

# **Privacy Guidelines for Developing Software Products and Services**

Version 3.1

*September, 2008*

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to patents, trademarks, copyrights, or other intellectual property.

© 2006 Microsoft Corporation. All rights reserved.

Microsoft, SharePoint, SQL Server, Windows, Windows Media, Windows Server, and Xbox are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Please direct all comments and inquiries to <http://go.microsoft.com/?linkid=5622337>.

### **Acknowledgements:**

These guidelines are based on Microsoft's internal best practices that have been under development since 2003. In 2005, privacy best practices were integrated into the Security Development Lifecycle (SDL) and deployed company wide. Compiling and advancing these guidelines has been a labor of love for many. This document has been compiled in several stages, with passionate and crucial contributions from Jeffrey Friedberg, Sue Glueck, Tina Knutson, JC Cannon, Bill Colburn, Rob Roberts, Colin Birge, Diane McDade, Kim Howell, Lyn Watts, Nicholas Judge, David Eitelbach, Mike Hintze, Susan Koeppen, Brendon Lynch, Maithili Dandige, and Tom Donahoe. We thank the members of the Microsoft Privacy Cabinet for Development, the Microsoft Privacy Management Committee, and the Trustworthy Computing Academic Advisory Board for their assistance in editing the document. We would also like to extend a special acknowledgement to Peter Cullen for continued Corporate Privacy Group sponsorship and Steve Lipner and Eric Bidstrup for their support integrating these practices into the SDL.

## Update History:

<b>Version</b>	<b>Date</b>	<b>High Level Description of Changes</b>
2.1	Sept., 2006	First publication of the Privacy Guidelines
2.1a	Apr., 2007	Update to the Acknowledgements
3.1	Sept., 2008	Added scenarios and definitions for Sharing and Collaboration features, new rules regarding collecting registration data and migrating privacy settings, and additional clarifications throughout.

# Table of Contents

Introduction .....	5
1 Basic Concepts and Definitions .....	6
1.1 User Data .....	6
1.1.1 User Data Categories .....	6
1.2 Data Minimization and Data Management .....	9
1.2.1 Minimizing Data Collected .....	10
1.2.2 Limiting Access to “Need to Know” .....	10
1.2.3 Reducing the Sensitivity of Data Retained .....	10
1.2.4 Reducing Duration of Data Retention .....	11
1.3 Notice, Choice, and Consent .....	11
1.3.1 Types of Notice .....	11
1.3.2 Types of Consent .....	14
1.4 Notice Mechanisms .....	18
1.4.1 Just-in-Time Notice .....	18
1.4.2 First Run Notice .....	18
1.4.3 Installation Time Notice .....	18
1.4.4 "Out of the Box" Notice .....	19
1.5 Security .....	19
1.6 Access .....	19
1.7 Data Integrity .....	19
1.8 Types of Privacy Controls .....	20
1.8.1 User Controls .....	20
1.8.2 Administrator Privacy Controls .....	21
1.9 Shared Computers .....	21
1.10 Children’s Privacy .....	22
1.11 Software Installation .....	22
1.12 Server Products .....	23
Third Parties .....	23
1.13 Web Sites and Web Services .....	23
1.13.1 Using P3P for Privacy Statements .....	24
1.13.2 Using Cookies .....	24
1.14 Special Considerations .....	24
1.14.1 Pre-Release Products .....	24
1.14.2 Essential Transfers and Updates .....	24
1.14.3 File and Path Names .....	25
1.14.4 IP Address .....	25
1.14.5 When Things Change .....	25
2 Guidelines .....	26
2.1 How to Use This Section .....	26
2.2 Scenarios .....	27
Scenario 1: Transferring PII to and from the Customer’s System .....	28
Scenario 2: Storing PII on the Customer’s System .....	31
Scenario 3: Transferring Anonymous Data from the Customer’s System .....	33
Scenario 4: Installing Software on a Customer’s System .....	35
Scenario 5: Deploying a Web Site .....	37
Scenario 6: Storing and Processing User Data at the Company .....	39
Scenario 7: Transferring User Data outside the Company .....	41
Scenario 8: Interacting with Children .....	43
Scenario 9: Server Deployment .....	45
Appendix A .....	47
Appendix B .....	48
Appendix C .....	51

## Introduction

Protecting customer privacy is critically important. In many areas of the world, privacy is considered a fundamental human right.<sup>1</sup> Additionally, protecting customer privacy can increase loyalty and be a market differentiator.

Customers are getting increasingly frustrated with software and Web sites that do not clearly communicate the behaviors that impact customer privacy and the controls available to them.<sup>2</sup> Currently, there are no industry-wide practices to help standardize the user experience and the software development process. For some, ignoring this growing frustration has led to an erosion of trust, negative press, and even litigation.

The software industry as a whole would benefit from establishing a higher bar for respecting customer privacy. Giving customers more information about how their privacy may be impacted (i.e. transparency) coupled with improved controls can empower customers and raise their level of trust. At the same time, it is important not to annoy customers with a barrage of notices that ultimately may be ignored.

The purpose of this document is to propose a baseline for establishing this higher bar. It offers guidance for creating notice and consent experiences, providing sufficient data security, maintaining data integrity, offering customer access, and supplying controls when developing software products and Web sites. These guidelines are based on the core concepts of the Organisation for Economic Co-operation and Development (OECD) Fair Information Practices and privacy laws such as the EU Data Protection Directive, the U.S. Children's Online Privacy Protection Act of 1998 (COPPA), and the U.S. Computer Fraud and Abuse Act (as amended 1994 and 1996). In the interest of developing a common set of industry best practices for privacy, we invite the community and other interested parties to participate in an open dialogue.

This document is only a starting point; there are other important topics that are not yet addressed such as adware<sup>3</sup> and location based services<sup>4</sup>. With the help of industry and subject matter experts, improvements and additional topics can be incorporated over time.

For several years, several groups within Microsoft® have been following guidelines similar to those contained in this document.<sup>5</sup> Recognizing that respecting customer privacy is essential, Microsoft's guidelines have been incorporated into the [Security Development Lifecycle \(SDL\)](#)<sup>6</sup> and deployed company-wide.

---

<sup>1</sup> Per the EU Data Protection Directive (95/46/EC): "data processing systems... must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy...."

<sup>2</sup> <http://www.epic.org/privacy/survey/>

<sup>3</sup> As defined by the Anti-Spyware Coalition:

<http://www.antispywarecoalition.org/documents/documents/ASCDefinitionsWorkingReport20060622.pdf>

<sup>4</sup> For more information on location based services see:

[http://www.truste.org/pdf/TRUSTe\\_Wireless\\_Privacy\\_Principles.pdf](http://www.truste.org/pdf/TRUSTe_Wireless_Privacy_Principles.pdf)

<sup>5</sup> Microsoft's internal privacy guidelines cover areas that are not included in this document such as marketing campaigns and e-mail best practices.

<sup>6</sup> See also Howard, Michael and Steve Lipner, [The Security Development Lifecycle](#), Microsoft Press, Redmond, Washington, 2006

This document is divided into two main sections. Section 1 provides an introduction to key privacy concepts and definitions. Section 2 enumerates detailed guidelines for specific software product and Web site development scenarios.

## 1 Basic Concepts and Definitions

The core principle driving these guidelines is:

*Customers will be empowered to control the collection, use, and distribution of their personal information.*

For customers to have control over their personal information, they need to know what personal information will be collected, with whom it will be shared, and how it will be used. In addition:

- Customers must provide consent before any personal information is transferred from their computer.
- If a customer's personal information is transferred over the Internet and stored remotely, they must be offered a mechanism for accessing and updating the information.

Before collecting and transferring personal information, you, as the entity requesting the information, must have a compelling business *and* customer value proposition. A value proposition that benefits customers may create a natural incentive for them to entrust you with their personal information. Only collect personal information if you can clearly explain the net benefit to the customer. If you are hesitant to tell customers “up front” what you plan to do with their information, *then do not collect their data*. This applies to data collected and stored locally on the customer's machine or transferred over the Internet.

Not all information collected from a customer is personal. The sections that follow define the different types of data referenced in this document.

### 1.1 User Data

“User Data” is defined as:

- (a) Any data that is collected directly from a customer (e.g., entered by the customer via an application's user interface)
- (b) Any data about a customer that is gathered indirectly (e.g., metadata in documents)
- (c) Any data about a customer's usage behavior (e.g., logs or history)
- (d) Any data relating to a customer's system (e.g., system configuration, IP address)

Different privacy practices are required depending on the nature of the User Data and the uses for which such data is collected. For example, User Data transferred from a customer's system requires different levels of notice and consent depending on the category of User Data collected.

#### 1.1.1 User Data Categories

User Data falls into the following two main categories:

- Anonymous Data
- Personally Identifiable Information (PII), which includes Sensitive PII

#### 1.1.1.1 Anonymous Data

Anonymous Data is non-personal data which, by itself, has no intrinsic link to an individual customer. For example, hair color or height (in the absence of other correlating information) does not identify a customer. Similarly, system information such as hardware configuration (e.g., CPU and memory size) is anonymous when it is not tied to an individual. If a unique identifier is introduced that ties the data to an individual, the data is no longer anonymous.

Data can also lose its anonymity as the volume of data collected increases. The more information that is known, the greater the chance a link to an individual can be made, especially in situations where there is a small population of possible candidates. For example, a report that listed average salary by group could expose an individual's salary if they were the only person in that group.

#### 1.1.1.2 Pseudonymous Data

Pseudonymous Data is unique information that by itself does not identify a specific person (e.g., unique identifiers, biometric information, and usage profiles that are not tied to an individual), but could be associated with an individual. Once this data is associated with an individual it must be treated as personal information. Until that time, it may be treated as anonymous.

For example, Web sites can be configured to track unique visitors. This is typically done using a unique identifier stored in a cookie. To the extent that the service does not associate this data with an individual, it may treat the data collected as anonymous. If the service connects the identifier with a customer, the data collected must be treated as personal information.

Note that if the data alone can be tied to an individual, it should be treated as personal information. For example, when the search history of an individual provides clues to the individual's identity, the data should be treated as personal information.

#### 1.1.1.3 Personally Identifiable Information

The definition of PII used in these guidelines is based on TRUSTe's<sup>7</sup> definition:

**Personally Identifiable Information** means any information... (i) that identifies or can be used to identify, contact, or locate the person to whom such information pertains, or (ii) from which identification or contact information of an individual person can be derived. Personally Identifiable Information includes, but is not limited to: name, address, phone number, fax number, e-mail address, financial profiles, medical profile, social security number, and credit card information.

---

<sup>7</sup> TRUSTe is an independent trust authority. See <http://www.truste.org>.

Additionally, to the extent unique information (which by itself is not Personally Identifiable Information)... is associated with Personally Identifiable Information, then such unique information will also be considered Personally Identifiable Information.

Personally Identifiable Information does not include information that is collected anonymously (i.e., without identification of the individual user) or demographic information not connected to an identified individual.<sup>8</sup>

Some PII can become anonymous if it is aggregated and stripped of its connection to an individual. Conversely, Anonymous Data can become PII when it is commingled with personal information.

#### **1.1.1.4 Sensitive Personally Identifiable Information**

Sensitive Personally Identifiable Information (Sensitive PII) is a subset of PII considered to be so important to the individual that it must be specially protected. For example, credit card numbers and bank account information are categorized as Sensitive PII because they could be misused, resulting in significant financial harm. The same can be true of government-issued identifiers such as Social Security Numbers and drivers' license numbers.

