

# DATA PROTECTION AND THE RIGHT TO PRIVACY IN THE UNITED STATES AND WEST GERMANY

## INTRODUCTION

The increasing use of computers in contemporary society has produced numerous threats to human rights. Computer data banks provide a vast amount of personal information<sup>1</sup> to governmental bodies and private firms. Consequently, a need has developed for protecting not only the accuracy but also the confidentiality of such personal data.<sup>2</sup> The present article examines and compares the developments that have taken place regarding data protection in West Germany and the United States. West Germany's experience may help the United States to further develop its present system.

## A SHORT HISTORY

In the United States, the individual's interest in privacy<sup>3</sup> first became recognized as a constitutional principle<sup>4</sup> in *Griswold v. Connecticut*.<sup>5</sup> *Griswold* expanded on earlier due process and equal protection

---

<sup>1</sup>Trubow defines personal information as follows:

Personal information is any information that identifiably refers to an individual by name, number, or any other identifying characteristic. Information is personal not because of its content but because of its reference. Therefore, information which describes or is about a specific individual is considered personal. Whether information is confidential depends upon the law or policy restricting its collection, use, or storage. The degree to which information is secure depends upon the technology and procedure designed to enforce the confidentiality of that information.

G. Trubow, *Information Law Overview*, 18 J. Marshall L. Rev. 817 (1985).

<sup>2</sup>A. Evans, *European Data Protection Law*, 29 Am. J. Comp. L. 571 (1981).

<sup>3</sup>Trubow defines privacy as follows:

Privacy is a characteristic of a natural person and, in informational terms, refers to what, how, and why information about an identifiable person is gathered. One's privacy is violated if personal information about him or her is collected or disclosed without lawful justification.

*Supra* note 1, at 817.

Turn defines privacy as follows:

[P]rivacy refers to certain rights of individuals vis-a-vis the collection, processing, storage, dissemination, and use in decision-making of personal data.

R. Turn, *Privacy Protection and Security in Transnational Data Processing Systems*, 16 Stan. J. Int'l L. 69 (1980).

Hondius points out that the expression "data protection" is derived from the German word *Datenschutz*. F. Hondius, *Data Law in Europe*, 16 Stan. J. Int'l L. 87, 89 (1980).

<sup>4</sup>Warren and Brandeis first introduced the legal concept of privacy into American jurisprudence in 1890 in their famous article *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890). See also J. Beach, *State Equal Rights Amendments: Models for the Future*, 184 Ariz. St. L. J. 693 (1984); Trubow, *supra* note 1, at 816.

<sup>5</sup>381 U.S. 479 (1965).

precedent.<sup>6</sup> In *Griswold*, the United States Supreme Court struck down a state law making it a crime for married couples to use contraceptives and for the Planned Parenthood League to recommend their use. The Court held that the state had invaded privacy interests.<sup>7</sup> The privacy right in *Griswold* served as the basis for the landmark decision in *Roe v. Wade*.<sup>8</sup> A great deal of legislation has since been enacted and public interest in privacy of information has grown.

In West Germany, the judiciary, influenced by the U.S., constitutionalized a law of privacy after the founding of the Federal Republic in 1949.<sup>9</sup> Article 1(1) of the German Constitution<sup>10</sup> declares that the state is obligated to respect and protect a person's dignity. Moreover, Article 2(1) provides that insofar as a person does not injure the rights of others and does not violate the constitutional order and moral law, he has the right to freely develop his personality.<sup>11</sup> These two articles in the German Constitution are looked upon as an omnibus clause.<sup>12</sup> If no other provision of the Constitution guarantees one's right to privacy, these two articles taken together will do so.<sup>13</sup> The state, however, can limit or expand upon this freedom if a "constitutional order" is authorized by the legislature, since it is the duty of the legislature and the judiciary to interpret and develop the German Constitution within the limits fixed by the Constitution itself.<sup>14</sup>

---

<sup>6</sup>*Pierce v. Society of Sisters*, 268 U.S. 510 (1925); *Skinner v. Oklahoma*, 316 U.S. 535 (1942).  
<sup>7</sup>*Griswold supra* note 5. F. Beytagh Jr., *Privacy in Perspective: The Experience under Foreign Constitutions*, 15 U. Tol. L. Rev. 449 (1984) gives an extensive analysis of the *Griswold* decision.

<sup>8</sup>410 U.S. 113 (1973). See also Beytagh, *supra* note 7, at 456-459.

