNUNGSBLATT [GVBl] 625; Rhein-Pfalz Data Protection Act of Jan. 24, 1974, GVBl 31.

30. *See* note 22 and accompanying text *supra*.

31. *See generally* Simitis, *Chancen und Gefahren der elektronischen Datenverarbeitung*, 24 NJW 673 (1971).

32. The *Grundgesetz* established a federal parliament (*Bundestag*) elected in "general, direct, free, equal and secret elections," Art. 38 GG, and a federal council (Bundesrat) whose members are "members of the land governments which appoint and recall them." Art. 51 GG. Article 62 defines the federal government as the "Federal Chancellor and the Federal Ministers." Art. 62 GG. The legislative procedure of the Federal Republic is "somewhat complex." A. GROSSER, GERMANY IN OUR TIMES 126 (1971) [hereinafter cited as GROSSER]. The government or either house of parliament may propose bills. *Id.* Federal bills must go first to the Bundesrat which has "a right to give its opinion on these bills within three weeks." Art. 76 GG. "Wherever a bill originates, it is for the Bundestag to vote on it as the first step of the legislative process." GROSSER, *supra*, at 126.

33. Resolution of the German Bundestag, Mar. 28, 1969 (Stenogr. Bericht der 226. Sitzung).

34. Oct. 5, 1970, BUNDESTAGS-DRUCKSACHE [BT-DRUCKS.] VI/1223.

35. ORDEMANN, *supra* note 1, at 43. The Bundestag first considered the bill on November 29, 1973. BT-DRUCKS. VII/1027. The bill went to the Bundestag on October 20, 1973. Auernhammer, *Das Bundesdatenschutzgesetz*, 32 DER BETRIEBSBERATER 205, 205 (1977) [hereinafter cited as AUERNHAMMER].

36. SIMITIS, BDSG, *supra* note 10, at 59. *Cf.* ORDEMANN, *supra* note 1, at 43 on the reaction of the Bundesrat: "The Bundesrat basically approved of [the law] on the first go-around, and asked for changes only in particulars." *Id.*

37. ORDEMANN, *supra* note 1, at 44.

38. *Id.* There were also open hearings on May 6, 1974 and Mar. 31, 1976. *See* SIMITIS, BDSG, *supra* note 10, at 60, an uncommon procedure in the German legislative process. *Id.*

39. Changes made in the law are, for the most part, beyond the scope of this Comment. For discussion of these changes, *see* BUNDESDATENSCHUTZGESETZ (BDSG) MIT MATERIALIEN (U. Dammann & S. Simitis eds., 2d ed. 1977) [hereinafter cited as SIMITIS, MATERIALIEN].

40. BT-DRUCKS. VII/5332.

41. Article 53a GG established the Joint Committee. The Joint Committee consists of eleven members of the Bundesrat (one for each land) and twenty-two Bundestag deputies. *Id.* "The commissioners . . . meet in closed session . . . and determine by majority vote the changes that they think will make a bill acceptable to both houses." GROSSER, *supra* note 32, at 126. For the changes suggested by the Joint Committee, *see* BT-DRUCKS. VII/5568.

ment voted in favor of the bill.[42] Yet when the law was promulgated on February 1, 1977[43] the prevailing attitude among both critics and legislators was one of skepticism rather than of satisfaction.[44] Even those who favored the BDSG were willing to say no more than that it was an acceptable compromise measure.[45]

III. THE CONTENT OF THE BDSG

A. *General Provisions*

1. Purpose of the Act

The purpose of the BDSG was to regulate the entire personal data processing field within Germany.[46] Section 1 of the law states: [T]he purpose of data protection is to ensure against the misuse of personal data . . . and thereby to prevent harm to any personal interests that warrants protection."[47] The Act does not protect personal data per se, but protects the privacy of the individual by protecting his data from misuse.[48] Indeed, the phrase "personal interests that warrant protection" is an alternative expression for the phrase "the right of privacy."[49]

The German legislature, when it passed the BDSG in 1977, sought to add to the existing safeguards of privacy by protecting personal data.[50] Arguably the most important provision of the BDSG is, therefore, Section 3, which "comprehends the ratio legis, the philosophy of the Act. . . . The processing of personal data is forbidden."[51] The thrust of the Act is negative in that it provides for a blanket prohibition on the processing of personal data unless the BDSG or another legal regulation specifically permits the processing, or the person affected has given his consent.[52] Some critics excepted to the consent requirement on the grounds that the individual has little choice but to comply with the requirements of government agencies and public authorities, or even those of large companies if he is, *inter alia,* to receive credit or quality for services.[53] One

42. SIMITIS, BDSG, *supra* note 10, at 60-61. The legislature voted for the bill only after the Joint Committee refused to consider the bill again. *Id.* at 61.

43. BGBl I 201. Most of the BDSG entered into force on January 1, 1978, though certain portions had become effective earlier, and others did not become effective until January 1979. BDSG § 47.

44. SIMITIS, BDSG, *supra* note 10, at 48.

45. Simitis, NJW, *supra* note 24, at 730.

46. BT-DRUCKS. VII/1027. Affects on transnational data transfer are incidental not intentional. SIMITIS, BDSG, *supra* note 10, at 72.

47. BDSG § 1(I).

48. ORDEMANN, *supra* note 1, at 44.

49. *Id.* at 52. *See also* Mallmann, *Zielfunktionen des Datenschutzes,* 6 KYBERNETIK, DATENVERABEITUNG, RECHT (1976).

50. *See* § II.A *supra.*

51. ORDEMANN, *supra* note 1, at 79.

52. BDSG § 3. BGB § 183 defines "consent" (*Einwilligung*) as "prior agreement" (*vorherige Zustimmung*).

53. *See, e.g.,* Schmidt, *Die Bedrohte Entscheidungsfreiheit,* 29 JURISTENZEITUNG [JZ] 241, 247 (1974);

critic, therefore, suggested omitting the consent requirement altogether,[54] but the law focuses on the privacy of the individual, and the legislature, therefore, chose to retain the requirement. In order to make obtaining consent more difficult, however, the legislature stipulated that an individual give his consent in writing before any data processing unit processes his data.[55] In the absence of a legal provision permitting data processing, failure to obtain consent would make any processing of personal data illegal.[56]

B. *Data Covered by the Act*

The BDSG defines personal data as "details on the personal or material circumstances of an identified or identifiable physical person (the person concerned)."[57] The Act makes no distinction between "ordinary" personal data and "sensitive" personal data.[58] The BDSG thus treats the most generally accessible data, such as an individual's name and address, in the same way as it treats the most intimate — data on his religion, race or political opinions.[59] In this regard, the BDSG differs from other data protection acts.[60] The BDSG's failure to distinguish among types of data initially appears to be an oversight since some personal data, telephone numbers, for example, are so readily available that the protection the Act affords would seem superfluous. In reality, however, by protecting all types of personal data rather than "sensitive" personal data alone, the Act avoids problems of definition. In addition, certain data might not appear sensitive to the legislature, yet be sensitive from the perspective of the individual.[61] By including all types of personal data within its protection, the BDSG avoids this difficulty as well.[62]

Bull, *Entscheidungsfragen in Sachen Datenschutz,* 8 ZEITSCHRIFT FÜR RECHTSPOLITIK 7, 10 (1975) [hereinafter cited as Bull].

54. *See* ORDEMANN, *supra* note 1, at 82.

55. BDSG § 3 (II) para. 2.

56. BGB §§ 125-26. Section 125 provides: "A legal proceeding which lacks the formalities required by law is void." Section 126 provides: "If a writing is required by law, the document must be personally signed by the maker, or signed by means of a mark authenticated by a notary." For a further discussion of these requirements *see* PALANDT, BÜRGERLICHES GESETZBUCH (36th ed. 1977) under the BGB sections noted. Violations would not, however, necessarily lead to a right to damages. ORDEMANN, *supra* note 1, at 82-83.

57. BDSG § 2(I). *Sic.* The term "natural person" is more usual.

58. *But see* § III.D.4 *infra.*

59. ORDEMANN, *supra* note 1, at 45.

60. *See, e.g.,* the French Data Protection Act, Law no. 78-17 of January 6, 1978 Relative à l'informatique, aux fichiers et aux libertés, [1978] JOURNAL OFFICIEL DE LA REPUBLIQUE FRANCAISE 227, 229 1978 Dalloz-Sirey Législation 77, 80, art. 31: "Il est interdit de mettre ou conserver en mémoire informatisée, sauf accord exprès de l'interresée, des donées nominative qui directement ou indirectement font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appertenances syndicale des personnes." *Id.*

61. Simitis, NJW, *supra* note 24, at 732.

62. *Id.* The Dutch draft of a data protection act also provided for differentiation of sensitive and ordinary data. The Dutch solved the difficulty by providing in Art. 2 for broadening the definition of sensitive data at any time. *Id.* at 732 n31.