Included in this category is any data that could (i) be used to discriminate (e.g., race, ethnic origin, religious or philosophical beliefs, political opinions, trade union memberships, sexual lifestyle, physical or mental health), (ii) facilitate identity theft (e.g., mother's maiden name), or (iii) permit access to a customer's account (e.g., passwords or PINs). Note that if the data described in this paragraph is not commingled with PII during storage or transfer, and it is not correlated with PII, then the data can be treated as Anonymous Data. If there is any doubt, however, the data should be treated as Sensitive PII.

User Data that historically has made customers nervous (such as a customer's real-time location<sup>9</sup>), while not technically Sensitive PII, should be treated as Sensitive PII. Company approval is required prior to the collection, storage, or transfer of a user's real-time location data. Also, data that has a reasonable expectation of embarrassing the user should also be treated as Sensitive PII. Determining what sort of information may be embarrassing can vary by culture, and may be difficult to define. If there is any doubt, the data should be treated as Sensitive PII.

The transfer of Sensitive PII should be avoided unless it is necessary to provide a service that the individual has requested, or unless it is required by law. Storing Sensitive PII on the customer's system should also be avoided when not absolutely necessary.<sup>10</sup> When it is necessary to store Sensitive PII on the customer's system, the customer must provide consent, and the data should be stored only for the shortest amount of time necessary to achieve the specific business purpose. Sensitive PII must be stored with the appropriate safeguards and mechanisms to prevent unauthorized access.

---

<sup>8</sup> See [http://www.truste.org/docs/Web\\_Seal\\_Self\\_Assessment\\_Form.doc](http://www.truste.org/docs/Web_Seal_Self_Assessment_Form.doc).

<sup>9</sup> For additional guidelines regarding location see the TRUSTe wireless/location services whitepaper at [http://www.truste.org/pdf/TRUSTe\\_Wireless\\_Privacy\\_Principles.pdf](http://www.truste.org/pdf/TRUSTe_Wireless_Privacy_Principles.pdf).

<sup>10</sup> Note that this does not apply to unsolicited Sensitive PII (e.g., the customer enters Sensitive PII in a word processing document). See section on [Unsolicited PII](#).

### **1.1.1.5 Hidden PII**

Hidden PII is PII stored with a file that is not typically visible to the customer. Examples of Hidden PII include the author's name stored as metadata in the Properties of a Microsoft Office document, comments or tracked changes stored as metadata in a Microsoft Office document, and PII stored in a cookie. Hidden PII may include information that the customer might not want to distribute publicly. If PII is stored in a hidden way, the customer must be made aware that Hidden PII exists and should be given appropriate control over sharing it.

### **1.1.1.6 Unsolicited PII**

Unsolicited PII is PII provided by the customer when none has been requested. Examples of Unsolicited PII include PII entered as search terms and in text fields of a Web form.

Minimize the entry of Unsolicited PII by using fields with predefined entries (e.g., list boxes and drop-down lists) wherever possible. When a text field is necessary, the User Interface (UI) should discourage the customer from entering PII.<sup>11</sup>

Whether Unsolicited PII is treated as PII depends on the context. If a customer enters PII into a field that warns against doing so, it is reasonable to treat the information as though it were Anonymous Data. When there is a likelihood that the data could identify the customer, it should be treated as PII. For example, a collection of search terms tied to a unique identifier could say a great deal about an individual's behavior and could include enough information to identify the individual so it should be treated as PII.

## **1.2 Data Minimization and Data Management**

One of the best ways to protect a customer's privacy is to not collect his or her User Data in the first place. The questions that should constantly be asked by architects, developers, and administrators of data collection systems include:

- "Do I need to collect this data?"
- "Do I have a valid business purpose?"
- "Will customers support my business purpose?"

The answers must explicitly address both the primary use of the customer's data (such as providing the feature or service the customer is requesting) and any planned secondary use (such as marketing analysis). Only collect data for which there is an immediate planned use. In addition, only transfer data that is absolutely necessary to achieve the business purpose, reduce the sensitivity of the data retained (e.g., aggregate data where possible), and delete data that is no longer needed for the business purpose.

Another important area to consider is how customers will react to the collection of their data. For example, while one customer may appreciate product recommendations derived from his or her purchase history, another may see such personalization as an invasion of his or her privacy.

The subsections that follow look at key characteristics of data minimization.

---

<sup>11</sup> Additional obligations may come into play when the customer submitting the unsolicited PII is a child. See [Interacting with Children](#).

### **1.2.1 Minimizing Data Collected**

When collecting PII from the customer, require only the data needed to provide the feature or service or complete the transaction. Additional data may be requested if it is clear to the customer that providing it is optional and there is a sound business purpose for collecting it. With a compelling value proposition, customers may be willing to provide the optional data. For example, while an e-mail address is required to deliver a newsletter, optionally requesting the subscriber’s postal code could enable personalization of the newsletter content. Also, the least sensitive form of data that fulfills the business purpose should be collected. For example, to deliver an annual birthday greeting and coupon, collect only birth month and day, not year<sup>12</sup>.

### **1.2.2 Limiting Access to “Need to Know”**

Employee access to User Data should be limited to those who have a legitimate business purpose for accessing the data. In addition, those employees should only be given access to the smallest amount of User Data needed to achieve the specific business purpose.

These concepts not only apply to employees, but also to third parties (i.e. company agents and independent third parties) to whom the data is transferred. Third parties should only be given the specific data they need to fulfill their business purpose. Before a company provides PII to a third party, they must enter into a contract that contains adequate data-protection provisions, including retention and destruction requirements. If Sensitive PII is involved, consider including procedures to be followed in the event that the third party experiences a breach.

Notice should be provided to employees and company agents accessing PII that informs them of their obligations around agreed use of the data. Access must be revoked if access to the data is no longer required as part of the employee’s or agent’s job function.

### **1.2.3 Reducing the Sensitivity of Data Retained**

The risk of data exposure can be further minimized by reducing the sensitivity of stored data wherever possible. One approach is to reduce the precision of the data retained after it has been collected. For example, if a customer phone number is to be used for statistical analysis, only a subset of the digits should be retained, such as the area code.

Another approach is to convert User Data to a less sensitive form. For example, when using the customer’s IP address to determine location for statistical analysis, discard the IP address after mapping it to a city or town. Another example is performing a one-way hash<sup>13</sup> of a unique identifier to reduce the ability to correlate the identifier with the customer or the customer’s system.

When data becomes less sensitive, security requirements for storing and transferring the data may be reduced (e.g., transferring Anonymous Data to a third party requires fewer security controls).

---

<sup>12</sup> In some cases, collecting year may be required, such as when the service providing the greeting is targeted at or attractive to children. See Scenario 9 for more information.

<sup>13</sup> A one-way hash converts text into a string of digits that is nearly impossible to convert back to the original text.

### **1.2.4 Reducing Duration of Data Retention**

The longer data is retained, the higher the likelihood of accidental disclosure, data theft, and/or data growing stale. User Data should be retained for the minimum amount of time necessary to support the business purpose or to meet legal requirements. Any User Data stored by a company should have a retention policy that states how long the data should be kept and the manner in which it should be removed from all data stores.

User Data stored on the customer's machine may be retained for an indefinite period. However, the customer should be able to view and remove PII. If the data stored is system configuration information that impacts the customer's privacy, it should be disclosed and the customer should be able to delete it. While most system configuration information does not impact the customer's privacy (e.g., system memory and operating system version), there are some types of information that may disclose the customer's personal behavior (e.g., event logs of applications used during a specific time period).

## **1.3 Notice, Choice, and Consent<sup>14</sup>**

All products and services that collect User Data and transfer it must provide an explanation (“give notice”) to the customer. The customer must be presented with a choice of whether to provide the information, and consent must be obtained from the customer before PII can be transferred from the customer's system. The type of notice and consent required depends on the type of User Data being collected and how it will be used.

### **1.3.1 Types of Notice**

What is included in a privacy notice depends on the feature and context, including what type of information is being collected or shared. This section describes two types of notice: prominent and discoverable. Regardless of type, all notices should be written in clear, easy-to-read language. See [Section 2](#) for guidelines governing which type of notice to use in various scenarios.

#### **1.3.1.1 Prominent Notice**

A “Prominent Notice” is one that is designed to catch the customer's attention. An example of a Prominent Notice is the privacy options page displayed the first time a customer runs Microsoft Windows Media® Player 10. This page invites customers to inspect the current privacy settings, learn more about their options, and make choices (see [Appendix A](#) for an illustration of this experience).

A Prominent Notice should contain a high-level, substantive summary of the privacy-impacting aspects of the feature such as the data being collected and how that data will be used. The summary ideally should be fully visible without additional action on the part of the customer, such as having to scroll down the page. A Prominent Notice should also include clear instructions for where the customer can get additional information (e.g., a link to the privacy statement). For example, the Windows® Error Reporting experience in Windows XP provides a summary and a link to examine what will be sent in more detail:

---

<sup>14</sup> Much of the terminology used herein is consistent with the AICPA's [Generally Accepted Privacy Principles](#).



A fill-in-the-blank form that collects personal information can be a Prominent Notice if the form clearly communicates how the personal information will be used. For example, the graphic below identifies required fields, informs the customer of how the information will be used, and offers a link to a more complete explanation:

## Contact Information

Sorry, you didn't win. However, if you fill out the following form, you will still be entered to win in the grand prize drawing.

Don't worry! We'll only use this information to contact you if you win, and won't share it with anyone or use it for anything else. [Learn more](#)

\* = Required

**First name:** \*

**Last name:** \*

**Address line 1:**

**Address line 2:**

**City:**

**State:**

**Zip:**

**Phone:**

**Email:** \*

### 1.3.1.2 Discoverable Notice

A “Discoverable Notice” is one the customer has to find (e.g., by locating and reading a privacy statement of a Web site or by selecting a privacy statement link from a Help menu in a software product). Discoverable Notices typically disclose:

- The type of data being stored
- How it will be used
- How it is protected
- With whom it will be shared
- Available user controls
- How the customer can update the information (if PII will be stored by the company for subsequent use)
- Company contact information

In some scenarios, a Discoverable Notice is all that is required (e.g., visiting a Web site page). In other cases it is used to provide additional information that may not fit in the user experience of a Prominent Notice. The customer should be able to print a Discoverable Notice. Certifying privacy statements with an independent privacy certification organization, such as TRUSTe, should be considered.