<sup>9</sup>In private law, the German Civil Code (*Bürgerliches Gesetzbuch* [BGB]) Section 823(1), recognizes a right to privacy to be among the "other rights" protected by BGB Section 823(1), long before the Federal Republic came into existence.

<sup>10</sup>Grundgesetz [GG].

<sup>11</sup>GG.

<sup>12</sup>See B. Schmidt-Bleibtreu and F. Klein, *Kommentar zum Grundgesetz* 158-168 (3d ed. 1975).

<sup>13</sup>Note, *The Reform of West German Data Protection Law as a Necessary Correlate to Improving Domestic Security*, 24 Colum. J. Transnat'l L. 605 (1986) gives a slightly different explanation of the interaction between Article 1(1) and 2(1) of the German Constitution. The viewpoint expressed in the present article, however, reflects the dominant opinion in West German literature and jurisprudence. See also *Basic Law for the Federal Republic of Germany*, 14 *Constitutions of the Countries of the World* (A. Blaustein & G. Flanz eds. 1983) and Beytagh, *supra* note 7, at 471-472.

<sup>14</sup>GG Art. 93 gives the Federal Constitutional Court the authority to decide cases on complaints of unconstitutionality by any person who claims that one of his basic rights has been violated by public authority. See Beytagh, *supra* note 7, at 472; Schmidt-Bleibtreu, *supra* note 12; K. Stollreither, *Der Gläserne Mensch - noch Zukunft oder schon Gegenwart?*, *Datenverarbeitung und Persönlichkeitsschutz - Beiträge zu aktuellen Problemen des Datenschutzes in Recht und Praxis* 17 (1986); and W. Teske, *Der Zugang zu den Datenbanken der Wirtschaft, Datenverarbeitung und Persönlichkeitsschutz - Beiträge zu aktuellen Problemen des Datenschutzes in Recht und Praxis* 106,107 (1986).

## DATA PROTECTION IN GENERAL

In contrast to West German law where one specific act (the Federal Data Protection Act) describes the law of data protection, there are several U.S. acts governing different areas of data protection. One is the Right to Privacy Act of 1973, which sets the rules governing the handling of personal information by federal agencies. Other significant acts are: the Fair Credit Reporting Act (1970), the Right to Financial Privacy Act of 1978, the Privacy Protection Act of 1980, the Electronic Fund Transfer Act of 1980, and the Family Education Rights and Privacy Act of 1974.<sup>15</sup>

The Fair Credit Reporting Act was the first legislation regulating private sector information. It requires credit investigation and reporting agencies to give access to their files so that data subjects are able to inspect and copy recorded information.<sup>16</sup> The Federal Data Protection Act of Germany also has some provisions regarding credit investigations.

The Right to Financial Privacy Act establishes procedures for federal agencies to gain access to bank records.<sup>17</sup> In West Germany, no similar protective code exists. Rather, financial records are protected through the *Bankgeheimnis* or banking secrecy rule. This rule can be described as the obligation of any bank or credit union to keep confidential all the information about a person's financial situation. Such a duty is implemented in any relationship between a bank and a private person or company. The *Bankgeheimnis*, however, reaches its limits as soon as certain federal agencies are involved. The *Bundesaufsichtsamt fuer Kreditwesen* (Federal Banking Supervisory Board) is entitled to certain bank information according to sections 13, 14, and 44 of the *Kreditwesengesetz* (Credit System Act). In addition, the *Finanzamt* (Revenue Department) is allowed access to bank information in specific cases as provided in the *Abgabenordnung* (Tax Code).

The Privacy Protection Act regulates the way law enforcement agencies may acquire print media records.<sup>18</sup> In Germany, the records of the public media are always considered to be private. Only a court order allowing the search and seizure of such records can result in their acquisition.

The Electronic Fund Transfer Act requires each bank to notify its customers about routine third party disclosures of personal records.<sup>19</sup>

---

<sup>15</sup>See Trubow, *supra* note 1, at 824-825. Trubow also lists the Freedom of Information Act (1966) and the Crime Control Act of 1973.

<sup>16</sup>Trubow, *supra* note 1, at 824.

<sup>17</sup>*Id.* at 825.

<sup>18</sup>*Id.* at 825. The Supreme Court decision in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978) compelled this legislation. The court permitted law enforcement access to a student newspaper's file where articles and photographs of a clash between demonstrators and police had been published.

<sup>19</sup>Trubow, *supra* note 1, at 825.

Although no such act exists in Germany, the Federal Data Protection Act touches on this area.