Nevertheless, the BDSG does not regulate all personal data. Only data which are, or can be, linked to a particular person are within the scope of the law. Thus, a data storage unit may process anonymous or aggregated[63] data freely, unless the unit has a means of reconstructing the identity of those to whom the data refer.[64] The law also does not protect the data of legal persons, such as corporations.[65] The fact that "[d]ata protection is conceived from the standpoint of the individual citizen, and thus remains limited to him" explains both exceptions.[66]

The BDSG does not protect some personal data which would ordinarily fall within the definition of the Act. For example, data processors who use non-automatic methods[67] may, if they do not intend to transmit the data to third parties, use data freely.[68] These data processors must fulfill both conditions: their storage units must process the data by hand, and must do so entirely for their own, internal, use.[69] The difficulty of administering an effective check on data processed entirely for internal use partially justified the exception,[70] but a more important constitutional justification is that the government may not interfere with the freedom to store and evaluate thoughts, opinions and information for purely internal purposes.[71] Thus, "any regulation of such storage would be subject to constitutional objections as an interference with the private sphere of those who store the data."[72]

The BDSG also contains an exception for the press. The law does not protect personal data which the press or its auxiliaries process exclusively for their own

---

63. Aggregated data might, for example, include data on a group of individuals, though the unit does not know to which individual any particular datum pertains.

64. DAMMANN in SIMITIS, BDSG, *supra* note 10, at 125. The determining factor with regard to the identifiability of a person is the knowledge, method and capacity of the storage unit. Reconstruction of the identity could be by a key number or some other means. If the unit could reconstruct the data only with the aid of specialized mathematical knowledge, such materials would not become "personal data," since the effort required to reapply them to particular individuals would be far beyond the ordinary. ORDEMANN, *supra* note 1, at 63, 64.

65. Some doubt whether this provision can be squared with Article 19 (III) GG which provides: "The fundamental rights also apply to native legal persons, in so far as their nature makes [such rights] applicable." *Id.* While legal persons cannot rely on Article 1(I) GG (Dignity of Man), VON MÜNCH, *supra* note 15, at 606, they do have "all those fundamental rights . . . necessary for the meaningful performance of the tasks for which they were founded." *Id.* at 608. Such rights include the right to free development of one's own personality guaranteed by Article 2(I) GG. *Id.* Almost all commentators agree that the basic rights apply only to legal persons of private law, and not to creations of public law such as cities, states and agencies. *Id.* at 606. For the texts of Articles 1 and 2 GG, *see* notes 16 and 17 *supra*.

66. Simitis, NJW, *supra* note 24, at 732.

67. Non-automatic methods would include manual files such as card files, for example. Documents and collections thereof are specifically exempted from the BDSG unless a storage unit can process them with automated methods. BDSG § 2(III)(3).

68. BDSG § 1(II)3, para. 2. The emphasis on automated methods is a consequence of the differing abilities of electronic (i.e., computer) and manual systems with regard to such things as speed and storage capacity. *See* Simitis, NJW, *supra* note 24, at 732.

69. BDSG § 1(II)(3) para. 2.

70. ORDEMANN, *supra* note 1, at 58.

71. *Id.*

72. *Id.*

journalistic purposes.[73] The *Grundgesetz* guarantees freedom of the press.[74] Full application of the BDSG to the media would have been unconstitutional,[75] since the Grundgesetz guarantees the independence of the press as an institution from the gathering of information to the final distribution of the news.[76]

The BDSG protects personal data during all phases of data processing.[77] The law, however, protects only data that are being processed.[78] One must, therefore, determine when data processing begins. "The law sees the deciding factor in the existence of a *Datei* [data file], and only when a *Datei* is present will the law interfere."[79] Unfortunately, the Act fails to define the term *Datei* very precisely.

A *Datei* consists of two components. A data file is a collection of data, and the file must be assembled on a uniform basis.[80] In addition, the data must be "recorded and arranged according to specific features, and [be capable of being] rearranged and evaluated according to other specific features."[81] The law thus leaves the number of specific features required to create a data file in doubt.

---

73. BDSG § 1(III).

74. Article 5(I) GG provides in pertinent part: "The freedom of the press and the freedom to inform through radio and film are guaranteed. There shall be no censorship." *Id.*

75. *See* ORDEMANN, *supra* note 1, at 58. The freedom of the press must remain consistent with the equally fundamental right of free development of the personality. *Id.* All laws on the rights and duties of the press previously in force remain in force. SIMITIS, BDSG, *supra* note 10, at 93. Duties include avoidance of negligence under BGB section 823 or of destruction of reputation through the dissemination of falsehoods (BGB § 824). On freedom of the press in German law, *see* VON MÜNCH, *supra* note 5, at 205-10; on the general level of care required of the press, *see* 3 MÜNCHENER KOMMENTAR ZUM BÜRGERLICHEN GESETZBUCH 1327 (2d *Halbband*) (P. ULMER ed. 1980).

76. G. LEIBHOLZ & H. RINCK, GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND, KOMMENTAR 123 (3d ed. 1968); *see also* Judgment of Oct. 6, 1959, 10 BVerfG 118 at 121; Judgment of Feb. 28, 1961, 12 BVerfG 205, 260.

77. BDSG § 2.

For the purposes of this Law

1. storage shall mean the acquisition, recording or retention of data on a storage medium so that they may be further used;
2. communication shall mean the passing of stored data or data acquired directly by means of data processing to third parties in such a way that the data are communicated by the storage unit or are held ready for inspection, i.e., for retrieval;
3. modification shall mean the alteration of the contents of stored data;
4. erasure shall mean the obliteration of stored data irrespective of the methods used.

Id. Whenever the term "data processing" appears in the BDSG, it refers to all of these phases. ORDEMANN, *supra* note 1, at 55. The last half-sentence of Section 2 ("irrespective of the methods used") makes it clear that the BDSG applies not only to automatic data processing, but to data processed by any means. *Id.* at 66. In this regard, the BDSG is somewhat unusual. The French Data Processing Law, *see* note 60, *supra,* applies only to automatic data processing, as does the Dutch draft. Simitis, NJW, *supra* note 24, at 732.

78. BDSG § 1(I).

79. Simitis, NJW, *supra* note 24, at 732.

80. BDSG § 2(III)(3). The requirement that the data be uniformly assembled means that data must be ordered according to a specific scheme, i.e., not at random. This order may exist because of physical characteristics of the data holders (*e.g.,* all cards) or because of a logical rule (*e.g.,* a program). *See* SIMITIS, BDSG, *supra* note 10, at 171.

81. BDSG § 2(III)(3). Translation by the author. The draft translation (*supra* note 5) seems less clear. The German reads: "die nach bestimmten Merkmalen erfaßt und geordnet, nach anderen Merkmalen umgeordnet und ausgewertet werden kann."

Some critics argue that the file must have a minimum of two features;[82] others argue for a minimum of four.[83] The fact that the term "specific features" is itself unclear further complicates interpretation. Only those features necessary for a meaningful ordering of the data file can be "specific."[84] One may, therefore, find it impossible to determine what "specific features" are in a given case without knowledge of the construction and purpose of the individual data bank.[85] The ambiguity of the term "specific features" is almost certain to lead to controversy, and may, in the hands of some data processors, provide a justification for limiting the operation of the Act.[86]

C. *Data Processing by Public Authorities and Other Public Establishments*

1. The BDSG and Land Law

Sections 7 through 21 of the BDSG[87] regulate data processing by federal authorities and other public establishments of the federal government,[88] as well as "public law entities, institutions and foundations directly owned, employed or operated by the federal government."[89] The BDSG thus effectively regulates all branches of government, *i.e.*, the legislative, executive and judicial.[90] These regulatory provisions are, however, complicated by the fact that the BDSG governs the actions of federal authorities, but governs actions of public au-

---

82. *See, e.g.*, von Witzlow, 3 BUNDESARBEITSGERICHT NACHRICHTEN; Karad, 1976 DER ARBEITGEBER 969.

