



Global Business Dialogue on Electronic Commerce

Consumer Confidence Personal Data Privacy Protection

September 14, 2001

Issue Chair	<i>Carleton S. Fiorina</i> Chairman & CEO Hewlett-Packard
Contact Point (Europe/Africa)	<i>Dr. Klaus Mangold</i> CEO DaimlerChrysler Services (debis) AG and Board Member, DaimlerChrysler AG
Contact Point (Asia/Oceania)	<i>Eiichi Yoshikawa</i> Executive Vice President and Member of the Board NEC Corporation

INTRODUCTION

The growth of electronic commerce has heightened concerns over the collection and use of personal data by companies. The GBDe recognizes that addressing these concerns is crucial to building confidence in the online medium whether fixed or mobile.

The wide variety of legal norms and cultural expectations regarding privacy make it difficult to develop a single set of rules to govern global information practices, and the diversity of online services and business models complicates the task. Greater consistency among privacy policies, however, would yield important benefits. If merchants agree to observe certain guidelines for privacy protection no matter where they do business, consumers will have an easier time understanding what to expect when they disclose personal data online. For

companies, a global consensus for privacy guidelines would encourage more uniform legal approaches as well as improving the prospects for winning and retaining customers by using the Internet.

For these reasons, the GBDe has prepared “GBDe Personal Data Privacy Protection Guidelines”, as set out below. This document contains guidelines, which have been developed by the GBDe for voluntary application by Internet merchants, by trustmark providers, and by any other businesses for whom they may be of relevance. The GBDe encourages all its members, and all other businesses to utilize these guidelines in the worldwide application of privacy data protection, (applied in parallel and with due respect to applicable law). These guidelines are developed from the 1980 OECD data protection guidelines and reflect two decades of technological and consumer

protection policy developments. At the same time, they are guidelines developed by and for businesses that operate across global borders in a dynamic business and technological environment. These GBDE “Personal Data Privacy Protection Guidelines” provide sufficient detail to be meaningful, while avoiding specifying details, in order to allow companies the necessary flexibility to adapt their privacy practices to specific legal, industry sector or cultural circumstances. For example, some consumer advocates have observed that even as a greater proportion of web sites have posted privacy policies, these policies are often encumbered with so many disclaimers and so much “fine print” that consumers are unlikely to read them. To avoid this problem, the guidelines provide that companies should disclose whatever information is necessary to make a proposed collection and use of information fair. An illustrative list of categories of information that may be appropriate to disclose is provided, but the guidelines recognize that the kinds of information that will be helpful or relevant to consumers depends on the specific situation.

The GBDE calls for companies to set company policies that respect and use these guidelines whether or not they are required by applicable law. The guidelines are not intended to be a substitute for applicable law, but rather are intended to promote certain widely recognized basic principles for the protection of consumer privacy in the context of electronic commerce. While some aspects of the guidelines are more flexible than substantive data privacy protection law in some countries, they are designed so that consumers can be confident that companies adhering to the guidelines will provide a fundamental level of protection for personal data that applies no matter where the consumer, company, or data is located. Other applicable legal standards will of course continue to provide added protection.

GBDE PERSONAL DATA PRIVACY PROTECTION GUIDELINES

1. DEFINITIONS

For the purpose of these Guidelines;

- 1.1 “Company” means any company which is to use these Guidelines or to which these Guidelines are recommended.
- 1.2 “Consumer” is any natural person who acts in his or her individual capacity for purposes outside his or her trade, business or profession and who is a customer or potential customer of a Company’s business.
- 1.3 “Personal Data” of any Consumer means any data collected online by the Company which can identify the Consumer or which, when easily combined with other available data, can identify the Consumer.
- 1.4 “Contact Point” means an organization, a department or employee of Company who is responsible for communications relating to the Consumer’s Personal Data.

2. GENERAL: FAIR COLLECTION AND USE

Protection and security of Personal Data are important. Personal Data supplied online by any Consumer needs to be collected, secured, processed and used fairly.

3. OTHER INFORMATION

A Company may gather and analyze certain data through a website (such as the Internet browser and operating system used, the domain name of an originating website, the number of visits, average time of visit, and accessed websites) which do not identify any specific Consumer and therefore are not Personal Data. The Company and its affiliates may use this data for purposes such as measuring the use of web sites or

improving the performance or contents of their online services. However, if this type of information is combined with other data in a way that ties the information to a specific Consumer, and otherwise falls within the definition of Personal Data, the Company will treat it in accordance with these Guidelines.

4. PURPOSE SPECIFICATION AND OPENNESS

Notice to Consumers

4.1 When collecting any Personal Data from a Consumer online, a Company will provide the Consumer with a reasonable notice of the purposes for collecting and using the Personal Data. The notice should be posted clearly and conspicuously (for example, on or linked from the home page), easy to find and understand, and available to the Consumer prior to or at the time when the Personal Data is collected.

4.2 A Company should provide enough information to allow Consumers to make informed decisions concerning the collection and the use of their Personal Data. At the same time, a Company should attempt to avoid providing unnecessarily lengthy disclosures that may cause confusion and discourage Consumers from expending the time and effort necessary to understand their choices. To that end, a Company should provide information needed to ensure that the collection and use of the Personal Data is fair. It should be the obligation of the Company to include the necessary information that Consumers may need in order to feel confident that their information will not be used in inappropriate or undesirable ways. Depending on the context and circumstances, the notice should include:

- (i) The identity of the Company that determines and controls the purposes and

the ways in which the processing of personal data is undertaken;

- (ii) The type of Personal Data that is collected;
- (iii) The purposes for which the Personal Data collected may be used;
- (iv) The types of third parties - if any - to which the Company discloses Personal Data;
- (v) The choices and means the Company offers Consumers for limiting use and disclosure of Personal Data;
- (vi) Whether the Consumer has the option of not providing the requested Personal Data and the consequences of not providing it;
- (vii) Whether the collection of Personal Data is optional or required (e.g., for purposes of performing the transaction or for enabling the fulfillment of a service offered by a particular website);
- (viii) What kinds of technologies or information-gathering techniques, such as cookies, are used;
- (ix) What to do if the Consumer wants to correct or review the Personal Data collected;
- (x) The procedure for communicating with the company, including a physical and electronic mailing address to which the Consumer can direct questions, express preferences concerning the handling of Personal Data, or lodge complaints.