#### 1.3.1.2.1 Layered Notice

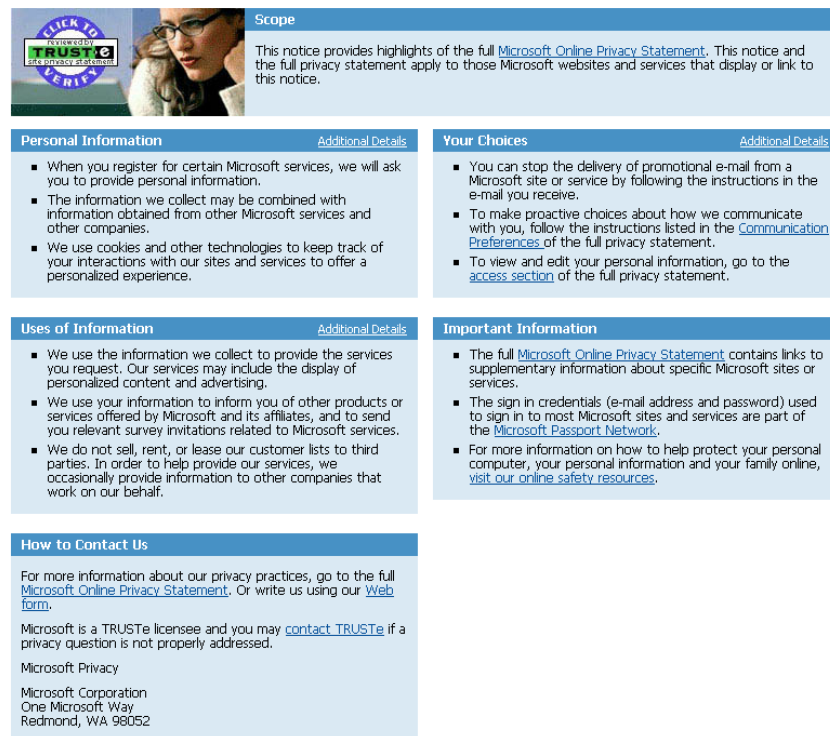
A “Layered Notice” can make it easier for the customer to understand a complex privacy statement. A layered notice typically includes a single-page summary of the privacy statement (that can be read without scrolling) divided into specific sections (e.g., “Personal Information,” “Uses of Information,” and “Your Choices”). The summary page includes links to more detail (i.e. specific sections within the full privacy statement). Layered Notices are a recommended practice for Web sites and products with complex, lengthy privacy statements. An example of a Layered Notice is the Microsoft Online Privacy Statement:<sup>15</sup>

---

<sup>15</sup> Other examples include the [Privacy Statement for the 2007 Microsoft Office system Pre-Release \(Beta\)](#), the [Windows Vista Pre-Release \(Beta 2\) Privacy Statement](#), and [IBM Privacy Practices on the Web](#).

## Microsoft Online Privacy Notice Highlights

(last updated January 2006)



**Scope**

This notice provides highlights of the full [Microsoft Online Privacy Statement](#). This notice and the full privacy statement apply to those Microsoft websites and services that display or link to this notice.

**Personal Information** [Additional Details](#)

- When you register for certain Microsoft services, we will ask you to provide personal information.
- The information we collect may be combined with information obtained from other Microsoft services and other companies.
- We use cookies and other technologies to keep track of your interactions with our sites and services to offer a personalized experience.

**Your Choices** [Additional Details](#)

- You can stop the delivery of promotional e-mail from a Microsoft site or service by following the instructions in the e-mail you receive.
- To make proactive choices about how we communicate with you, follow the instructions listed in the [Communication Preferences](#) of the full privacy statement.
- To view and edit your personal information, go to the [access section](#) of the full privacy statement.

**Uses of Information** [Additional Details](#)

- We use the information we collect to provide the services you request. Our services may include the display of personalized content and advertising.
- We use your information to inform you of other products or services offered by Microsoft and its affiliates, and to send you relevant survey invitations related to Microsoft services.
- We do not sell, rent, or lease our customer lists to third parties. In order to help provide our services, we occasionally provide information to other companies that work on our behalf.

**Important Information**

- The full [Microsoft Online Privacy Statement](#) contains links to supplementary information about specific Microsoft sites or services.
- The sign in credentials (e-mail address and password) used to sign in to most Microsoft sites and services are part of the [Microsoft Passport Network](#).
- For more information on how to help protect your personal computer, your personal information and your family online, [visit our online safety resources](#).

**How to Contact Us**

For more information about our privacy practices, go to the full [Microsoft Online Privacy Statement](#). Or write us using our [Web form](#).

Microsoft is a TRUSTe licensee and you may [contact TRUSTe](#) if a privacy question is not properly addressed.

Microsoft Privacy  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052

© 2006 Microsoft Corporation. All rights reserved. [Anti-Spam Policy](#)

### 1.3.2 Types of Consent

Consent can be obtained from a customer through a number of different methods including a UI presented by the application or Web site, a dialog presented by the setup tool that installs the application, or an agreement that the customer accepts prior to running the application. The following sections explain various types of consent. See [Section 2](#) for guidelines governing which consent mechanism to use in various scenarios.

#### 1.3.2.1 Explicit Consent

"Explicit Consent" requires the customer to take or have the ability to take an explicit action before data is collected or transferred. Explicit Consent is necessary if PII will be transferred or Anonymous Data will be continuously collected and transferred. A separate Explicit Consent experience is also necessary if PII being transferred will be used for secondary purposes such as marketing.

There are two styles of Explicit Consent: Opt-In and Opt-Out, which are illustrated below.

##### 1.3.2.1.1 Opt-In Explicit Consent

An Explicit Consent experience that is Opt-In means that the proposition presented will only occur after the customer takes an action. When Opt-In Explicit Consent is needed, consider making "no selection" the default and disabling the "Submit" or "Next" button until the customer

takes an action on the page. Requiring the customer to make a choice acts as a “speed bump,” and helps ensure the customer makes a conscious decision.

*Checkboxes:* If you are presenting an option with a checkbox, the Opt-In style of Explicit Consent requires the customer to actively check the box with text containing the privacy choice in order to enable the data collection, use, or transfer (i.e. the checkbox cannot be pre-checked). For example:

- I want to help make Microsoft products and services even better by sending Player usage data to Microsoft.**

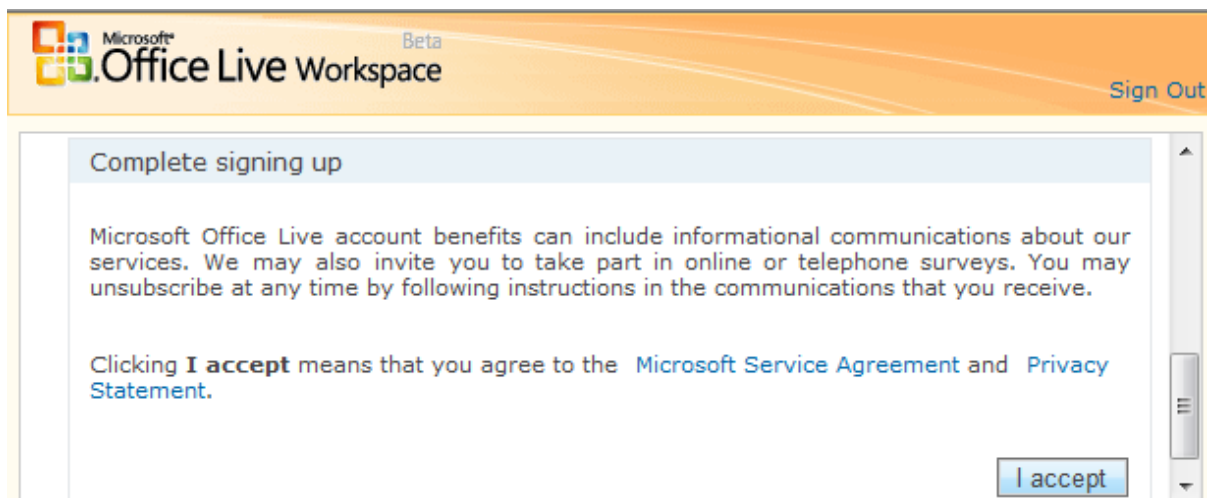
*Radio Buttons:* Alternatively, if you are providing multiple choices to the customer, Opt-In Explicit Consent requires the customer to select an option that wasn’t selected by default:

- Yes, I want to send my data to Microsoft.**
- No thank you.**

Not selecting any radio buttons by default (i.e. requiring the customer to actively select Yes or No) also fulfills the Opt-In Explicit Consent requirement.

*Labeled Buttons:* Another Explicit Consent mechanism is a button with a description that makes clear what the choice represents.

A “Submit” button on a Web form that collects PII is Opt-In Explicit Consent for primary use of the data submitted. For example, if a customer is buying a product from a Web site, clicking a “Submit” button after filling in the mailing address would constitute the customer’s consent to have the product shipped to that address. However, depending on the country/region, a ‘Submit’ button on a Web form may not be sufficient consent for some secondary uses, such as e-mail or SMS marketing.



*Next Button in a Wizard:* As mentioned above, consider disabling the “Next” button until the customer takes an action on the page.



Ideally, Opt-In Explicit Consent should be obtained in the UI. In some cases, this is not possible, such as when the feature or service does not have a UI. In these cases, or when collection and transfer of Anonymous Data is essential to the functioning of the product or service, consent can be obtained in the license agreement or terms of use.

When sensitive information is transferred and then retained for the customer’s future use (e.g., credit card information stored for quick check-out), a separate Opt-In Explicit Consent experience is necessary.

### 1.3.2.1.2 Opt-Out Explicit Consent

An Explicit Consent experience that is Opt-Out means that the proposition presented will occur if the customer does not take an action.

*Checkboxes:* If you are using the Opt-Out style of Explicit Consent, the checkbox that enables data collection or transfer would be pre-checked. For example:

**Please send me the latest information on special offers of Xbox® games.**

The checked box indicates that this is an Opt-Out choice. If the customer does not un-check the box, promotional offers will be sent.

*Radio Buttons:* Radio buttons can be used in a manner similar to check-boxes for Opt-Out Explicit Consent. For example:

- **Yes, I want to send my data to Microsoft.**
- **No thank you.**

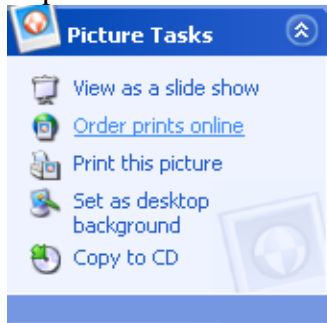
If the customer does not change the selection to “No thank you,” data will be sent.

### 1.3.2.2 Implicit Consent

“Implicit Consent” for sending User Data over the Internet does not require an explicit action indicating consent from the customer; the consent is implicit in the operation the customer initiates. The online nature of the operation can be implied in the branding of the product or service (e.g., Microsoft Office Online), the text of the link or button (e.g., Get Online Help), or where it is reasonable to expect that the customer will recognize that the action is online.

Examples include:

*Labeled Links:* A link that makes it clear that the customer will be sending information over the Internet or browsing to an Internet site (e.g., a link entitled "Order prints online") constitutes Implicit Consent:



*Entering URLs in a browser:* When a customer types a URL in the address bar of the browser, the customer has implicitly consented to sending that information as well as standard header information over the Internet.

*Entering information where the customer may not be aware he or she is in a browser window:* When a customer obtains information or types in a pane without any browser UI (e.g., a Help window), customer consent can only be implied if the customer realizes from the context that he or she is browsing the Web (e.g., for Online Help).

*Sending E-mail:* When a customer sends an e-mail, that customer has implicitly consented to sending the mail and standard header information over the Internet.

*Web sites:* Visiting pages on a Web site implicitly means the customer consents to the site’s privacy statement and terms of use.

## **1.4 Notice Mechanisms**

In designing notice for customers, consider the most appropriate moment to provide the notice. A “Just-in-Time” design would explain the collection and use of User Data just prior to the moment when data was to be collected or shared. A “First Run” design would provide this explanation and the associated choices the first time the customer runs your product or service. An “Installation” design would provide privacy information and choices during the installation of your product. An “Out of the Box” design would provide an initial notice for preinstalled software. It may be appropriate for components to use a combination of notices.