83. DAMMANN in SIMITIS, BDSG, *supra* note 10, at 174. The argument that four specific features are necessary is based on the fact that the Act twice uses the plural "features," i.e., specific features must be modified using other specific features. *Id.*

84. ORDEMANN, *supra* note 1, at 75. An address may be composed of such information as city, street and house number, but if the storage unit arranges the data file by address, the entire address is a single feature. If, on the other hand, the data processor could break the material down farther (*e.g.*, all residents of a specific street), the individual components of the address could also be specific features. *Id.* at 75-76.

85. *Id.* at 76.

86. Simitis, NJW, *supra* note 24, at 732.

87. BDSG §§ 7-21.

88. The Law on Administrative Procedures (*Verwaltungsverfahrensgesetz* [VwVfG]) of May 25, 1976 BGBl 1, 1253 defines "public authorities" as "every agency which attends to the duties of public administration." *Id.* This definition is extremely broad and, despite the VwVfG, not entirely clear. In the view of some critics, for example, a governmental department within a city could be a separate *Behörde*. *Cf.* SCHEDL, BDSG-BUNDESDATENSCHUTZGESETZ § 2 (1977) *with* H. MEYER & H. BORGS-MACIEJEWSKI, VW VFG-VERWALTUNGSVERFAHRENSGESETZ-KOMMENTAR § 1 at comment 29 (1976).

89. The BDSG also applies to "public law entities, institutions and foundations directly owned, employed or operated by the Federal Government." BDSG § 7. Sections 7-21 also apply to associations of such entities. *Id.* But only Sections 15-21 apply to those governmental entities that compete in the open market. The law provides no exact definition of such entities, but the deciding criterion is that they must take part in competition. The entity must "offer services which also are offered by comparable private undertakings." ORDEMANN, *supra* note 1, at 100. No profit motive is necessary. *Id.* Examples of such entities include public credit institutions and public hospitals. *Id.* at 100-04.

90. ORDEMANN, *supra* note 1, at 97.

thorities in the lands[91] only if these land authorities administer federal law, and "[i]nsofar as data protection is not governed by land law."[92] The legislature added this provision because the lands feared that they would be forced to administer two differing sets of data protection laws.[93] The original government proposal would have forced the lands to conform to the BDSG, but now data protection in the federal and land spheres may differ.[94] There is already some divergence between land and federal data protection law,[95] though great divergence now seems unlikely. In passing data protection acts after the BDSG, lands have generally patterned themselves on the Act, sometimes using identical wording.[96] The laws remain unitary, despite some fears to the contrary.[97] The restriction of Section 7(III) makes sense, however, only if the lands are supposed to be free to experiment with data protection. The legislature intended Section 7(III) primarily to be understood to allow land legislation to serve as a vehicle for the improvement and development of data protection.[98] Some experimentation is taking place and certain critics see in individual provisions of the land data protection acts possible alterations which would improve the BDSG; still, land orientation to the BDSG remains the rule rather than the exception.[99]

2. Data Processing by Governmental Entities

Governmental entities subject to the regulatory provisions of the BDSG may only store and modify data where such storage and modification are necessary for the legitimate accomplishment of the government unit's assigned tasks.[100] No storage unit may randomly collect and store data without reference to a particular job,[101] nor may a unit collect data because the unit can more conveniently do so immediately, then store the data for future use.[102] The data collected must be

91. Germany is a federal republic; the lands are roughly analogous to American states.

92. BDSG § 7(II). The Bundesrat added this provision in the second advisory reading. *See* Simitis, NJW, *supra* note 24, at 733.

93. The ostensible reason for the provision was a like provision allowing land law to prevail over federal law in VwVfG § 1(III). ORDEMANN, *supra* note 1, at 101.

94. Simitis, NJW, *supra* note 24, at 733.

95. *See, e.g.,* the Hessian and Rhein-Pfalz data protection laws, Hessian Data Protection Act of Oct. 7, 1970, GVBI 625 and Rhein-Pfalz Data Protection Act of Jan. 24, 1974, GVBI 31, which differ widely in their administrative provisions.

96. *See, e.g., Niedersächisches Datenschutgesetz* [NDSG] of May 26, 1978, NIEDERSÄCHISCHES GESETZ- UND VERORDNUNGSBLATT 421. For wording, *compare* §§ 1-6 NDSG *with* §§ 1-6 BDSG. According to at least one critic, the use of identical wording is in the interest of helping the citizens of various states to understand their rights by not subjecting them to the necessity of interpreting differently worded statutes. *See* Tuner, *Die Weiterentwicklung im Datenschutz,* 7 DVR 29, 35 (1978) [hereinafter cited as Tuner].

97. Many lands simply waited to pass data protection acts because of the proposed federal data protection law. Simitis, NJW, *supra* note 24, at 733.

98. *Id.*

99. *See generally* Tuner, *supra* note 96.

100. BDSG § 9(I).

101. Bull, *supra* note 53, at 12.

102. *Id.*

necessary to the current task.[103] If any legal provision mandates collection of the data, the collecting unit must show the person affected the relevant provision.[104] If no applicable provision regarding data collection exists, those collecting the data must inform the person from whom the data are to be gathered that he has a right to withhold the information.[105] The right to withhold data may be a "psychologically valuable aid,"[106] but how much choice the individual really has when faced with the power of a governmental agency remains open to question.[107]

Two sections of the BDSG control the communication of personal data held by the public sector.[108] Section 10[109] regulates communication between and among units belonging to the public sector, while Section 11[110] sets parameters for the transmission of data from the public sector to establishments outside of it.

---

103. *Id. But see* Simitis, NJW, *supra* note 24, at 734. "All in all, one shouldn't hope for too much from this. The American experience demonstrates clearly enough that such formulations, occurring in almost every data protection act, quickly go by the boards. Precious little changes in the attitude of the officials." *Id.* at 734. For details of the American experience, *see* DOMESTIC COUNCIL COMMITTEE ON THE RIGHT OF PRIVACY, NATIONAL INFORMATION POLICY, REPORT TO THE PRESIDENT OF THE UNITED STATES, 38 (1976).

104. BDSG § 9(II).

105. *Id.*

106. Hümmerich, *Das Bundesdatenschutzgesetz* 4 JURISTISCHE SCHULUNG 270, 272 (1977) [hereinafter cited as Hümmerich].

107. REH in SIMITIS, BDSG, *supra* note 10, at 184-87.

108. The public sector includes those establishments defined by BDSG Section 7. *See* § III.C.1 *infra*.

109. BDSG § 10 states:

> I The communication of personal data to public authorities and other public establishments shall be permissible where it is necessary for the legitimate accomplishment of the tasks for which the communicating unit or the recipient is competent.
>
> Where the personal data are subject to professional or special official secrecy (Section 45, second sentence, paragraph 1, third sentence) and where they have been communicated to the communicating unit by the person committed to secrecy in the performance of his professional or official duty, the permissibility of communication shall also be subject to the condition that the recipient requires the data for the accomplishment of the same purpose as that for which the communicating unit obtained them.
>
> II The communication of personal data to establishments of public-law religious societies is permissible by application, mutatis mutandis, of the provisions concerning the communication of data to public authorities and other public establishments, provided that adequate data protection measures are taken by the recipient.

110. BDSG § 11 states:

> The communication of personal data to persons and other establishments than those specified in Section 10 is permissible where it is necessary for the legitimate accomplishment of tasks for which the communicating unit is competent or where the recipient can demonstrate convincingly that his interest in the data to be communicated is justified and the communication of the data does not harm interests of the person concerned that warrant protection. Where the personal data are subject to professional or special official secrecy (Section 45, second sentence, paragraph 1, third sentence) and where they have been communicated to the communicating unit by the person committed to secrecy in the performance of his professional or official duty, the permissibility of communication shall also be subject to the requirement that the same conditions are met under which the person committed to secrecy would be permitted to communicate them. As regards the communication of data to public authorities and other establishments not governed by this Law and to supranational and international establishments, the first and second sentences shall apply subject to the laws and agreements applicable to such communication.