The Family Education Rights and Privacy Act, also known as the Buckley Amendment, sharply limits the disclosure of student records to third parties. However, such control in the educational sector is not necessary in Germany since the system of disclosing records works differently. Neither schools nor universities keep public records. Instead, every student gets the original plus as many official copies of his grades as necessary for his own records. If additional copies are needed, photocopies can be verified by the city or a notary public.

### COMPARISON OF THE RIGHT TO PRIVACY ACT IN THE U.S. AND THE FEDERAL DATA PROTECTION ACT IN WEST GERMANY

In 1977, West Germany enacted the Federal Data Protection Act<sup>20</sup> in order to ensure that the right to privacy is protected when personal data is processed.<sup>21</sup> The purpose of the German Federal Data Protection Act is to prevent the infringement of valuable interests of those affected by abuses in storing, transferring, altering, and deletion of personal data.<sup>22</sup> The same intent can be seen in the U.S. Privacy Act.<sup>23</sup> Each of the eleven German states is entitled to enact its own state data protection law. Hessen had a state data act even before the federal counterpart was authorized. In general, the German Federal Data Protection Act is distinguishable from the U.S. Privacy Act.

#### *Disclosing Records Without Consent*

##### In the U.S.

According to 5 U.S.C. §§552a(b) and 552, agencies, as defined in 5 U.S.C. §552a(a), are allowed to disclose records pertaining to an individual without his consent only under certain circumstances. Disclosures are permitted in the following generalized cases:<sup>24</sup> (1) in the performance of agency duties; (2) for publication in the Federal Register;<sup>25</sup> (3) for routine use; (4) for census purposes; (5) for statistical research; (6) for historical value; (7) for a civil or criminal law enforcement

---

<sup>20</sup>Bundesdatenschutzgesetz [BDSG].

<sup>21</sup>R. Ehlke, *The Privacy Act After a Decade*, 18 J. Marshall L. Rev. 829 (1985).

<sup>22</sup>BDSG § 1(1). See also *supra* note 13, at 600-601.

<sup>23</sup>Evans, *supra* note 2, at 571.

<sup>24</sup>5 U.S.C. § 552a(b)(1)-(12).

<sup>25</sup>As required under 5 U.S.C. § 552.

activity; (8) for health or safety purposes; (9) to the House of Congress or its committees; (10) to the Comptroller General; (11) pursuant to a court order; and (12) to a consumer reporting agency. Federal agencies must account for such disclosures.<sup>26</sup>

### In West Germany

The official collection of personal data is not protected under the Federal Data Protection Act.<sup>27</sup> Storage and alteration, however, is permissible only with the written consent of the data subject.<sup>28</sup> The Act distinguishes between data processing by public agencies and by other non-public organizations.<sup>29</sup>

#### a. Data Processing in Regard to Public Agencies

Governmental or public agencies are allowed to process personal data if necessary to fulfill their duties.<sup>30</sup> All governmental agencies are allowed to transfer personal data if they decide it is necessary to accomplish the authorized objectives of the particular agency.<sup>31</sup> Thus, an extensive blanket clause permits the misuse of personal data. The data subject who desires protection can only find help in state data protection laws. Bavaria, for example, only permits the processing of personal data if the state government enacts a statutory provision defining when such a procedure is permissible.<sup>32</sup>

The Federal Data Protection Act of West Germany also allows agencies to transfer nonconfidential personal data to other data users such as professional data banks and private persons.<sup>33</sup> In general, however, federal governmental agencies and everyone dealing with confidential data have an obligation of secrecy.<sup>34</sup> In addition, every agency is legally bound to take special measures for protection from theft,<sup>35</sup> sabotage, fire, and water damage.<sup>36</sup>

---

<sup>26</sup>5 U.S.C. § 552a(c).

<sup>27</sup>M. Knott, *Die Angst vor dem Computer - berechtigt oder nicht? — Technische Möglichkeiten und rechtliche Schranken*, Datenverarbeitung und Persönlichkeitsschutz — Beiträge zu aktuellen Problemen des Datenschutzes in Recht und Praxis 37, 38 (1986).

<sup>28</sup>BDSG § 3(1). See also *supra* note 13, at 601-602, *supra* note 26.

<sup>29</sup>BDSG §§ 22-40.

<sup>30</sup>BDSG §§ 9(1), 10, 11 and 14(3). See also Knott, *supra* note 26, at 37.

<sup>31</sup>BDSG § 10(1). See Knott, *supra* note 26, at 37.