Striking a balance between informing the user and annoying the user can be difficult. Informing the user is critical, but providing too many notices may cause the user to ignore important messages. The goal is to provide the appropriate level of notice so that the user remains engaged and is able to make informed decisions. Usability tests can help teams structure key aspects of the user experience to strike this balance.

### **1.4.1 Just-in-Time Notice**

As referenced above, a “Just-in-Time” notice occurs just prior to the moment when data could be collected or shared. The control choices are typically more meaningful to the customer for an operation that is about to occur. Windows Error Reporting is an example of a component that provides Just-in-Time notice. It gives each customer a chance to examine the actual data that would be transferred, thus giving the customer more context to make his or her decision.

The advantage of Just-In-Time Notice has to be balanced against the potential annoyance of displaying privacy notices too often. Also, some customers may prefer to make their privacy decisions prior to installing a product or accepting the terms of a service.

### **1.4.2 First Run Notice**

As noted, a “First Run” notice occurs the first time each user on a customer’s system runs a program after it has been installed. A First Run experience provides an opportunity to explain the key privacy issues and choices offered by a product. These choices are unique to each user so they can make independent choices. For an example of this approach, see the Windows Media Player 10 experience in [Appendix A](#).

A potential disadvantage of a First Run notice is that the customer has not yet used the product and may not understand its features well enough to properly evaluate the privacy choices. Any disadvantage may be offset by providing a combination of First Run and Just-in-Time notices within the product.

### **1.4.3 Installation Time Notice**

The installation of a product offers another opportunity for notice and choice. If the application is installed on a per-user basis, the experience is similar to First Run. However, if the application is installed by an administrator for all users, the notice and choice experience will only be seen by the person installing the product. The advantage of this approach is administrator control. A potential disadvantage is that subsequent users may not realize what was set or have the ability to customize the experience.

#### **1.4.4 "Out of the Box" Notice**

When software is pre-installed, another way to provide notice and choice is during the initial "Out of the Box" or "setup" experience (e.g., when the system is first powered on by a customer). Note that presenting multiple consent experiences during setup might annoy a customer who is eager to start using the product. Consider limiting these experiences to critical features that require customer consent (e.g., when some versions of Windows are launched for the first time, customers are offered the opportunity to turn on automatic updating). An "Out of the Box" experience can be the equivalent of First Run for the administrator, with the administrator configuring the privacy choices for all subsequent users. Alternatively, it can be combined with a First Run experience for all users, where the administrator selects defaults, but each subsequent user is given the opportunity to change his or her settings.

### **1.5 Security**

Security is an essential element of privacy. Reasonable steps should be taken to protect PII from loss, misuse, unauthorized access, disclosure, alteration, and destruction. Preventive measures include access controls, encryption in transfer and storage, physical security, disaster recovery, and auditing. Security requirements vary depending on the type of User Data collected and whether it will be stored locally, transferred, and/or stored remotely. When storing Sensitive PII on a customer's system, it must be stored using appropriate security mechanisms to prevent unauthorized access (e.g., file permissions and encryption). Sensitive PII transferred to or from a customer's system over the Internet must be transferred using a secure method that prevents unauthorized access. In general, non-sensitive PII should also be transferred using a secure method, however, if the PII is a unique identifier fundamental to the routing (such as IP address or e-mail address), such protection may not be possible.

Contractual obligations may also come into play when sensitive data is collected, transferred, and stored. For example, when displaying account numbers, Visa and MasterCard require their partners to mask all but the first 6 and last 4 digits unless there is a specific and immediate need to see the full credit card number.<sup>16</sup> For more information see the security requirements in [Section 2](#) and [Appendix B](#).

### **1.6 Access**

Customers must be able to access and update PII that is stored remotely. When customer contact preferences are collected, customers must be able to view and update their preferences. Customers must be authenticated prior to accessing or modifying their PII or contact preferences. Where possible, real-time access should be provided at no cost.

### **1.7 Data Integrity**

Reasonable steps must be taken to ensure that PII is accurate, complete, and relevant for its intended use. Otherwise, there is a possibility that incomplete data will be collected which will impact the ability to provide the services or carry out the transaction requested by the customer. Detective and corrective processes should be in place to monitor and minimize inaccuracies through routine checks on systems that contain PII. Additionally, because PII may be stored in multiple systems and

---

<sup>16</sup> From the [Visa Payment Card Industry Security Audit Procedures](#).

databases, those systems must be designed to ensure that PII (including customer preferences) remains accurate when data is merged or replicated from one system to another.

Data validation controls should be used to avoid inconsistent, incomplete, or incorrect PII:

What is your primary role in your company or organization?  
Specialist/Professional

What is the total number of employees within your company or organization?  
25,000 - 49,999

Please Select from the Following Options

- 0
- 1
- 2 - 4
- 5 - 10
- 11 - 24
- 25 - 49
- 50 - 99
- 100 - 249
- 250 - 499
- 500 - 999
- 1,000 - 1,499
- 1,500 - 4,999
- 5,000 - 24,999
- 25,000 - 49,999
- 50,000 or more

## 1.8 Types of Privacy Controls

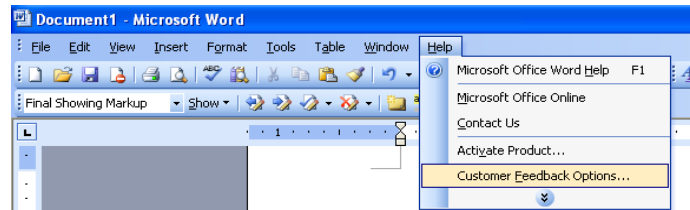
For customers to express their privacy preferences, in addition to consenting to data transfer and use, customers must also have the ability to later change their minds. In most cases, this is done by providing an explicit control (e.g., when a customer opts-in to automatic error reporting, the customer should have a mechanism to opt-out in the future). However, there may be times when providing an explicit control may not make sense. For example, software provided by an ISP for Internet access may need to collect some data from the customer's machine in order to provide the service. It is acceptable to require the customer to stop using or uninstall the Internet access software to halt the data transfer. The customer must be informed of this requirement prior to initial use of the software or service.

When providing privacy controls, make sure that you are taking into account the needs of the customers and administrators, as well as considering special requirements for shared computers.

### 1.8.1 User Controls

User controls permit individuals to manage the privacy of their data and change their privacy preferences, such as the ability to delete any stored PII or hidden PII stored on their system. This data may reside on a computer, within a Web Service, or on a mobile device. Customers should also be given the ability to control software installation and to uninstall. If a customer consents to automatic updating, he or she also must be given the ability to stop automatic updates. Privacy controls should be easy to find and use. For example, Windows Media Player 10 places these controls in the Options page under the Tools menu. Web Services should provide a Web page that allows customers to make privacy choices. Mobile devices can provide controls on the device, in the UI provided by a connected computer, or via a link to a Web site where the customer can modify his or her settings.

If the customer provides consent to have data collected over time, the customer must be given a chance to later stop that collection (e.g., Microsoft Office Customer Experience Improvement Program):



## 1.8.2 Administrator Privacy Controls

Products targeted at or likely to be installed in enterprises and other organizations should provide administrators with the ability to centrally set values for key privacy controls and prevent their users from changing these values. For programs that run on Windows and Windows Server®, this is typically done through a mechanism like Group Policy. Group Policy provides administrators with a way to distribute software packages to targeted groups of customers and computers, control password complexity, and limit access to certain applications and functions (e.g., see [Managing Windows XP Service Pack 2 Features Using Group Policy](#)). For other server products or enterprise services, this is typically done through privacy features built into the server product (e.g., administrators choose whether Microsoft SQL Server™ 2005 will send error reports, not the individual end users). See [Section 2](#) for scenarios and details.

Administrator controls must provide the ability to prevent transfers of PII from the end-user’s machine, and the ability to control any automatic collection of User Data independent of the end-user’s preference, and where applicable should provide the ability to set group data retention policies.

Please note: in an enterprise, the administrator may act on behalf of the enterprise to provide consent to install software on and collect data from enterprise machines. Various legal considerations may impact administrators’ decisions, such as labor laws or works council agreements, but ultimately the responsibility for making those decisions lies in the hands of the administrator.

## 1.9 Shared Computers

For products that may be used on computers shared by multiple users (such as family members), features that collect or store PII should provide or identify a mechanism that allows the customer to control which other users have access to this data (e.g., via encryption or a feature of the operating system such as file permissions). By default, other users should not be able to view this data. If a customer’s PII would be accessible to other users, the customer should be informed (e.g., by clearly marking shared folders as “Shared”) and have the ability to clear the data. Informing customers each time PII becomes accessible could annoy them or cause them to ignore important warnings. A one-time notification the first time this occurs may be a better way to inform customers that the information may be visible to other users.

## **1.10 *Sharing and Collaboration Features***

Sharing and Collaboration Features allow content to be shared among members of a community, which may include personal contacts, members of the public or a combination of the two. Examples include online services such as MSN Spaces, collaboration software such as Office Live Meeting or Office Communicator, and software features, such as Shared Folders in Microsoft Windows. The users of Sharing and Collaboration Features should be given appropriate notice to help protect them from accidentally sharing information or sharing information with the wrong audience.

## **1.11 *Children's Privacy***<sup>17</sup>

Children may lack the discretion to determine when revealing their PII may put them at risk. This risk can be particularly acute with Sharing and Collaboration Features. Adding Parental Controls to products, Web sites, and Web Services can help protect the privacy of children. Web sites and Web Services that target children or collect the age of their customers must make special efforts to ensure that parents retain control over whether their children can reveal PII.<sup>18</sup> Age must be collected when the site or service is attractive to or directed at children and the site collects, uses, or allows the customer to disclose PII. If the site or service is not directed at or attractive to children, age should not be collected unless there is a compelling business justification. Once age is known, collection and disclosure of a child's PII must be blocked until parental consent is received. Some PII may be collected for a limited time while awaiting parental consent. If consent is not granted, the PII must be deleted. Once parental consent is received, parents must be provided reasonable access to information collected from and about their children. See [Section 2](#) for more details.

## **1.12 *Software Installation***

The advent of spyware has resulted in greater scrutiny of software installation practices. Spyware is often installed covertly and can compromise the customer's personal information. Customers are also exposed to other malicious software such as viruses and worms. With growing awareness of these risks, customers increasingly expect to be able to control what software is installed on their systems.<sup>19</sup> Not having control can erode their trust and lead them to perceive that innocuous software is harmful. Providing the customer with Prominent Notice and getting Explicit Consent prior to software installation are key to avoiding this pitfall.

When automatically updating the customer's system, providing separate notice and consent experiences for every update could annoy the customer and cause notice fatigue. Where updates do not materially impact the customer's experience or privacy, a single notice and consent

---

<sup>17</sup> The guidelines described are mandated by law in certain jurisdictions (e.g., South Korea, Spain and the United States). For other jurisdictions, these guidelines are recommended.

<sup>18</sup> Relevant statutes include the Act on Promotion of Information and Communications Network Utilization and Data Protection in South Korea, Royal Decree 1720/2007 in Spain, and the Children's Online Privacy Protection Act (COPPA) in the United States.

<sup>19</sup> There are also legal obligations. See the Computer Fraud and Abuse Act (18 USC §1030) and California SB 1436.

experience may be sufficient. However, if an update will materially impact the customer, separate notice should be provided and consent obtained.

### **1.13 Server Products**

Server software products (such as Windows Server 2003 and Windows SharePoint® Services) have a unique privacy audience since their operation affects both the server administrator (the person who configures and operates a server) and the end users (to whom the server's services are offered.) Generally, the design of server products must:

- respect the privacy of the administrator(s) who are the “customers” of a server product, and
- allow the administrator(s) to respect the privacy of their end users.