Section 10[111] allows data communication between units in the public sector if either unit needs the data for the legitimate accomplishment of its tasks.[112] When a unit requests data and the BDSG has no specific regulations governing the request, the rules of the Law on Administrative Procedures (VwVfG) govern.[113] VwVfG provides that agencies have a duty to aid one another in the accomplishment of their tasks.[114] Theoretically, no public agency has the power to procure personal data simply by invoking the general duty of interagency aid,[115] since interagency aid is not itself a justification for data communication.[116] The unit sending the data must still examine the purported need for data independently.[117] Despite the requirement for independent verification of need, some observers claim that public agencies may continue to transfer personal data without regard to need. Misgivings are strengthened by the provisions of BDSG Section 12(II)[118] which exempts numerous federal authorities from the general disclosure requirements of Section 12(I).[119] The suspicion is strong that the "good of the State" was placed before the rights of the citizen.[120] In theory, then, the individual citizen has a "right to information,"[121] but in the Federal Republic no general right to information as against the State exists. Political theory asks

---

111. *Id.* § 10.

112. *Id.* § 10(I).

113. BDSG § 44 provides: "For the purposes of implementing this Law, the Law on Administrative Procedures [VwVfG] shall also be applied insofar as such implementation is the responsibility of the Lander." *Id. See* the Law on Administrative Procedures, VwVfG of May 25, 1976, BGBl 1, 1253.

114. VwVfG § 4(I) provides: "Every authority shall supply supplemental aid (interagency aid [Amtshilfe]) to other authorities upon request." *Id.* An agency may refuse aid under certain conditions, *id.* § 5(II)(2), but the office requesting help may insist. *Id.* § 5 (V). The supervisory authority responsible for the department must then render a decision. If there is no such supervisory authority, the supervisory authority in charge of the *Behörde* from which help was requested renders the decision. *Id.*

115. Hümmerich, *supra* note 106, at 272.

116. ORDEMANN, *supra* note 1, at 1i2.

117. *Id.*

118. BDSG § 12(I) is theoretically a major disclosure provision:

> Immediately following the initial storage[,] public authorities and other official establishments shall announce in the relevant official bulletin for their sector
> 1. the type of personal data stored by them or on their behalf,
> 2. the tasks for which knowledge of these data is required.
> 3. the group of persons concerned,
> 4. the establishments to which they regularly communicate personal data, and
> 5. the type of data to be communicated.
>
> On request, previous notices shall be made available to the person concerned.

Id. The law also exempts registers required by law or other data files which must be maintained under legal or published administrative provisions. Storage units must fulfill the requirements of § 12(I), *i.e.*, the type of personal data stored, etc., must be specified in the legal or administrative provision. BDSG § 12(II)(3). The requirements of § 12 have been further implemented by the Datenschutzveröffentlichungsordnung of Aug. 3, 1977, BGBl I 1477.

119. These authorities include the authorities responsible for the protection of the constitution, the federal intelligence service, the military counter-intelligence service, the federal criminal investigation office, the departments of the public prosecutor and the police, and federal and land financial authorities. BDSG § 12(II).

120. Hümmerich, *supra* note 106, at 272.

121. *Cf.* the discussion of Art. 5 GG, at note 23 *supra*.

for transparence in administrative actions but the theory is not descriptive of the realities of administration.[122] If public data storage units can transfer personal data without regard to need and these criticisms hold true, citizens will benefit little from those portions of the BDSG controlling public administration. The BDSG will not, then, as intended, protect privacy since government departments may transmit data freely without informing the individual. To date, however, critics have presented no evidence that the BDSG has been ineffective in the regulation of public data flow.[123]

3. Transmittal of Data From the Public Sector to Third Parties

When storage units in the public sector release data to outside third parties, the requirements of Section 11 apply.[124] As under Section 9,[125] units may only release the data when such release is necessary for the legitimate accomplishment of the unit's assigned tasks. One such legitimate task involves data transfers required by law.[126] Most data transfers are not, however, required by law, and in such cases the unit desiring to transmit the data must scrutinize necessity more closely.[127] One test of necessity weighs the possibility of transfer against the task the unit must perform: if the unit can perform the task without transferring any data, the unit may transfer no data.[128]

Units outside the public sector may, of course, request data from the public sector.[129] In order to receive the data, an outside unit must first demonstrate that it has a justified interest in the data requested.[130] The concept of a "justified interest" is broad, encompassing any interest which the legal system recognizes as worthy of protection.[131] In order to receive the data, an outside unit must demonstrate that it has a specific legal basis for the request, such as a contract.[132] Individuals may also request data under the same conditions.[133] The authority undertaking to transfer the data must, however, also be satisfied that com-

---

122. Scherer, *Datenschutz und Datenzugang*, 34 JURISTENZEITUNG [JZ] 389 (1979). The lack of transparence in the German system is, according to Scherer, in direct contrast to ideas of public administration in some countries, notably the United States, which has "creat[ed] a basic general right to information: everyone has a basic right to all the information of the executive branch." *Id.* at 389, on the basis of the Freedom of Information Act, 5 U.S.C. § 552 (1976).

123. Criticism has so far, at least, been purely theoretical. *See* Simitis, NJW, supra note 24, at 732.

124. BDSG § 11.

125. BDSG § 9.

126. BDSG § 45 provides in pertinent part: "Where special provisions of the Federal Republic are applicable to personal data stored in data files, they shall take precedence over the provisions of this Law." *Id.*

127. ORDEMANN, *supra* note 1, at 117.

128. *Id.*

129. BDSG § 11.

130. *Id.*

131. LACKNER, STGB-STRAFGESETZBUCH MIT ERLÄUTERUNGEN, § 193 at comment 3 (1976).

132. *Id.*

133. BDSG § 11.

municating data "does not harm interests of the person concerned that warrant protection."[134] A unit will have to consider on a case-by-case basis whether such interests exist.[135] A possibility of some "trifling" harm will not suffice to invalidate the transfer.[136] The BDSG prohibits storage units from transferring data if the transfer would adversely affect an individual, or would involve some special risk.[137]

4. Rights of Affected Persons as Against Government Entities

Section 4 of the BDSG lists the rights generally available to a person affected by data processing activities.[138] These rights are: (1) a right to information on data stored which concern him; (2) the right to have incorrect data corrected; (3) the right to have access to data blocked when neither he nor the storage unit can demonstrate the data's accuracy or inaccuracy, or when the original need for the data no longer exists; and (4) the right to have the data erased if the storage unit had no initial right to store it.[139] Sections 13,[140] 14,[141] and 21[142] elaborate on these rights, as well as limitations on them, as against public administrative units.

a. The Right to Information

The individual has the right to receive information on stored data which concern him.[143] In order to get this information, he must request it.[144] The data processing unit then determines the procedure by, and form in which it will provide the information.[145] The information provided by the storage unit must be understandable.[146]

---

134. *Id.*

135. ORDEMANN, *supra* note 1, at 118; DAMMANN in SIMITIS, BDSG, *supra* note 10, at 384.

136. The interests of the person concerned and more of the person wishing to receive the data must be weighed against one another. DAMMANN in SIMITIS, BDSG, *supra* note 10, at 384-86. "The view taken in the rough draft — that every harm, no matter how slight, to personal interests warranting protection should lead to refusal to communicate the data — did not survive." ORDEMANN, *supra* note 1, at 118.

137. As examples, general harm might result if the address of the person affected were a prison. A special risk might exist if he had concealed his address due to threats. ORDEMANN, supra note 1, at 118.

138. BDSG § 4.

139. *Id.*

140. *Id.* § 13.

141. *Id.* § 14.

142. *Id.* § 21.

143. *Id.* § 13(I).