4.3 A company should have an easily-accessible system in place to handle any Personal Data complaints that a Consumer may address to the company.

- (i) As a first and preferred remedy in any dispute over use of Personal Data,

Consumers should be offered access to an internal complaints handling process.

- (ii) A Company should also consider the use of third party alternative dispute resolution systems (ADR) when a Personal Data complaint cannot be resolved in direct negotiations between the Company and the Consumer.

5. PURPOSE LIMITATION AND USE OF PERSONAL DATA

5.1 A Company will collect, use or disclose Personal Data supplied by a Consumer online only for the purposes disclosed to the Consumer, unless the disclosure:

- (i) is a use of the Personal Data for any additional purpose that is directly related to the original purpose for which the data was collected,
- (ii) is necessary for the performance of a contract to which the Consumer is a party or in order to take steps at the request of the Consumer prior to entering into a contract;
- (iii) is required by law, including cases where the life or health of the consumer is being threatened;
- (iv) is necessary to establish or preserve a legal claim or defense;
- (v) is necessary to prevent fraud or other illegal activities, such as willful attacks on security systems of the Company.

5.2 Obtaining Consent

A Company that plans to use a Consumer's Personal Data for another purpose not disclosed at the time of its collection should provide the Consumer with a reasonable and timely notice and a clear and conspicuous opportunity to opt out of the new use and any related disclosure prior to the time of such use or disclosure.

6. SPECIAL CATEGORIES OF SENSITIVE DATA

6.1 Sensitive data

If a Company wishes to collect or use sensitive Personal Data of a Consumer, such as medical records, racial or ethnic origin, political views, religious beliefs, sexual orientation or other matters of a highly personal nature, it is expected for the Company to provide the Consumer with a reasonable notice and to obtain the Consumer's unambiguous consent to the proposed collection or use. In deciding what Personal Data should be treated as sensitive, the Company should take into account applicable law as well as national and regional concerns about particular kinds of Personal Data.

6.2 Children

A Company will not knowingly collect Personal Data from children without insisting that they seek prior parental consent. In addition to other provisions set out in these Guidelines, the use or disclosure of Personal Data collected from children shall be subject to the opportunity for the child's parent or guardian to opt out from such use or disclosure at any time prior to the first disclosure; except that Personal Data about the child may be used or disclosed for the purposes of seeking parental consent pursuant to local laws or regulations, to protect the safety of a child, or to respond to a request from law enforcement.

The Company's definition of "child" for purposes of this paragraph should take into account applicable law as well as national and regional cultural norms.

7. DISCLOSURE OF PERSONAL DATA

Transfer of Personal Data to agents, affiliates and third parties

7.1 Mere processing

When transferring Personal Data to a third party for the sole purpose of processing – that is, for the collecting Company’s benefit and not for the further use of the party performing the processing function (processing on behalf of the collecting Company), the Company should ensure that the processing party handles the Personal Data in a manner consistent with the terms of the collecting Company’s data privacy protection notice made available to the Consumer.

7.2 Third Parties

If the Company intends to disclose Personal Data to third parties (including new third parties created by any divestiture of the company) who want to offer other services or products to the Consumer, or for other direct marketing purposes, the Company should provide the Consumer with an opportunity to opt out from such disclosure at the time of the collection of the Personal Data or no later than at the time of the first disclosure.

7.3 Affiliates

In case of transfer or disclosure of personal data to corporate affiliates, the collecting Company should ensure that the affiliate handles Personal Data in conformity with Section 5 above and in a manner consistent with the Company’s data privacy protection notice made available to Consumers.

7.4 Acquisitions

In case the collecting Company is acquired by a third party, the Company should ensure that the acquiring Company grants the Consumers of the acquired Company at least the same level of Data Protection offered by the acquired Company at the time of the acquisition, except where the acquiring and/or acquired Company provides the Consumer with an opportunity to opt out from new uses of that data not disclosed by the acquired Company (as described in Section 5.2).

8. SECURITY SAFEGUARDS

A Company should take reasonable measures to protect Personal Data collected from a consumer online against loss, manipulation, falsification, unauthorized access or unauthorized disclosure by any party inside or outside the Company.

9. ENSURING THE QUALITY AND INTEGRITY OF PERSONAL DATA

When a Company collects and retains Personal Data from a Consumer online, the Company should respond to reasonable Consumer requests to review that information and correct, amend or delete any inaccuracies.

10. INDIVIDUAL PARTICIPATION

A Company should observe procedures designed to respond to Consumers’ requests. Should a Company be unable to respond to requests, either because the information is not maintained in retrievable form, or retrieval is not reasonably cost-effective, the Company should provide:

- (i) an explanation of why retrieval cannot be effectuated; and
- (ii) a Contact Point for further information.

11. LINKS TO OTHER WEBSITES

A Company’s web sites or other interactive services may contain links to information provided by third parties. The company should disclose to Consumers that it is not responsible for the Personal Data protection policies or practices of linked sites.

12. ACCOUNTABILITY

The Company will establish and maintain policies concerning the collection, use and disclosure of Personal Data together with a system to implement these policies within the company.