To help enterprises protect the privacy of their end users, it is important to document the privacy impacting behaviors and available controls in server products (e.g., in a deployment guide). This will help the enterprise to manage its end users' privacy and accurately disclose these behaviors (e.g., in its employee handbook or Works Council agreement). When building a server product, consider identifying or providing a mechanism for the administrator to display a privacy statement to his or her end users.

### **Third Parties**

There are two types of third parties considered by these guidelines: agents and independent third parties. Agents act on a company's behalf and may only use the data as instructed by the company, in accordance with the company's privacy practices (e.g., delivery services, consultants, and suppliers). Independent third parties, on the other hand, use customer information for their own purposes and follow their own privacy practices (e.g., joint marketing partners and unrelated third parties). All third parties must have a contract specifying data protection requirements. Before sharing PII with an independent third party, the customer must provide opt-in consent. If PII could be transferred to an agent, only Discoverable Notice is required.

### **1.14 Web Sites and Web Services**

In addition to the notice and consent requirements discussed in preceding sections, all externally facing Web sites must have a link to a privacy statement on every page. This includes pop-ups that collect PII. Whenever possible the same privacy statement should be used for all sites within a domain.

Web Services<sup>20</sup> are used by software products and Web sites to transfer data to and from the Internet. Examples of Web Services include Really Simple Syndication (RSS) feeds and services that provide album art for music playback. Web Services typically rely on the applications and Web sites that use them to provide the requisite notice and consent experiences.

---

<sup>20</sup> Web Services are programmatic interfaces that allow machine-to-machine and application-to-application communication. See <http://www.w3.org/2002/ws/>.

### **1.14.1 Using P3P for Privacy Statements**

The Platform for Privacy Preferences Project (P3P) is a protocol designed to help inform Web users about the data-collection practices of Web sites. It provides a way for a Web site to encode its data-collection and data-use practices in a machine-readable XML format known as a P3P policy. In general, publishing a P3P policy is recommended.

### **1.14.2 Using Cookies**

Cookies act as a local store for data that a Web site has collected about the customer. When the customer returns to the Web site, the Web site is able to retrieve the data that was previously stored in the cookie in order to know something about the identity or past behavior of the customer.<sup>21</sup> For example, PII and identifiers that facilitate tracking are sometimes stored in cookies. Privacy guidelines for cookie usage apply to locally stored text files that allow a server side connection to store and retrieve information, including HTTP cookies (i.e. Web cookies) and Flash cookies (i.e. Flash Shared Objects).

As with other transferred data, steps should be taken to reduce the privacy risk posed by cookies (e.g., encrypt PII, persist the cookie for the shortest period that meets the business need, and use the least sensitive form of tracking such as an anonymous visitor ID). Persistent cookies must not be used where a session cookie would satisfy the purpose. PII should not be stored in a persistent cookie unless it is absolutely necessary. The customer must be given Prominent Notice and must provide Opt-In Explicit Consent before PII can be stored in a persistent cookie. Persistent cookies should expire within the shortest timeframe that achieves the business purpose. PII stored in a persistent cookie must be encrypted.

## **1.15 *Special Considerations***

### **1.15.1 Pre-Release Products**

A pre-release product is an early version of a product (e.g., a “beta” release) that is distributed to test functionality and obtain customer feedback. Some products include automatic feedback mechanisms that collect anonymous usage and error data. Companies sometimes require this data in exchange for an early look at the product. In these cases, it is acceptable to have this collection on by default provided the user is adequately notified and consent is obtained (e.g., via the terms of service). See [Section 2](#) for more guidelines reflecting the unique needs of pre-release products.

### **1.15.2 Essential Transfers and Updates**

Sometimes, transferring data or updating an application is essential to the function or service offered (e.g., the product would not work without the transfer or update, or the product is marketed as including the transfer or update). For example, an ISP may require periodic transfers of Internet connection status information to maintain its quality of service. Alternatively, an antivirus service advertised as “ever vigilant” may frequently pull down updated virus definitions. In these cases, where data transfer and system updates are essential, it is important to notify customers prior to installation that it is an all-or-nothing proposition: to

---

<sup>21</sup> <http://www.antispywarecoalition.org/documents/GlossaryJune292006.htm>

prevent the behavior, the customer must not install the product. After installation, the customer will need to uninstall the product in order to prevent subsequent transfers or updates.

### **1.15.3 File and Path Names**

File and path names do not fit neatly within any single category of User Data. File and path names may be anonymous or may contain PII, depending on what names the customer chose. When file or path names will be transferred, steps should be taken to lower the sensitivity of the data captured. When capturing file names, consider including only the names of files with specific extensions that are less likely to be named by the user such as .exe or .dll. When capturing path names, consider removing the unnecessary portions of the path.

### **1.15.4 IP Address**

When information is transferred over the Internet, the customer's IP address is always sent with the data as part of the communication protocol. Whether or not an IP address is PII is a subject of great debate.<sup>22</sup> Either way, IP addresses should be treated with care. To reduce the chance of unintended correlation (e.g., when trying to maintain anonymity), storing an IP address with PII should be avoided, unless it is essential to the business purpose. Wherever possible, strip the IP address from the payload, reduce its sensitivity by keeping a limited number of digits, or discard the IP address after translating it to a less-precise location.

### **1.15.5 When Things Change**

The privacy implications of software, Web sites, and Web Services may change over time. When customers have given consent for the use of their data, they have consented to the specific use and business purpose disclosed to them. Additional consent must be received in order to use the customer's data for a different purpose. When there is a material change to the privacy implications of an application, Web site, or Web Service, additional notice should be given to the customer.

---

<sup>22</sup> See [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf) and [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2008/wp148\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf).

## 2 Guidelines

These guidelines reflect the following principles: notice, choice, onward transfer (to third parties), access, security, and data integrity. With respect to choice, the guidelines cover not only initial consent, but also the ability for customers to later change their minds through user controls. In addition, the guidelines specify administrator-level controls for deployments within an enterprise.

### 2.1 How to Use This Section

In the scenarios that follow, bold text indicates a **guideline**, while italicized text provides additional explanation or common *exceptions* to the guideline. The words “must” and “should” have special meaning. “Must” indicates the practice is required. “Should” indicates the practice is recommended. Other words that have special meaning include:

<i>Company:</i>	The entity that builds or provides the software or service.
<i>Company Approval:</i>	The consent of the authorized privacy council or privacy decision makers within the Company, which may include legal counsel.
<i>Enterprise:</i>	A corporate or governmental entity that deploys the software or service developed by the Company within the bounds of its organization.
<i>Customer:</i>	The individual that uses the software or service developed by the Company. Customers include consumers and employees of an Enterprise.
<i>Security Guidelines:</i>	Company or industry-wide security standards (e.g., see <a href="#">Appendix B</a> ).

Section 2 includes requirements for servers and server products based on the role an administrator may be playing. These roles include:

<i>System Administrator:</i>	The operating system administrator of the computer in an Enterprise where server software is installed.
<i>Application Administrator:</i>	The administrator of a server application (e.g., Microsoft Exchange Server). In some cases, but not all, the application administrator and the system administrator may be the same person.
<i>Instance Administrator:</i>	The administrator of a single “instance” within a server application. For example, in the context of a SharePoint Portal Server, the administrator of a single SharePoint site or sub-site is an instance administrator. In Internet Information Server (IIS), the administrator of a single Web site is an instance administrator. Again, in some cases, the instance administrator and the application administrator may be the same person.

## 2.2 Scenarios

The pages that follow provide the guidelines for the following scenarios:

- **Transferring PII to and from the User's System**
  - Example: *Sending product registration to the Company*
  - Example: *Transferring a file containing hidden PII*
  - Example: *Submitting data entered by the customer in a Web form*
  - Example: *Displaying profile information stored at the Company to the customer*
- **Storing PII on the Customer's System**
  - Example: *Storing the customer's contacts*
  - Example: *Caching Web pages that contain PII*
  - Example: *Storing PII in a cookie*
- **Transferring Anonymous and Pseudonymous Data from the Customer's System**
  - Example: *Anonymous monitoring by an ISP to assess the quality of an Internet connection (i.e. Quality of the Service or QoS)*
  - Example: *Sending anonymous error reports to the Company*
  - Example: *Sending a cookie with an anonymous tracking ID to a Web site when a customer clicks on a hyperlink.*
- **Installing Software on a Customer's System**
  - Example: *Automatically updating software*
- **Deploying a Web Site**
  - Example: *Creating a Web portal directed at consumers*
- **Storing and Processing User Data at the Company**
  - Example: *Storing User Data in a database or Web log*
  - Example: *Generating statistics from collected User Data*
  - Example: *Employees accessing stored data*
  - Example: *Transferring data from one internal group to another internal group*
- **Transferring User Data outside the Company**
  - Example: *Sending PII from the Company to an agent*
  - Example: *Sending PII from the Company to an independent third party that will use the PII for its own purposes*
- **Interacting with Children**
  - Example: *Hosting a Web site intended to help elementary school children with their homework*
  - Example: *Collecting a customer's age or birth date on a Web site that is not inherently attractive to children*
- **Server Deployment**
  - Example: *Installing server software in an Enterprise*
  - Example: *Storing User Data in an Enterprise*
  - Example: *Transferring User Data outside the Enterprise firewall*

# Scenario 1: Transferring PII to and from the Customer's System

## 1.1 Collection and Transfer of PII from the Customer's System or Transfer of PII from the Company to the Customer's System

Examples include:

- *Sending product registration to the Company, transferring a file containing hidden PII or submitting data entered by the customer in a Web form.*
- *Displaying profile information stored at the Company to the customer.*

<b>Category</b>	<b>Guidelines</b>
<b>Notice and Consent</b>	<p><b>1.1.1 Must provide Prominent Notice and get Opt-In Explicit Consent prior to transfer of PII from customer's system.</b></p> <p><i>When the customer enters PII directly (versus automatic collection), the consent requirement can be fulfilled if the customer clicks a properly labeled submit button.</i></p> <p><i>For automatic collection, the Prominent Notice and Explicit Consent experience should ideally be provided in the UI, not in the License Agreement or Terms of Use.</i></p> <p><i>Software that stores and transfers hidden PII should provide Prominent Notice and get Explicit Consent prior to each transfer unless customer has indicated otherwise (e.g., the customer checks a box that states "do not ask me each time").</i></p> <p><i>With Company Approval, the Prominent Notice and Explicit Consent requirement may be waived if the PII is unsolicited.</i></p> <p><b>1.1.2 Must provide Prominent Notice and get Explicit Consent if PII being transferred will be used for secondary purposes such as marketing.</b></p> <p><i>Consent should be obtained via a separate mechanism.</i></p> <p><i>Whether opt-out or opt-in is appropriate depends on local law. Before using Opt-Out Explicit Consent, get Company Approval.</i></p> <p><b>1.1.3 Must have Explicit Consent if Sensitive PII (e.g., credit card number) being transferred will be retained at the Company for future use by the customer.</b></p> <p><i>A separate consent mechanism should be used in the case of a one-time transaction (as opposed to an ongoing billing relationship such as a subscription).</i></p> <p><b>1.1.4 Must get Company Approval prior to collecting, storing or transferring a user's real-time location data.</b></p> <p><b>1.1.5 Must provide customer with access to a Company Approved Discoverable Notice (e.g., privacy statement) within the notice and consent experience.</b></p> <p><i>The link should be prominently included near the "submit" (or equivalent) button. The link text must not be smaller than other similar links on the page, such as Terms of Use. If supplementing the Discoverable Notice with text in the Prominent Notice, the text must not contradict any restrictions presented in the Discoverable Notice (e.g., assert on the form that data will be used in a way that is prohibited in the privacy statement). The Prominent Notice can be more restrictive (e.g., notice asserts data will not be shared with a third party while the privacy statement does not prohibit onward transfer). The Prominent Notice may also provide additional information (e.g., an alternative method for accessing the data collected).</i></p>