144. *Id.* This request could be a general one; the affected person could ask for all data stored about him. But the requirements for publication under § 12 will, in most cases, inform a person in advance of what sort of data a particular unit stores, and thus enable him to frame requests for data more narrowly. ORDEMANN, *supra* note 1, at 129. Ordemann's view may, however, be optimistic in light of the numerous disclosure exceptions provided in § 12(II). *See* notes 118 and 119 and accompanying text *supra.*

145. BDSG § 13(I).

146. ORDEMANN, *supra* note 1, at 129-30. Thus, if the data report consists of figures or abbreviations, some key must be provided for deciphering them. *Id.*

Under the BDSG, the affected person will, nonetheless, not always obtain the information he requests. Section 13(II) states that the state security authorities listed in Section 12(II) need provide no data storage information.[147] Because these authorities are not subject to any disclosure requirements, an individual may not be able to discover whether a unit has stored any data on that person.[148] Section 13(III)[149] allows other storage units to refuse to provide information if: (1) the information would be prejudicial to the legitimate accomplishment of the tasks which the storage unit is competent to perform; (2) the information would be prejudicial to public security or order; applicable law requires that the data, or the fact that they are being stored be kept secret; or (4) the information concerns transfer of data to the security authorities.[150] Although at least one critic has interpreted Section 13(III)(1) as regulating only the abuse of requests for data,[151] the language of the law does not directly support such a narrow reading.[152]

b. The Right to Data Correction

The BDSG requires storage units to correct incorrect personal data.[153] The BDSG does not require that the person affected demand correction. The unit is under an affirmative duty to correct inaccurate data.[154] A storage unit need not always correct data which have become incorrect merely through the passage of time.[155] The data may remain unchanged if they were collected only to reflect conditions current at the time of their collection.[156] The correctness of data may also depend upon their purpose: "If the set purpose is very specific, there is no right to have [the data] corrected by supplementation with data that, in context, might be useful, but are unnecessary for the purposes of the data file."[157] Finally,

147. BDSG § 13(II).

148. *See, e.g.,* Judgment of Feb. 4, 1977, Verwaltungsgerichtshof Kassel, reported at 30 NJW 1844 (1977); and the annotation of Scherer 31 NJW 237 (1978).

149. BDSG § 13(III).

150. *Id.*

151. ORDEMANN, *supra* note 1, at 131.

> It is not enough that requests for information may burden the storage unit greatly, or under certain circumstances slow down the completion of requests for other information. A request for information may [under this clause] be refused only if there is clear evidence that the affected person is not seeking information, but seeking merely to block the work of the storage unit and cause other citizens to suffer legal detriment.

Id.

152. *Id.* The narrowing is perhaps justified by the fact that otherwise anyone who repeatedly paid the fee the storage unit may charge under BDSG § 13 (IV) would be entitled to information. This fee is low (currently DM 10). *See Datenschutzgebuhrenordnung* [Regulation on Data Protection Charges] of Dec. 22, 1977, BGBl I 3153, § 2. A group of such persons could seriously impede the completion of the storage units' legitimate tasks.

153. BDSG § 14(I).

154. *Id.*

155. ORDEMANN, *supra* note 1, at 136.

156. *Id.*

157. *Id.* at 136-37.

although the incorrectness of an individual datum may be obvious, cases may also arise in which data otherwise correct have been assembled in a way that yields a false total picture. The storage unit must correct such a false picture as well.[158]

c. The Right to Block Access and the Right to Erasure

The storage unit must block access to data when an affected person disputes the accuracy of the data, and neither party can establish whether the data are accurate.[159] An affected person can challenge the correctness of data stored concerning him without having to prove they are incorrect.[160] If the storage unit cannot demonstrate that the data are correct, the storage unit must, except under certain conditions, block access to the data.[161] As a practical matter, then, the data become unusable. While the ability to shield his data in this fashion is a major advantage for the individual, critics fear that some people may abuse the privilege.[162] Certain types of data, such as opinions and recommendations, are not amenable to proof.[163] The Act in its present form may allow a person to prevent a storage unit from making legitimate use of his personal data merely by challenging the data.[164]

A storage unit must also block data when the data are no longer necessary for the task for which they were collected.[165] The unit must mark such blocked data appropriately,[166] and may not use or communicate the blocked data in any way, or reveal to outside parties that the storage unit has blocked data on an individual.[167] The purpose of this provision is to prevent third parties from unfairly concluding that the stored data are unfavorable to an individual.[168] The storage unit may, however, permit access to the data if they are "scientifically indispensable,"[169] or their release serves the overriding interests of the storage unit or of a third person.[170]

158. SIMITIS, DVR, *supra* note 28, at 144.

159. BDSG § 14(II). For conditions under which access to blocked data may be permitted, *see* notes 169 and 170 and accompanying text *infra*.

160. *Id.*

161. *Id.*

162. ORDEMANN, *supra* note 1, at 138.

163. *Id.*

164. *Id.* The original government draft recognized the possibility of abuse. This draft called for marking such data "disputed." *Id.*

165. BDSG § 14(II).

166. *Id. See also* Zapata, *Die Automatisierung der Sperrung nach dem BDSG* [sic], 2 DATENSCHUTZ UND DATENSICHERUNG 82 (1977).

167. ODERMANN, *supra,* note 1, at 139-40.

168. *Id.*

169. BDSG § 14(II). The term "scientifically indispensable" is practically meaningless, since "[t]here is no basis for such an exception. Questionable data are not material for scientific work, and little is gained with formulations like 'indispensable'," Simitis, NJW, *supra* note 24, at 735.

170. BDSG § 14(II). An example of such an overriding interest would be where data are evidence in a trial. *Id.* The storage unit may erase data when they are no longer necessary for the immediate task at

5. The Federal Data Commissioner

Section 21[171] of the BDSG is an especially important safeguard for the individual. Under this section, "any person" may apply to the Federal Commissioner[172] for Data Protection if he believes authorities of the federal government have violated his rights by processing personal data.[173] The Federal Commissioner for Data Protection is a new federal authority[174] responsible for overseeing the federal data protection laws in the public sphere.[175]

The Federal Commissioner's duties are broad. His oversight activities are not confined to enforcing the BDSG, but extend to other enactments concerning data protection.[176] Public authorities must assist the Federal Commissioner by providing information, granting him access to data files related to personal data, and allowing him entry to all offices at all times.[177] The Federal Commissioner must keep a register of automatic data files in which untis store personal data.[178] He must also submit an activity report to the Bundestag annually.[179]

Despite his duties, the Federal Commissioner has few real powers. While his right of inspection is virtually unlimited,[180] that right affords him little power of enforcement. Although he can, for example, suggest measures for improving the data protection laws, he can only submit complaints regarding violations of the BDSG and other data protection acts, or irregularities in the processing of personal data.[181] But since the enforcement mechanism is loose, "The effective-

---

hand. The unit *must* erase personal data when their initial storage was contrary to law, or when the unit has blocked them as no longer necessary, and the person affected requests their erasure. *Id.* § 14(III).

171. *Id.* § 21.

172. The draft translation employs the word "commissary"; The author has silently substituted the word "commissioner" throughout this Comment.

173. BDSG § 21.

174. Hümmerich, *supra* note 106, at 272. Sections 17 and 18, not otherwise discussed here, give such details as the minimum age of the Federal Commissioner (35), his term of office (5 years), and the oath he is to swear. BDSG § 17. Section 18 covers procedures for resignation, dismissal, and receipt of gifts, etc. *Id.* § 18.

175. Hümmerich, *supra* note 106, at 272.

176. BDSG § 19(I).

177. BDSG § 19(III)(1), (2) provides that the Commissioner is to have access "especially to stored data in storage and to data processing programmes [sic]." *Id.* § 19(III)(1).

178. The Law sets up two sets of registers. Most public authorities must register their data files with the Federal Commissioner. One register is open and any person may inspect it. Another register is restricted, and consists of lists of data files kept by authorities exempt from the general disclosure requirements of BDSG § 12(I). However, the Federal Office for the Protection of the Constitution, the Federal Intelligence Service and the Military Counterintelligence Service need not report their data files at all. BDSG § 19(IV).

179. *Id.* § 19(II).

180. The security authorities of BDSG § 12(II) are once again exempt from allowing inspection "where the competent supreme federal authority decides . . . that the inspection of documents and files would jeopardize the security of the Federal Republic or of a land." *Id.* § 19(III).

181. *Id.* § 20. The Commissioner submits the complaints, where federal administration is concerned, to the highest responsible federal authority; in the case of the federal railroad (*Bundesbann*) and other public law entities, the Commissioner submits complaints to the managing board. *Id.* Storage units responsible must reply to the Commissioner by a date specified by him and indicate the measures they are taking as a result of the complaint. *Id.*

ness of the work of the Federal Commissioner will . . . be determined not only by his legal position, but also by the amount of [political] weight he can muster to support his task."[182] Whether the office of Federal Commissioner will have real substance or whether, as some critics fear, will become a mere placebo for the executive branch remains open to question.[183]

D. *Data Processing in the Private Sector*[184]

The BDSG defines establishments in the private sector as physical and legal persons, companies and other private law associations.[185] But the law regulates data processing by these entities in somewhat different ways, depending on whether they process data for their own internal purposes, or commercially for third parties.