<sup>32</sup>Datenschutzgesetz of Bavaria §§ 16-18. See Knott, *supra* note 26, at 37-38; and *supra* note 13, at 600.

<sup>33</sup>BDSG § 11(2). See Knott, *supra* note 26, at 38; and *supra* note 13, at 602.

<sup>34</sup>BDSG §§ 5, 10(1) and 11(2). See Knott, *supra* note 26, at 38.

<sup>35</sup>Computer hackers are within this context.

<sup>36</sup>BDSG § 6. See Knott, *supra* note 26, at 37.

### b. Data Protection in Regard to Non-Governmental Agencies

The Federal Data Protection Act has special provisions for processing data for one's own purpose<sup>37</sup> and for processing data for others.<sup>38</sup> In the first case, data processing is generally permissible as long as it is within the boundaries of a contractual or a similar confidential relationship.<sup>39</sup> In the second case, three categories were formed:<sup>40</sup>

- 1) those organizations that store and transfer data, such as commercial agencies, trade protection societies, detective agencies, and agencies trading addresses. They can process personal data if there is no violation of the rights of the data subject.<sup>41</sup>
- 2) agencies that research public opinions and investigate consumer behavior. Since they deal with anonymous data, they are only allowed to process personal data with the consent of the data subject.
- 3) data service groups. They also are allowed only to process personal data with permission.

#### *Right to Access, Notice, and Deletion*

##### In the U.S.

5 U.S.C. §552a(d) provides that an individual is to be granted access to the records which an agency possesses pertaining to him. He is also granted the opportunity to amend inaccurate records or object to their content.

##### In West Germany

The right of a data subject differs according to the Federal Data Protection Act.

### a. Governmental Data Processing

Concerning the governmental data processing procedure, the person affected has a right to seek information regarding his personal data but must pay for the information.<sup>42</sup> If security aspects are affected, the agency

---

<sup>37</sup>BDSG §§ 22-30.

<sup>38</sup>BDSG §§ 31-40.

<sup>39</sup>BDSG §§ 23(1), 24(1), and 25. See Knott, *supra* note 26, at 38.

<sup>40</sup>BDSG § 31. See Knott, *supra* note 26, at 38.

<sup>41</sup>BDSG §§ 23 and 24(1).

<sup>42</sup>BDSG § 13. See Knott, *supra* note 26, at 39.

can refuse to give out the information. Public notice has to be given of the storage and processing of personal data in the *Bundesanzeiger* four times a year.<sup>43</sup> False data must be corrected or deleted, and every agency regularly receiving personal data from another agency has to be informed about the correction.<sup>44</sup> State data protection may differ in some respects. In Bavaria, for example, the “data victim” can sue for up to \$130,000.00 for compensation in case of unlawful data processing.<sup>45</sup>

#### b. Non-Governmental Data Processing for One’s Own Purposes

Every data subject has the right of access to all personal data and he is entitled to be informed as to which data is transferred to what agency.<sup>46</sup> However, there is no notice requirement for the transferral to other agencies.<sup>47</sup> Deletion is required as soon as it has been discovered that the data is incorrect.<sup>48</sup>

#### c. Non-Governmental Data Processing for Outside or Other Purposes

Generally, the same rights are available as in the group of non-governmental data processing for one’s own purpose. However, there are a few notable differences. After five years of storage, the data must be blocked. There is no right to control data processing since the data subject has to give permission to the consumer reporting agencies and service groups to process personal data.<sup>49</sup>

### *Agency Maintenance Requirements*

Several maintenance requirements must be observed by U.S. agencies.<sup>50</sup> These requirements are: (1) maintaining only those personal records relevant and necessary for agency purposes; (2) collecting information to the greatest extent possible from the subject individual; (3) informing each individual who supplies information about the authority and the purposes of gathering the information; (4) publishing information in the Federal Register about the functioning of the records systems and their access; (5) assuring the accuracy, relevance, timeliness, and completeness of such personal records; (6) maintaining no records

<sup>43</sup>BDSG § 12. See Knott, *supra* note 26, at 39; and *supra* note 13, at 603.

<sup>44</sup>BDSG § 14 (correction/deletion) and § 16(3) (informing other agencies). See Knott, *supra* note 26, at 39.

<sup>45</sup>Bayrisches Datenschutzgesetz § 13. See Knott, *supra* note 26, at 39.

<sup>46</sup>BDSG § 26. See Knott, *supra* note 26, at 40.