	<p><b>1.1.6 Should clearly distinguish in UI between optional and required data.</b></p> <p><i>If some of the data to be entered by the customer is optional, should make it clear which items are mandatory (e.g., mark fields with an asterisk) and permit the customer to submit without any entries in the optional fields.</i></p> <p><b>1.1.7 Should provide a relevant and clear value proposition for users to provide registration data.</b></p> <p><b>1.1.8 Should not use free-form text fields (e.g., scrolling text boxes) when a defined field (e.g., pre-populated list box) can be used instead. If free-form text fields are used, they should be accompanied by a privacy warning directly in the UI.</b></p> <p><i>The warning should caution the customer to not enter PII in the free-form text field. Only use free-form text fields if absolutely warranted.</i></p> <p><b>1.1.9 Must follow the requirements in Scenario 8 if PII will be transferred to a third party.</b></p> <p><i>This transfer could be from the Company, or directly to the third party from Company supplied software on the customer's system (e.g., via a plug-in).</i></p>
<p><b>Security and Data Integrity</b></p>	<p><b>1.1.10 Must transfer Sensitive PII to or from a customer's system over the Internet using a secure method that helps prevent unauthorized access.</b></p> <p><i>Secure methods include using a minimum of 128-bit SSL encryption (Consult Company security guidelines and <a href="#">Appendix B</a> for additional guidance).</i></p> <p><i>Secure methods may not be required if:</i></p> <ul style="list-style-type: none"> <li>(a) The transfer is a local transfer to a third party component on the customer's system, or</li> <li>(b) Sensitive PII is unsolicited.</li> </ul> <p><b>1.1.11 Should transfer non-Sensitive PII to or from a customer's system over the Internet using a secure method that helps prevent unauthorized access.</b></p> <p><i>Secure methods may not be required if:</i></p> <ul style="list-style-type: none"> <li>(a) The transfer is a local transfer to a third party component on the customer's system,</li> <li>(b) Non-Sensitive PII is unsolicited,</li> <li>(c) The transfer is of unique identifiers that in transfer are not associated with PII (for example, a unique identifier sent with a page view), or</li> <li>(d) The non-Sensitive PII is a unique identifier that is fundamental to the routing of the data via industry standard protocols (e.g., e-mail address).</li> </ul> <p><b>1.1.12 Should not use methods of form submission that potentially expose data in a Web form intended for, or likely to result in, the collection of PII.</b></p> <p><i>In general, the GET method should not be used (it has inherent risk of revealing information to third-party Web sites).</i></p> <p><b>1.1.13 Must only transfer minimum amount of data to achieve business purpose.</b></p> <p><b>1.1.14 Should only transfer customer specific data like GUIDs, computer serial numbers, or user IDs if essential to business purpose.</b></p> <p><i>Should avoid storing IP address with other User Data unless it is essential to do so.</i></p> <p><b>1.1.15 Should use data validation controls to filter out inconsistent, incomplete, or incorrect PII.</b></p> <p><i>Use reasonable measures to ensure that the data types are consistent and correct by using dropdown and data value lookup tests against the data elements entered by the customer.</i></p>

	<p><b>1.1.16 Should mask passwords or pins when collecting or displaying this information.</b></p> <p><i>For example, use dots to represent keystrokes.</i></p> <p><b>1.1.17 Should suppress a majority of the digits when displaying a credit card number that has been stored.</b></p> <p><i>For example, display only the last four digits of the credit card number. This also applies to other sensitive identifiers such as Social Security numbers.</i></p>
<b>Customer Access and Controls</b>	<p><b>1.1.18 Customer must be able to control automatic collection and transfer of PII.</b></p> <p><i>If ongoing collection and transfer of PII is “essential” to the functioning of the product or service then no special customer control needs to be provided -- collection can continue until customer stops using the product or service (i.e. "all or nothing").</i></p> <p><b>1.1.19 Customer should be able to remove hidden PII prior to transfer.</b></p> <p><i>Files may contain PII in metadata of which users are not aware, such as GPS location in a photograph. Users should be given access and control of this data if the Company’s product or service was used to create it. When metadata is not from a Company product or service, give information as it can about how the user can access and control PII in metadata (such as adding a warning to a photo sharing web service that some photographs may include PII in metadata).</i></p> <p><b>1.1.20 Must follow the requirements in Scenario 6 if data will be transferred to and stored at the Company.</b></p> <p><i>For example, must provide the ability for the customer to correct stored PII and update contact preferences.</i></p>
<b>Additional Controls</b>	<p><b>1.1.21 Must follow the requirements in Scenario 8 if age-indicative information is collected or the user experience is targeted at children.</b></p> <p><b>1.1.22 Must get Company Approval prior to collecting and transferring Sensitive PII.</b></p> <p><i>Examples of Sensitive PII include Social Security Number, credit card and bank account numbers, religious beliefs, ethnicity, and information about sexuality (see section 1.1.1.3).</i></p> <p><b>1.1.23 Administrator should be able to prevent transfers of PII.</b></p> <p><i>This is typically fulfilled by firewall controls when transfers are to a specific URL or e-mail address.</i></p> <p><b>1.1.24 Administrator should be able to control whether PII is automatically collected.</b></p>

## Scenario 2: Storing PII on the Customer’s System

### 2.1 Storage of PII on the Customer’s System

Examples include:

- Storing the customer’s contacts, caching Web pages that contain PII, or storing PII in a cookie.

Category	Guidelines
<p><b>Notice and Consent</b></p>	<p><b>2.1.1 Must provide the customer with notice and get consent prior to storage of Sensitive PII.</b></p> <p><i>While Explicit Consent is preferred, Implicit Consent is sufficient when the nature of the product makes it clear to the user that the data will be persisted.</i></p> <p><i>Storing Sensitive PII for the purpose of Automatic completion (e.g., AutoComplete of passwords) requires Explicit Consent.</i></p> <p><i>Notice and consent are not required when the PII is unsolicited.</i></p> <p><b>2.1.2 Must provide the customer with Prominent Notice and get Opt-In Explicit Consent when storing PII in a persistent cookie.</b></p> <p><b>2.1.3 Should provide at a minimum a Company Approved Discoverable Notice that specifies what data is stored and what controls are available prior to storing Hidden PII.</b></p> <p><i>Hidden PII includes PII stored as "metadata" and cached Web pages not obvious to customer.</i></p> <p><b>2.1.4 Should make it clear to customers if PII could be accessed by other users.</b></p> <p><i>Goal is to prevent accidental disclosure of PII. For example, shared folders on a shared machine or network should be clearly marked. When storing data in a shared database, should inform the customer in UI or at a minimum in the Discoverable Notice.</i></p>
<p><b>Security and Data Integrity</b></p>	<p><b>2.1.5 Must store Sensitive PII using appropriate security mechanisms that help prevent unauthorized access.</b></p> <p><i>Suitable mechanisms may include encryption and file permissions. Consult Company security guidelines to determine whether encryption is necessary, the algorithm to be used, and whether it should be enabled by default or provided as an option. See <a href="#">Appendix B</a> for additional guidance.</i></p> <p><b>2.1.6 Should identify or provide appropriate security mechanisms that will help the customer prevent unauthorized access to stored Non-Sensitive PII.</b></p> <p><i>If a mechanism is not enabled by default, customers should have the ability to enable it at their discretion. Suitable mechanisms may include encryption and file permissions.</i></p> <p><b>2.1.7 Must encrypt PII when stored in a persistent cookie.</b></p> <p><i>Regardless of the type of cookie, Sensitive PII must be encrypted.</i></p> <p><b>2.1.8 Must restrict access to Sensitive PII by default unless the customer has authorized such access.</b></p> <p><i>Consent can be implicit (e.g., dragging a file into a folder that is clearly marked "shared").</i></p> <p><b>2.1.9 Should restrict access to stored non-Sensitive PII by default.</b></p>

	<p><b>2.1.10 Should avoid persisting Sensitive PII on the customer's system whenever possible.</b></p> <p><i>Avoid creating temporary files (e.g., cached Web pages) with Sensitive PII. If they are required, remove them when the session ends or application closes.</i></p> <p><i>Disable caching of Web page content that could contain Sensitive PII.<sup>23</sup></i></p> <p><b>2.1.11 Should persist PII for the shortest time possible to meet the business purpose.</b></p>
<b>Customer Access and Controls</b>	<p><b>2.1.12 Customer should be able to control whether PII is stored.</b></p> <p><i>Controls are even more important when customer is a guest (e.g., kiosk scenario).</i></p> <p><b>2.1.13 Customer should be able to delete any PII that was stored on the customer's system, including Hidden PII.</b></p> <p><i>Removal of this information is commonly referred to as "clearing your tracks". For example, being able to clear your personal history like "files recently accessed" and "Web sites visited".</i></p> <p><b>2.1.14 Customer must be able to view and edit stored PII they entered.</b></p> <p><i>For example, the customer's contact information.</i></p>
<b>Additional Controls</b>	<p><b>2.1.15 Must get Company Approval if storing Sensitive PII on the customer's system.</b></p> <p><b>2.1.16 Consider whether Administrator should be able to prevent clearing of PII by the customer.</b></p> <p><i>For example, in financial application, the administrator may need to ensure the integrity of logs for auditing purposes.</i></p>

---

<sup>23</sup> For example, insert the following code in the HTTP header: <META HTTP-EQUIV="Pragma" CONTENT="no-cache"> for use over a secure connection or <META HTTP-EQUIV="Expires" CONTENT="-1"> for non-secure pages.

## Scenario 3: Transferring Anonymous and Pseudonymous Data from the Customer's System

### 3.1 Ongoing Collection and Transfer of Anonymous and Pseudonymous Data

Examples include:

- Anonymous monitoring by an ISP to assess the quality of an Internet connection (i.e. Quality of the Service or QoS), or sending anonymous error reports to the Company.

Category	Guidelines
<b>Notice and Consent</b>	<p><b>3.1.1 Must provide the customer with Prominent Notice and get Explicit Consent prior to collection.</b></p> <p><i>The Prominent Notice and Explicit Consent experience should generally be provided in the UI, not in the License Agreement or Terms of Use.</i></p> <p><i>If the ongoing collection and transfer of Anonymous or Pseudonymous Data is "essential" to the functioning of the product or service, it may be disclosed and agreed to as part of product/service acceptance (e.g., via Terms of Service, Terms of Use, or other prominent Opt-In experience). Examples of essential Anonymous or Pseudonymous Data collection include: (a) anonymous QoS monitoring by an ISP and (b) enabling by default collection of anonymous usage statistics for pre-release products to obtain feedback.<sup>24</sup> Classifying anonymous or pseudonymous collection and transfer as "essential" requires Company Approval.</i></p>
<b>Security and Data Integrity</b>	<i>No special requirements because the data is anonymous or pseudonymous.<sup>25</sup></i>
<b>Customer Access and Controls</b>	<p><b>3.1.2 Customer must be able to stop subsequent collection and transfer.</b></p> <p><i>If ongoing collection and transfer of Anonymous or Pseudonymous Data is "essential" then no special customer control needs to be provided -- collection can continue until customer stops using the product or service (i.e. "all or nothing").</i></p>
<b>Additional Controls</b>	<p><b>3.1.3 Administrator must be able to enable/disable transfer independent of customer's preference.</b></p> <p><i>If ongoing collection and transfer of Anonymous or Pseudonymous Data is "essential" then no special administrator control needs to be provided -- collection can continue until customer stops using the product or service or the administrator prevents use of the product or service (i.e. "all or nothing").</i></p>

### 3.2: Discrete Collection and Transfer of Anonymous and Pseudonymous Data

Examples include:

- Sending a cookie with an anonymous tracking ID to a Web site when a customer clicks on a hyperlink.