1. Data Processing for Internal Use

A company may store personal data, such as personnel files, for its own use. However, if the data do not come from publicly accessible sources, the data must meet one of two tests before storage is permissible. The first test permits storage if the data "serve the purpose of a contractual or [contract-like] relationship of trust with the person concerned."[186] If a contract exists, the purpose for which the contract was formed will be clear from its contents.[187] A company may then store all data necessary to accomplish that purpose.[188] The company may also store data on matters that might endanger the contract, such as adverse credit information on one of the parties.[189] In the same manner, the existence of a contract-like relationship may establish which data a company may store.[190]

The second test applies if neither a contractual nor contract-like relationship is present. The unit desiring to store the data must show that it has a "justified interest"[191] in them, and that the data are necessary for fulfillment of the

---

182. Hümmerich, *supra* note 106, at 272.

183. *Id.* The positive experience with a comparable Data Commissioner at the land level in Hesse may serve to allay such fears. *Id.*

184. The provisions of the sections discussed below generally apply as well to public law undertakings that participate in competition.

185. BDSG §§ 22, 31.

186. *Id.* § 23. The draft translation uses the term "quasi-contractual." The author has substituted "contract-like" to avoid confusion with the notion of "quasi contract" (unjust enrichment). Contract-like relationships may arise, for example, during negotiations for a contract and entail duties, the violation of which may give rise to damages, though no contract is ever formed. *See, e.g.*, Kessler & Fine, *Culpa in Contrahendo*, 77 HARV. L. REV. 40 (1964). Other examples can be found in ORDEMANN, *supra* note 1, at 182-83.

187. ORDENMANN, *supra* note 1, at 181.

188. *Id.*

189. *Id.* at 181-82.

190. *Id.* at 182-83.

191. *See* note 124 and accompanying text *supra*. The definition of "justified interest" is the same as that for Section 11.

company's business tasks. The company must also have no reason to believe that data storage will harm personal interests that warrant protection.[192] The law does not specify who is to decide whether harm to personal interests will result. The party most likely to make the determination is, therefore, the data storage unit itself.[193]

If a company wishes to modify or transfer data, the same two tests must be applied: under Section 25,[194] there must be a contract or contract-like relationship, or the particular data processing activity in question must be both necessary and benign.[195] If the company satisfies either test, it may modify or communicate the data.[196] However, the company may not retransfer any data it receives subject to professional secrecy or special official secrecy under Section 45.[197] The limitation on transfer places an additional check on data transfer where the data are "sensitive."

2. Commercial Data Processing

Companies which process personal data for commercial purposes may store data if they have no reason to assume that storage will harm interests of the person concerned that warrant protection.[198] The company may also store data

---

192. BDSG § 23.

193. ORDEMANN, *supra* note 1, at 239-40. In the interests of practical administration the data storage unit would have to have serious grounds for believing that data storage would result in damage to an affected party before rejecting data storage. *Id.* at 240.

194. BDSG § 25.

195. The same basic rules apply when a storage unit wishes to transfer personal data outside of Germany. If no contractual or contract-like relationship exists, and the country to which the unit is to send the data has no data protection act, the transferring unit may find it difficult to determine that no interests warranting protection are likely to be harmed. Under such circumstances, the unit should refuse to transfer the data unless there is a contractual relationship with the receiving unit which would protect the data as the BDSG itself would. *See* Schwappach, *Internationale Datenflüsse,* 1 DATENSCHUTZ UND DATENSICHERUNG 24 (1978). In the absence of such an arrangement, the permission of the person affected would be needed. ORDEMANN, *supra* note 1, at 192-93.

196. Certain data need not meet the test of necessity before a unit can communicate them. BDSG § 24(II) provides in part:

> By way of derogation from paragraph 1, the communication of data, in lists or otherwise compiled concerning members of a group of persons shall be permissible where this is confined to
> 1. name,
> 2. title, academic qualifications,
> 3. date of birth,
> 4. occupation, trade or business activities,
> 5. address,
> 6. telephone number,
>
> and where there is no reason to suppose that interests of the person concerned warranting protection would be harmed thereby.

Id. Commercial data processors may also assemble lists although the information they may transfer is more limited. Thus, commercial data processors may not transfer such information as birthdate, telephone number or trade, information some persons might consider "sensitive." BDSG § 32(III).

197. *Id.* § 24.

198. *Id.* § 32.

if the data come from publicly accessible sources.[199] This rule is not quite the same rule as that which applies to data processing for internal uses. While companies may process such data intended for internal use only by non-automatic methods,[200] they may use any method of processing data intended for commercial use. The BDSG does not explain the reason for the difference in the treatment accorded internal versus commercial use of data. The exception for generally accessible information is grounded on the freedom of information guaranteed by Article 5 of the Grundgesetz.[201] However, no reason exists for affording the individual less protection when a company stores his data specifically for the purpose of profiting from their commercial use or exploitation.[202] At least one critic considers the difference in treatment a concession to business which the Legislature made at the expense of data protection.[203] The same explanation may account for a difference in the data modification requirements.[204] A company may modify data for internal use unless the company has "reason to suppose" that modification will injure personal interests. In the commercial sphere, actual harm must result before data modification is impermissible.[205]

Section 32[206] of the BDSG permits a company to transfer personal data if the recipient demonstrates convincingly that he has a justified interest in the data.[207] The transfer may not harm any personal interests.[208] The party desiring information does not, however, have to prove that his interest is justified; he need only assert his justified interest in credible fashion.[209] The party transferring the data must record the means used by the requesting party to establish credibility.[210]

Some provisions of the BDSG deal more stringently with commercial data processors than with non-commercial data processing units. For example, only those units that process personal data commercially are responsible for the obligatory notification requirements of Section 39.[211] These units must report certain aspects of their data processing activities to the supervisory authorities

---

199. *Id.*
200. *Id.* § 23.
201. *See* note 23 and accompanying text *supra.*
202. Simitis, NJW, *supra* note 24, at 732-33.
203. *Id.* at 733 n33.
204. BDSG §§ 25, 33.
205. ORDEMANN, *supra* note 1, at 243.
206. BDSG § 32.
207. The concept of justified interest remains the same. *See* note 124 and accompanying text *supra.*
208. ORDEMANN, *supra* note 1, at 241.
209. BDSG § 32(II). The requesting unit need not justify its interest in detail; a simple catchword such as "contract" will suffice. ORDEMANN, *supra* note 1, at 241.
210. BDSG § 32(II).
211. *Id.* § 31(I)(3). This provision concerns notice to the supervisory authorities only; all companies must still provide information to the person affected. *Id.* § 34.

responsible for data protection under land law.[212] A commercial data processing unit must also notify the same supervisory authorities within one month of beginning or ending the processing of personal data.[213] Perhaps most important, those companies that process personal data solely for internal purposes need employ a Commissioner for Data Protection[214] only if the companies employ more than five persons to process data automatically, or twenty to process it by other methods.[215] In the commercial area, all companies must employ such a Commissioner, regardless of the company's size.[216] The Commissioner for Data Protection is an employee of the company, and is directly subordinate to the owner, or other properly appointed managers.[217] He is free to use his own knowledge of data protection "at his own discretion," and his employers may not discriminate against him for using this power.[218] The Commissioner's position is equivocal. He is a part of the company, yet his most important function is to provide the best possible protection for personal information which the company stores. If a conflict arises between the Commissioner's duties and the requirements of the company, the BDSG requires that the Commissioner uphold the data protection interests against those for whom he works.[219]

3. Supervisory Authorities

Supervisory authorities in the lands are responsible for assuring that data processing units in the private sector conform to the BDSG and other data protection acts.[220] Their powers are, however, somewhat limited especially with regard to companies which process data only for internal use. The authorities may investigate the practices of these companies only if an affected person submits evidence that a company has violated his rights during the processing of his personal data,[221] or if a company data protection commissioner asks for aid. The mere fact that an individual alleges a violation will not suffice to trigger an

212. These include the name of the firm and of its management, the type of data processing equipment used, the name of the firm's data protection commissioner, and the type of personal data stored. *Id.* § 39(II).

213. *Id.*

214. The company Commissioner for Data Protection should not be confused with the *Federal* Commissioner, a federal authority. *See* § III.C.5 *supra.*

215. BDSG § 28.

216. *Id.* § 38. A company required to have a Commissioner for Data Protection must appoint him or her in writing, and the Commissioner must have the specialized knowledge necessary for the job. *Id.* §§ 28(II), 35.

217. *Id.* §§ 28(III), 38.