<sup>47</sup>Knott, *supra* note 26, at 39.

<sup>48</sup>BDSG § 27. See Knott, *supra* note 26, at 40.

<sup>49</sup>Knott, *supra* note 26, at 40.

<sup>50</sup>5 U.S.C. § 552a(e)(1)-(10).

on first amendment activities of individuals; and (7) establishing rules of conduct for persons handling personal records, including safeguards.

There is no significant difference between the requirements of the U.S. Privacy Act and the German Federal Data Protection Act regarding these maintenance requirements.

### *Remedies*

#### In the U.S.

Civil remedies as well as criminal penalties for violation of the Act are available.<sup>51</sup>

#### In West Germany

The Federal Data Protection Act does not include criminal or civil remedies. However, the provision of the *Buergerliches Gesetzbuch* (Civil Code) and the *Strafgesetzbuch* (Criminal Code) apply to violations of the Data Protection Act. For example, Civil Code § 839, together with Article 34 of the German Constitution, guarantee civil remedies for the data victim. Therefore, there is no need for additional regulations in the Federal Data Protection Act.

### *The Data Commissioner*

An additional supervisory check unknown in the U.S. but present in Germany is the Data Commissioner. The federal government and each state have independent commissioners, who monitor compliance with governmental and private data processing with the Federal Data Protection Act. The office has a dual function. On one hand, the commissioner is the point of contact for every citizen. All affected persons have the right to address the commissioner. On the other hand, it is the commissioner's duty to guide public agencies in their data processing. Should the agencies have any questions, they, too, are encouraged to ask the commissioner for help and guidance. Finally, the state and the federal government may request the commissioner's expert opinion. Every year, the data commissioner publishes an overview regarding matters of concern and providing suggestions for improvements. Overall, the independent data commissioner is an important part of effective and just data protection.

---

<sup>51</sup>5 U.S.C. § 552(g) and (i).

## THE CENSUS DECISION

Following a few important decisions on the right to privacy,<sup>52</sup> in 1983 the West German Federal Constitutional Court imposed demanding restrictions on the government's use of personal data.<sup>53</sup> A statute called *Volkzsaehlungsgesetz*, which had been unanimously enacted, was declared unconstitutional. The major concern of the court was that data gleaned from a census was intended to be used not only for statistical purposes, but also to update and correct information in local registration agencies, where every citizen and legal resident is requested to register. The court concluded that individual privacy and participation in public affairs could only be guaranteed if the existing public policy was reversed.<sup>54</sup>

## CONCLUSION

Both countries have taken giant steps toward establishing the data protection rights of individuals. However, neither country has fully protected a person's right to privacy with respect to personal data. The U.S. Privacy Act of 1974 applies solely to the federal government. Only a few states have enacted similar laws.<sup>55</sup> In addition, a supervisory check such as a Data Commissioner is unknown in the U.S. Furthermore, only American citizens and permanent resident aliens are protected under the Privacy Act, whereas the German law protects all persons regardless of citizenship or nationality.<sup>56</sup> However, one significant advantage of the U.S. right to privacy over the German system is that the U.S. protects manual as well as automated record-keeping systems.<sup>57</sup> United States data protection law might take into account the following suggestions:

- 1) Data protection laws should be made uniform throughout the 50 states.
- 2) Independent commissioners should be appointed on both state and federal levels.
- 3) Data protection should be for everyone, not just citizens and permanent residents.
- 4) In certain cases, the right of the individual should outweigh the

---

<sup>52</sup>In 1969, the West German Federal Constitutional Court developed principles concerning human dignity as part of the right to privacy in *Mikrozensus-Beschluss*, 27 BVerfGE 1. See Stollreither, *supra* note 14, p. 17-18.

<sup>53</sup>Judgment of Dec. 15, 1983, 65 BVerfGE 1.

<sup>54</sup>See also *supra* note 13, at 597-598.

<sup>55</sup>Turn, *supra* note 3, at 75-76.

<sup>56</sup>GG Art. 3 provides that everyone is to be treated equally. Therefore, the Data Protection Act applies equally to all. See Turn, *supra* note 3, at 76.

<sup>57</sup>Turn, *supra* note 3, at 76.

interest of the government and other agencies collecting and processing data. Therefore, the Privacy Act should be revised to increase protection of privacy rights.

- 5) Data protection should take precedence if there is a conflict between two statutory rules.
- 6) The public should be kept informed of their basic legal rights.

*Angela Daniel-Paczosa\**



---

\*Attorney at Law, West Germany.