Category	Guidelines
----------	------------

<sup>24</sup> Typically, a pre-release product provides customers with an early look at an upcoming software release in exchange for their feedback. In this context, collection of anonymous usage statistics is a form of feedback that may be classified as essential.

<sup>25</sup> To enhance anonymity, should not retain IP address. If IP address needs to be retained (e.g., to help detect Denial of Service attacks), it should be stored separately from the payload of the Web request (e.g., the usage statistics).

<b>Notice and Consent</b>	<p><b>3.2.1 Must get consent from the customer prior to transfer and provide a Company Approved Discoverable Notice.</b></p> <p><i>Consent may be Explicit or Implicit (e.g., clicking a hyperlink that indicates the Internet will be accessed).</i></p> <p><i>In the case of visiting a Web site, may provide the Discoverable Notice immediately after the transfer (e.g., displaying a link to a privacy statement at the bottom of the Web page that was launched).</i></p> <p><b>3.2.2 Should highlight applicable controls in the Discoverable Notice.</b></p> <p><i>If cookies are used, document how they can be blocked.</i></p>
<b>Security and Data Integrity</b>	<i>No special requirements because the data is anonymous or pseudonymous.</i>
<b>Customer Access and Controls</b>	<p><b>3.2.3 No special control necessary.</b></p> <p><i>Customer initiates transfer and implicitly has control.</i></p>
<b>Additional Controls</b>	<p><b>3.2.4 Administrator must be able to prevent transfer to the Internet.</b></p> <p><i>Mechanism can be high level (e.g., disable entire feature or a global offline mode).</i></p>

## Scenario 4: Installing Software on a Customer's System

### 4.1 Install software on a customer's system

Category	Guidelines
<p><b>Notice and Consent</b></p>	<p><b>4.1.1 Must provide the customer with Prominent Notice and get Explicit Consent prior to installation of software on a customer's system.</b></p> <p><i>In an enterprise, administrators should be given a mechanism to consent on behalf of their end users. It is the administrators' responsibility to ensure that the use of such a mechanism complies with their internal policies and local law.</i></p> <p><b>4.1.2 Should provide Prominent Notice in the UI when privacy settings are migrated.</b></p> <p><i>The Prominent Notice may simply indicate that settings are being migrated with a link to more information about which settings are being migrated.</i></p> <p><b>4.1.3 Should not migrate a privacy setting on upgrade if the meaning of the privacy setting has changed.</b></p> <p><b>4.1.4 Should not migrate any privacy settings from a pre-release version to a final release version.</b></p> <p><b>4.1.5 Must provide the user with Prominent Notice and get consent prior to exposing the user's PII in a Sharing or Collaboration Feature.</b></p> <p><i>For example, in instant messaging software, the user's phone number must not be exposed to other users unless the user or an enterprise administrator has opted in to sharing the phone number.</i></p> <p><i>In addition to obtaining consent from the organizer of a collaborative workspace, the software should enable the organizer to get consent from each of the participants, or obtain that consent on behalf of the organizer.</i></p> <p><i>If a feature shares a user's desktop, the desktop must be considered PII since PII could be visible in open documents.</i></p> <p><b>4.1.6 Must provide the user with notice and get consent prior to exposing Anonymous or Pseudonymous data in a Sharing or Collaboration Feature.</b></p> <p><i>For example, if a user creates an e-mail account that includes the option to create a pseudonymous online profile (e.g., nickname) as part of the service, the user must be given notice and the ability to Opt-Out.</i></p> <p><b>4.1.7 Must provide the user with notice and get consent prior to changing file extension associations already associated with another application</b></p>
<p><b>Security and Data Integrity</b></p>	<p><b>4.1.8 Should digitally sign software with a certificate from a well-known, trusted certification authority to help ensure integrity.</b></p> <p><i>This helps the customer to determine whether the software is from a trusted source.</i></p> <p><i>At a minimum, trusted certification authorities should have passed a Web Trust Audit.</i></p>
<p><b>Customer Access and Controls</b></p>	<p><b>4.1.9 Should use standard mechanisms for installing software so that customers have control over installing and uninstalling the software.</b></p> <p><i>When possible use a mechanism such as Add/Remove Programs to uninstall or modify the software.</i></p>

	<b>4.1.10</b> Should provide users with choices regarding the amount and types of data they wish to share in a Sharing and Collaboration Feature.
--	---

## 4.2 Ongoing update of software on a customer’s system

Examples include

- Automatically updating software.

Category	Guidelines
<b>Notice and Consent</b>	<p><b>4.2.1</b> Must provide the customer with <b>Prominent Notice</b> and get <b>Explicit Consent</b> prior to enabling automatic update of software on a customer’s system.</p> <p><i>Consent may be one-time and obtained up front; however, if a particular update will materially change the customer’s experience, it is a best practice to provide an additional notice and/or consent experience.</i></p> <p><i>If ongoing updates are “essential” to the functioning of the product or service, it may be disclosed and agreed to as part of product/service acceptance (e.g., via Terms of Service, Terms of Use or other prominent Opt-In experience). An example of essential ongoing updates is an antivirus software service that would not be effective without ongoing updates to the virus signatures. Classifying ongoing updates as “essential” requires Company Approval.</i></p> <p><i>In an enterprise, administrators should be given a mechanism to consent on behalf of their end users. It is the administrators’ responsibility to ensure that the use of such a mechanism complies with their internal policies and local law.</i></p>
	<p><b>4.2.2</b> Should provide the customer with a mechanism to track the automatic updates that have been installed.</p>
<b>Security and Data Integrity</b>	<p><b>4.2.3</b> Should digitally sign software with a certificate from a well-known, trusted authority to help ensure integrity.</p> <p><i>This helps the customer to determine whether the software is from a trusted source.</i></p>
<b>Customer Access and Controls</b>	<p><b>4.2.4</b> Customer must be able to stop subsequent updates.</p> <p><i>If ongoing updates are “essential” then no special customer control needs to be provided - updates can continue until the customer stops using the product or service (i.e. “all or nothing”).</i></p> <p><i>In an enterprise, it is sufficient to only provide this control to administrators.</i></p>
<b>Additional Controls</b>	<p><b>4.2.5</b> Administrator must be able to enable/disable ongoing update mechanisms.</p> <p><i>If ongoing updates are “essential” then no special administrator control needs to be provided – updates can continue until the customer stops using the product or service or the administrator prevents use of the product or service (i.e. “all or nothing”).</i></p>

# Scenario 5: Deploying a Web Site

## 5.1 Deploy a Public Web Site

Examples include:

- Creating a Web portal directed at consumers.

Category	Guidelines
<p><b>Notice and Consent</b></p>	<p><b>5.1.1 Must provide a link to a Company Approved privacy statement on every Web page.</b></p> <p><i>Applies to all externally facing Web pages regardless of whether PII is collected. Privacy statement link must not be smaller than other links on the page, such as legal notices, and should be placed in a consistent location such as the page footer.</i></p> <p><i>Pop-ups are included if they collect PII. For example, a survey presented in a pop-up that requests customer's name would require a privacy link. Pop-ups that only collect PII that is unsolicited or part of a communication protocol (e.g., e-mail address in the address line of an e-mail) are excluded.</i></p> <p><i>Pages hosted by the Company on behalf of a third party may be excluded if there is little or no Company branding on the hosted pages (e.g. nothing more than a small notice such as: "This page is hosted for [Third Party] by Company"). Where the third party may collect PII, must provide a mechanism for the third party to display its privacy statement.</i></p> <p><i>Whenever possible use the same privacy statement for all sites within a domain. Likewise, use the existing infrastructure around data collection and storage, contact preference management, customer data access, and customer inquiry response. Get Company Approval if a different privacy statement or infrastructure is required.</i></p> <p><b>5.1.2 Must provide the user with Prominent Notice and get consent prior to exposing the user's PII in a Sharing or Collaboration Feature.</b></p> <p><i>For example, to create a public profile with the user's contact information when the user creates an online e-mail account, you must first get the user's consent.</i></p> <p><i>In addition to obtaining consent from the organizer of a collaborative workspace, the software must enable the organizer to get consent from each of the participants, or obtain that consent on behalf of the organizer.</i></p> <p><i>If a feature shares a user's desktop, what may be open on the user's desktop must be considered PII.</i></p> <p><b>5.1.3 Must provide the user with notice and get consent prior to exposing Anonymous or Pseudonymous data in a Sharing or Collaboration Feature.</b></p> <p><i>For example, if a user creates a mail account that includes the option to create a pseudonymous online profile (e.g., nickname) as part of the service, the user must be given notice and the ability to Opt-Out.</i></p> <p><b>5.1.4 Must provide the user with Prominent Notice and get separate Explicit Consent prior to exposing age in a Sharing or Collaboration Feature.</b></p> <p><i>If age will be exposed, must meet the requirements in Scenario 8.</i></p> <p><b>5.1.5 Should adopt the Layered Notice approach for privacy statements that are lengthy or complex.</b></p> <p><b>5.1.6 Should provide both compact and full P3P privacy policy.</b></p> <p><b>5.1.7 Should certify privacy statement with an independent privacy certification</b></p>

	<p><b>organization.</b></p> <p><i>Certification (e.g., by an organization such as TRUSTe) is recommended for Web sites that collect PII and are intended for large audiences. Certification may not be suitable for sites aimed at a limited audience or of limited duration.</i></p>
<b>Use of Cookies</b>	<p><b>5.1.8 Must not use persistent cookies where a session cookie would satisfy the business purpose.</b></p> <p><i>For example, if the purpose of a cookie is to maintain session state, then a persistent cookie must not be used.</i></p> <p><b>5.1.9 Should not store PII in a persistent cookie unless absolutely necessary.</b></p> <p><b>5.1.10 Must get Opt-In Explicit Consent from the customer for persistent cookies that store PII.</b></p> <p><b>5.1.11 Must encrypt PII when stored in a persistent cookie.</b></p> <p><i>Regardless of the type of cookie, Sensitive PII must be encrypted.</i></p> <p><b>5.1.12 Should not persist cookies for longer than necessary to fulfill the business purpose.</b></p> <p><i>When the necessary duration is unknown, a best practice is to set cookies to expire after a limited period of time such as two years.</i></p>
<b>Additional Requirements</b>	<p><b>5.1.13 Must meet the requirements in Scenario 2 if persisting data on the customer’s system.</b></p> <p><i>Includes cookies and alternative storage mechanisms such as locally stored objects.</i></p> <p><b>5.1.14 Must meet the requirements in Scenario 1 for any Web page or pop-up that collects PII.</b></p> <p><b>5.1.15 Must meet the requirements in Scenario 8 if the user experience is targeted at children.</b></p> <p><b>5.1.16 Should provide users with choices regarding the amount and types of data they wish to share in a Sharing and Collaboration Feature.</b></p>