218. *Id.*

219. Simitis, NJW, *supra* note 24, at 734-35. The management of the company must aid the Commissioner for Data Protection in carrying out his job. BDSG § 28(IV). But the Commissioner may also turn to the supervisory authority responsible for data protection under land law for any assistance he may request. *Id.* §§ 29, 30.

220. BDSG § 30, 40.

221. *Id.* § 30(I).

investigation, and the supervisory authorities cannot investigate on their own initiative.[222] Where units process personal data commercially, however, the supervisory authorities may initiate action.[223]

In both the commercial and non-commercial fields, once the supervisory authorities have properly begun an investigation they may enter property and inspect records insofar as such inspection is necessary.[224] Company personnel are obligated to provide information to the commissioner and must permit such entry and inspection.[225] If the storage unit does not act when the authorities discover irregularities, supervisory authorities have no enforcement powers and can merely recommend that the person affected "take his case to court."[226] In many cases, however, the fact that authorities are investigating irregularities may prompt companies to initiate corrective action to avoid a court suit.[227]

4. Rights of Affected Persons as Against the Private Sector

The individual has several rights against data processors in the private sector. Private companies must act like data processors in the public sector in correcting incorrect data, blocking access to personal data where neither party can establish the data's accuracy or inaccuracy, or when the data are no longer necessary for the purpose for which they were collected.[228] In addition, private companies must erase data if their initial storage was illegal, or the data are no longer necessary for their original purpose and the person affected requests erasure.[229] However, the BDSG contains a significant additional provision directed at the private sector. Under Section 27(III),[230] data concerning health, criminal offenses, offenses against public order and religious or political opinion must be erased if the storage unit cannot prove they are accurate.[231] The BDSG thus places the burden of proof of accuracy on the storage unit. This provision is not without problems. As noted above,[232] an affected person can, under Section

222. *Id.*

223. *Id.* § 40. *See also,* ORDEMANN, *supra* note 1, at 253-54.

224. BDSG §§ 30(III), 40. The BDSG, therefore, correspondingly limits the fundamental right of inviolability of the home guaranteed by Article 13, GG. BDSG §§ 30(III), 40(II).

225. *Id.* The management of the company must aid the Commissioner for Data Protection in carrying out his job. *Id.* § 28(IV). But the Commissioner may also turn to the supervisory authority responsible for data protection under land law for any assistance he may request. *Id.* §§ 29, 30.

226. ORDEMANN, *supra* note 1, at 230.

227 *Id.* In the case of commercial data processors, the fact that the supervisory authorities may investigate on their own is likely to result in tighter control because of the possibility of unexpected inspections or investigations. *Id.*

228. In the public sector, the test for blocking is whether the data are still necessary for tasks for which the storage unit is competent. BDSG § 14.

229. Failure to correct, block or erase data properly could give rise to an action for damages under BGB § 823. *See* note 22 and accompanying text *supra*.

230. BDSG § 27(III).

231. *Id.*

232. *See* § III.C.4.c *supra*.

14(II),[233] block access to his disputed personal data. But under Section 27(III), an affected person could extinguish particularly sensitive personal data altogether just by disputing accuracy of the data.[234] Often the storage unit will not be able to prove the accuracy of data known only to the unit and the person affected.[235] Furthermore, in some situations, a unit may be unable to provide proof of accuracy immediately, proof which may, however, be forthcoming later. If a unit has then erased the data, vital, or even merely useful, information may be permanently lost.[236]

Sections 26[237] and 34[238] of the BDSG accord the individual additional rights. A storage unit must notify the person affected when it initially acquires and stores data concerning him.[239] The individual also has the right to demand information about the data stored.[240] If the storage unit processed data automatically, the person affected has a right to information about those who regularly receive his data.[241] The storage unit must reply to data information requests in writing,[242] unless special circumstances make another form of communication appropriate.[243]

The BDSG also provides penalties for violations. The BDSG specifies two categories of illegalities: (1) offenses per se and (2) administrative offenses.[244]

---

233. BDSG § 14(II).

234. *Id.*

235. ORDEMANN, *supra* note 1, at 211-12.

236. Despite the possibility for abuse, Simitis states: "It would have been very much more convincing if the exception had been made the rule, *i.e.*, [in these circumstances] to provide for a general duty to erase." Simitis, NJW, *supra* note 24, at 732.

237. BDSG § 26.

238. *Id.* § 34.

239. *Id.* § 26. This provision applies unless the individual has gained knowledge of the storage by other means. *Id.* In the commercial sphere, the person affected has the right to such information when a data processing unit first transfers his data. *Id.* § 34.

240. *Id.* §§ 26(II), 34(II).

241. *Id.* "The term 'regularly' does not mean 'repeatedly.' . . . The deciding factor is whether data [are transferred] in all comparable cases." ORDEMANN, *supra* note 1, at 200.

242. Since providing information may involve substantial costs, the storage unit may charge a fee. The storage unit may not, however, make a profit from doing so. The fee may not exceed the actual costs the storage unit incurred. BDSG §§ 26(III), 34(III).

243. Such circumstances might arise, for example, where the person affected sees the data, then waives his right to a written response. ORDEMANN, *supra* note 1, at 201. Exceptions to the rights enumerated also exist and differ slightly according to whether the data processing unit is commercial or non-commercial. In the latter case, the primary reasons a unit may reject a request for data information are: (1) releasing the information would substantially undermine the aims of the storage unit; (2) a "competent public establishment" has determined that its release would constitute a threat to security or public order; or (3) their release is forbidden by law, or the unit must keep them secret in the overriding interest of a third party. BDSG 26(IV)(1)-(3). The only difference in the commercial case is that (1) is not an excuse for failure to provide information. *Id.* § 34(IV).

244. *Id.* §§ 41, 42. Administrative offenses are punishable with a fine of up to 50,000 D.M. Such offenses include any failure to observe the more important procedural requirements of the law, *e.g.*, failure to notify an affected person when a storage unit first stores his data, *id.* §§ 26, 34, or failure to employ a data protection commissioner. *Id.* §§ 28, 38.

Under Section 41,[245] any person who communicates, modifies, retrieves[246] or procures personal data without authorization is subject to the imposition of a fine or imprisonment.[247] However, an individual must file a complaint before the government will prosecute.[248]

IV. ANALYSIS OF THE BDSG

In light of the complicated legislative history of the BDSG,[249] the skepticism with which critics first greeted the Act is understandable. To one critic, the law represented a "Magna Charta" for the modern citizen;[250] to another, the BDSG appeared "vitiated by compromise."[251] Criticism far outweighed approval, however, and within a few months of the laws's passage both the government and opposition parties agreed that the BDSG needed revisions.[252]

Critics frequently concentrate their criticisms on the law's lack of precision.[253] Although the BDSG represents the most complete attempt yet made anywhere to regulate personal data processing,[254] its broad reach results in a lack of precision.[255] For example, the exact definition of such basic terms as "data file" is unclear, and the law fails to enumerate explicitly those specific features comprising a data file.[256] Other language is too general. For example, the statute contains no explanation or definition of the "justified interest" that a third party must show before a data unit can transfer data to him under Sections 11,[257] 24,[258] and 32.[259] The Act fails to define even those phrases that appear frequently such as "interests of the person concerned warranting protection." Interpretive difficulties are likely to remain thorny, yet the fate of the law rests on that interpretation. The more lax the interpretation of crucial concepts, the more data protection becomes an illusion.[260]

---

245. *Id.* § 41.

246. The term "retrieving" appears in its technical sense, *i.e.*, automated data retrieval.

247. For laws that continue to be valid and would authorize such procedures, *see* BDSG § 45. If a person commits the offense for gain, or in order to harm another, the prison term may be increased to two years. *Id.* § 41(II).

248. *Id.* § 41(II). The person affected by unauthorized data transfer may file such a complaint, as may the storage unit in the event of data theft. ORDERMANN, *supra* note 1, at 258.

249. SIMITIS, BDSG, *supra* note 10, at 61, notes that "few laws in the history of the Federal Republic can have had so complicated a parliamentary background."

250. Auernhammer in H. KRAUCH, ERFASSUNGSSCHUTZ, 57 (1975).

251. Steinmüller, 7 BILD DER WISSENSCHAFT 76, 76 (1976).

252. BT-DRUCKS. VIII/191; BT-DRUCKS. VIII/266.

253. *See, e.g.*, the discussion by Simitis of the terms "justified interest" and "necessity." SIMITIS, BDSG, *supra* note 10, at 73-74.

254. *Id.* at 72.

255. *Id.* "General clauses rule the field." *Id.*

256. *See* § III.B *supra*.

257. BDSG § 11.

258. *Id.* § 24.

259. *Id.* § 32.

260. Simitis, NJW, *supra* note 24, at 732.

An example will demonstrate the difficulties the terminological imprecision of the Act may generate. As previously discussed, the BDSG regulates data processing units in different ways, depending on the purpose for which the unit processes data. Yet, large conglomerates have subsidiaries which not only process data for themselves, but transfer data to one another for purposes affecting the entire conglomerate as well. The BDSG does not specifically determine whether such a unit processes data for internal purposes or for third parties. The BDSG states that a company must process data in the "normal course of business," [geschäftsmäßig][261] if it is to be considered as processing data for third parties. However, the meaning of "normal course of business" is also vague. One critic contends that to be within the "normal course of business," data processing must itself be the business of the company.[262] Other critics would not reach that conclusion.[263] These disparities in interpretation may prove fatal to proper application of the BDSG, since the degree of inspection the BDSG requires will turn on this distinction. A company which processes data only for its own purposes is, for example, not subject to the extensive registration provisions of Section 39.[264]

In order to avoid registration, a company will have every reason to assert that it is processing data only for internal purposes.[265] Some critics have asserted, in addition, that the Act is so unclear that it is unconstitutionally vague.[266] They contend that neither the person affected nor the person seeking to process personal data could learn from the law what it required of him.[267] This criticism seems unduly harsh since the regulatory scheme of the act is clear, but critics have raised other constitutional objections, as well. Since Article 19 of the *Grundgesetz* makes fundamental rights applicable to legal persons,[268] the legislature may have to include the "personal" data of such entities as corporations within the BDSG's protections.

Another constitutional difficulty may exist because certain public law entities (banks and credit institutions, for example) participate in competition in the open market, yet are exempt from certain of the BDSG's requirements for private storage units.[269] These exempted entities need not, for example, employ a commissioner for data protection, nor do they need to comply with the registration provisions of Section 39.[270] Such exempting may give the public-law

261. BDSG § 31.

262. ORDEMANN, *supra* note 1, at 236.

263. Simitis, NJW, *supra* note 24, at 733. Even Ordemann admits that "it will not always be clear in the individual case whether the data processing of personal data should be assigned to part 3 or part 4 [of the Act]." ORDEMANN, *supra* note 1, at 236.

264. BDSG § 39. *See* notes 192-93 and accompanying text *supra*.

265. Simitis, NJW *supra* note 24, at 733.

266. Müller-Lutz, 1976 VERSICHERUNGSWIRTSCHAFT 908.

267. SIMITIS, BDSG, *supra* note 10, at 72-73.

268. *See* note 64 and accompanying text *supra*.

269. BDSG §§ 22, 31.

270. *Id.* § 39.

entities a business advantage, and, in certain circumstances, "such limitations on private enterprise in favor of public law undertakings are unconstitutional."[271] No one has yet tested these exemptions.

Another serious objection to the BDSG is that despite its attempt to regulate the entire field of personal data processing, it does not do so. Although it is usual in Germany for federal law to take precedence over land law,[272] the BDSG specifically allows land data protection acts superiority over the BDSG in wherever land law applies to data protection.[273] Both companies and those carrying out the Act will, therefore, need constantly to refer to land data protection acts. This provision is particularly problematic. Data protection would seem to require national uniformity if business and individuals are not to be subjected to the vagaries of local (land) law. Land legislation since the advent of the BDSG has shown itself sensitive to this problem by orienting itself to the BDSG, but the provision might easily have led to a chaos of inconsistent regulations. Fortunately, this has not been the case.

The BDSG is also incomplete due to its failure to deal directly with international data transfer. The omission was deliberate,[274] but unfortunate, especially in the light of the increasing importance of international data flow. The BDSG could not have regulated all transnational data traffic,[275] but a clear formulation of rules for international data transfer both into and out of West Germany would greatly have simplified the problems of multinational companies dealing in the German market. In its present form, the BDSG deals with transnational data flow only indirectly,[276] and in a fashion hardly commensurate with the importance of the problem.[277]

For the time being, however, both government and business must implement the law in its present form. Both will find the task difficult. The law will require organizational, technical and personnel changes in almost all business and administrative fields.[278] Businesses and administrative units will have to rewrite the texts of contracts and other routine business documents to conform to the Act.[279] Both sectors' personnel will also have to train personnel to understand the law

---

271. Schweizer, *Kernprobleme des Bundesdatenschutzgesetzes,* 30 DER BETRIEB 289 (1977). The argument rests on "equal protection." Art. 3(I) GG provides: "All persons are equal before the law." *Id.* This is a fundamental right, and applies to native legal persons as well as natural ones through Art. 19 GG. *See* Gubelt in VON MÜNCH, *supra* note 15, at 122, and cases there cited. The phrase "before the law" is also binding for legislation. That is, all legislation must incorporate the fundamental right of equality before the law. *Id.* at 123. Here, the Act, without apparent ground, treats companies participating in the open market differently depending on whether they are publicly or privately owned.

272. *See* GG article 31; *see also* B. SCHMIDT-BLEIBTREU & F. KLEIN, KOMMENTAR ZUM GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND 475-77 (5th ed. 1980).

273. BDSG § 7.

274. SIMITIS, BDSG, *supra* note 10, at 547-48.

275. For such regulation, an international treaty would be necessary. *See id.* at 548.

276. Simitis, NJW, *supra* note 24, at 737.

277. *Id.*

278. SIMITIS, MATERIALIEN, *supra* note 39, at 9.

279. *Id.*

and apply its standards.[280] Given the difficulties inherent in the BDSG, one cannot be sure how readily or effectively this goal can be accomplished.

Perhaps the most important flaw in the BDSG is its failure to provide for damages when a data processing unit misuses personal data. The injured citizen has recourse to the courts and may sue for damages under the Civil Code. In order to recover damages, however, he will have to demonstrate that the unit was at fault in some way, either deliberately or through negligence,[281] and such fault will generally be difficult to prove.[282] One might overcome this difficulty by creating a system of strict liability for the misuse of personal data protected by the BDSG.[283] Such a system would almost certainly make the storage unit more attentive to the requirements of the law, and thus more attentive to individual rights.[284]

V. CONCLUSION

The German Federal Data Protection Act of 1977 (BDSG) protects all forms of personal data on an identified or identifiable natural person. The Act provides protection during all phases of data processing: storage, modification, transfer and erasure. Under the BDSG, data processing units in both the public and private sectors may process personal data only if the BDSG or another law specifically permits it, or the person whose data a unit wishes to process has given his consent. The BDSG treats data processors in the public and private sectors somewhat differently.

Storage units in the public sector may store, transfer or receive data only when the data are necessary for the accomplishment of the legitimate tasks of the storage unit. The affected person has the right to request information on the data stored concerning him, and a right to its correction, blockage or erasure under certain conditions. He may also appeal to the Federal Commissioner for Data Protection if he feels that a data processing unit has violated his rights.

As applied to the private sector, the rules for data storage, transfer, modification and erasure vary according to whether a unit processes personal data for its internal use, or for a commercial purpose. Storage units must erase particularly sensitive data, such as those pertaining to race or religion, if the storage unit cannot demonstrate that the data are accurate.

Despite criticisms, the BDSG is an improvement over earlier German attempts to protect personal data. The Act grants the individual a measure of respect for

---

280. *Id.*

281. *See* note 22 and accompanying text *supra*.

282. Tuner, *supra* note 96, at 37.

283. *Id.*

284. The possibility exists, of course, that individuals might abuse such a system by bringing false or ill-founded claims, but this danger can be lessened by providing that the amount of damages should be contingent on the actual harm suffered.

his personal integrity, and indicates a willingness on the part of the German legislature to work against dangers to privacy which may arise out of data processing. But the BDSG is seriously flawed, by its lack of precision, undefined terms and failure to provide adequate damages for the misuse of personal data. The Germans themselves recognize that future legislation in the area of personal data processing must be directed at specific and precise problems, since data processing is so complex. No single law can manage the entire field, and the BDSG will require considerable updating and improvement. The BDSG is, therefore, not a final answer, but a commendable first step in regulating the processing of personal data.

J. Lee Riccardi