## Scenario 6: Storing and Processing User Data at the Company

### 6.1 Store and Process User Data at the Company

Examples include:

- Storing User Data in a database or Web log, or generating statistics from collected User Data.
- Transferring data from one internal group to another internal group

Category	Guidelines
<b>Notice and Consent</b>	<p><b>6.1.1 Must have provided the customer appropriate notice and obtained appropriate consent prior to using data.</b></p> <p><i>See Scenarios 1-3 for notice and consent requirements.</i></p> <p><i>PII use must be limited to what was originally disclosed and/or agreed to by the customer when the data was collected.</i></p> <p><i>To use PII in ways that exceed the original notice, must provide additional notice and obtain consent to cover the expanded use.</i></p>
<b>Security and Data Integrity</b>	<p><b>6.1.2 Must only store minimum amount of data necessary to achieve business purpose.</b></p> <p><i>Should only store customer specific data like unique IDs, computer serial numbers, or user IDs if essential to business purpose. Should obfuscate or remove IP address if not essential.</i></p> <p><b>6.1.3 Must store PII using appropriate security mechanisms to help prevent unauthorized access.</b></p> <p><i>Suitable mechanisms may include encryption and file permissions. Which mechanisms are appropriate depends on the sensitivity of the data (e.g., credit card numbers should be encrypted). See Company security guidelines and <a href="#">Appendix B</a>.</i></p> <p><b>6.1.4 Must restrict PII access to those with a need to know.</b></p> <p><i>Use both physical and electronic mechanisms (e.g., door locks, file permissions, and storage in approved data center as appropriate). Additionally, consider limiting access based on job function. See Company security guidelines and <a href="#">Appendix B</a>.</i></p> <p><b>6.1.5 Must maintain integrity of the data.</b></p> <p><i>In order to help protect data integrity and to reduce the complexity with regard to other compliance efforts (such as security, customer access, etc.), PII should be maintained in a Company Approved central database, or as few databases as possible.</i></p> <p><i>When storing User Data in multiple databases, must accurately retain and update customer's contact information and preferences across all databases. Updates must be applied in a timely manner.</i></p> <p><b>6.1.6 Should aggregate stored data to reduce sensitivity wherever possible.</b></p> <p><i>To the degree minimization has reduced data sensitivity (e.g., by anonymizing, aggregating, or removing sensitive data), security and access requirements can be reduced.</i></p>
<b>Customer Access and Controls</b>	<p><b>6.1.7 Must provide a secure mechanism for customers to access and correct stored PII.</b></p> <p><i>Secure mechanisms include using encryption (e.g., via SSL) to transfer PII.</i></p> <p><i>Applies to PII stored in a persistent database (e.g., a database used to maintain customer</i></p>

	<p>contact information).</p> <p>Includes the ability to make changes to their contact preferences if the PII will be used for secondary purposes such as marketing. Changes to contact preferences must be applied across all relevant databases in a timely manner.</p> <p>When possible, should provide real-time access at no charge.</p> <p><b>6.1.8 Must authenticate customers via a Company Approved process before collecting, displaying, or modifying PII or contact preferences.</b></p>
<b>Additional Requirements</b>	<p><b>6.1.9 Must store PII for the shortest time necessary to achieve the business purpose.</b></p> <p>Implement a Company Approved data retention policy that reflects this requirement. Consider all aspects of data storage, including data that has been backed up or archived.</p> <p><b>6.1.10 Should provide a mechanism to audit access to PII.</b></p> <p><b>6.1.11 Must meet the requirements in Scenario 8 if the customer is a child.</b></p>

## 6.2 Access To Stored Data by Employee or Company's Agent

Examples include:

- Employees accessing a customer database.

<b>Category</b>	<b>Guidelines</b>
<b>Notice and Consent</b>	<p><b>6.2.1 Should provide notice to employees and agents accessing PII informing them of their obligations.</b></p> <p>Obligations include using PII only for legitimate business purposes and in a manner consistent with the terms under which the data was collected.</p> <p>Such notice should not be the sole means of informing employees and agents of their obligations, but rather should serve as a timely reminder to be used in conjunction with training, documented policies and procedures, and other appropriate compliance measures.</p>
<b>Security and Data Integrity</b>	<p><b>6.2.2 Must limit access to those with a valid business need.</b></p> <p><b>6.2.3 Should only provide access to records and data fields necessary to accomplish the business purpose.</b></p> <p><b>6.2.4 Must revoke access if no longer required as part of an employee or agent's job function or when the agent's contract has ended.</b></p> <p>Should follow a consistent policy for revoking access to User Data.</p> <p>Must review and update access list on a regular basis. Access must be consistent with terms under which the data was collected.</p>
<b>Customer Access and Controls</b>	<p>See Scenario 6 for customer access requirements.</p>
<b>Additional Requirements</b>	<p><b>6.2.5 Must have a Company Approved contract with agent that specifies data protection requirements.</b></p> <p><b>6.2.6 Should provide a mechanism to audit access to PII.</b></p>

## Scenario 7: Transferring User Data outside the Company

### 7.1 Transfer PII to a Third Party

Examples include:

- Sending PII from the Company to an agent or sending PII from the Company to an independent third party that will use the PII for its own purposes.

Category	Guidelines
<b>Notice and Consent</b>	<p><b>7.1.1 Must provide a separate Opt-In Explicit Consent experience if PII will be shared with independent third parties.</b></p> <p><i>If the experience is co-branded, separate consent is not required when it is conveyed to the customer that both parties will receive the data, and the data is only shared between the Company and the named third party.</i></p> <p><b>7.1.2 Must provide a link in the UI to an independent third party's privacy statement, if the UI specifies that the third party will receive the data.</b></p> <p><i>If the data will also be transferred to the Company, links to both privacy statements or a joint privacy statement must be provided. If both privacy statements are used, the UI needs to make it clear that both parties will use the data.</i></p> <p><b>7.1.3 Must disclose in the UI the type of independent third party that may receive the data when the recipients of the transfer are not specified.</b></p> <p><i>Examples of types of independent third parties include business partners, hardware vendors, and software vendors.</i></p> <p><b>7.1.4 Must disclose in a Discoverable Notice if PII could be transferred to agents of the Company.</b></p> <p><b>7.1.5 Must limit third party use to what was originally disclosed to the customer in the notice and consent experience when the data was first collected.</b></p> <p><i>To use the data in ways that exceed the original notice, must provide additional notice and obtain consent to cover the expanded use.</i></p>
<b>Security and Data Integrity</b>	<p><b>7.1.6 Must transfer PII using a secure method that prevents unauthorized access.</b></p> <p><b>7.1.7 Must only transfer minimum data necessary to achieve the business purpose.</b></p> <p><b>7.1.8 Should require agents to access and maintain PII on the Company's network when possible.</b></p> <p><i>Maintaining the data at the Company increases the level of confidence that data will be appropriately secured.</i></p> <p><i>However, in some cases it makes sense for agents to process data at their sites (e.g., delivery and fulfillment services).</i></p>
<b>Customer Access and Controls</b>	<p><b>7.1.9 Must provide the ability for a customer to update contact preferences for future transfers of PII to independent third parties.</b></p>
<b>Additional Requirements</b>	<p><b>7.1.10 Must have a Company Approved contract containing adequate data protection provisions with the third party to whom PII will be transferred.</b></p>

	<p><i>Applies to agents acting on the Company's behalf (e.g., vendors) and independent third parties who will use the data for their own purposes.</i></p> <p><i>Terms must comply with the original customer notice.</i></p> <p><i>For agents, contract must include a provision that prohibits use of PII for the agent's own independent purposes.</i></p> <p><b>7.1.11 Must meet any relevant legal requirements if data transfer will cross borders.</b></p>
--	---

## Scenario 8: Interacting with Children

### 8.1 Collect, Use or Disclose PII on a Web site or Online Service Directed at or Attractive to Children<sup>26</sup> or from Customers Known to be Children on a Web site that is not Directed at or Attractive to Children.

Examples include:

- Hosting a Web site intended to help elementary school children with their homework.
- Collecting a customer's age or birth date on a Web site that is not inherently attractive to children.

Category	Guidelines	
<b>Notice and Consent</b>	8.1.1	<p><b>Must<sup>27</sup> collect age of all customers if site or service is attractive to or directed at children and the site collects, uses, or discloses the customer's PII.</b></p> <p><i>Company should avoid collecting age if site or service is not directed at or attractive to children.</i></p> <p><i>Any age collection/screening UI must be neutral (i.e. must not warn that children's access will be blocked).</i></p>
	8.1.2	<p><b>Must either block PII collection and disclosure, or notify parent and obtain parental consent prior to collection, use, or disclosure of customer's PII, if Company has actual knowledge that a customer is a child regardless of whether the site or service is directed at or attractive to children.</b></p> <p><i>Some PII such as the child's name and parent's e-mail address may be collected from the child and stored at the Company for a limited period of time while awaiting parental consent. If consent is not granted, the PII must be deleted.</i></p> <p><i>When obtaining parental consent, must use a Company Approved mechanism, such as requiring the parent to enter a credit card number.</i></p> <p><i>A site or service that could allow a child to disclose PII to others, such as instant messaging or chat rooms is considered a form of disclosure.</i></p>
<b>Security and Data Integrity</b>	8.1.3	<p><b>Must block PII collection and disclosure after age has been collected if parental consent cannot be obtained.</b></p> <p><i>A common method for blocking is to set a session cookie.</i></p> <p><i>Message about the denial must be neutral so the child does not know denial was due to age.</i></p>
<b>Customer Access and Controls</b>	8.1.4	<p><b>Must provide parents reasonable access to information collected from their children.</b></p> <p><i>When providing access, must use a Company Approved mechanism that reasonably verifies the person seeking access is the parent or legal guardian of the child.</i></p> <p><i>In countries where providing parental access is not legally required, Company should balance the privacy rights of the child with the interests of safety and parental rights.</i></p>
<b>Additional Requirements</b>	8.1.5	<p><b>Must obtain Company Approval before knowingly collecting PII from children.</b></p>

<sup>26</sup> The age at which special privacy protections should be provided for children varies by jurisdiction. For example, it is under 13 in the United States and under 14 in South Korea and Spain.

<sup>27</sup> The guidelines described are mandated by law in certain jurisdictions (e.g., South Korea, Spain, and the United States). For other jurisdictions, these guidelines are recommended.

	<p><b>8.1.6</b> Must follow the requirements in Scenario 5 if deploying a Web site.</p> <p><b>8.1.7</b> Must following the requirements in Scenario 1 if collecting PII.</p>
--	--

## Scenario 9: Server Deployment<sup>28</sup>

### 9.1 Installation in an Enterprise

Category	Guidelines
Notice and Consent	<p><b>9.1.1 Must disclose any known privacy implications for server features (e.g., in a deployment guide).</b></p> <p><i>The target audience for this notice is an administrator, not individual end users like internal employees or external customers. The material is to help the enterprise understand the privacy impacting behavior, properly configure the software or service, and, if necessary, craft a privacy notice that is targeted at its end users (e.g., a notice in the employee handbook).</i></p>
	<p><b>9.1.2 Should consider identifying or providing a mechanism for the enterprise to display a privacy statement to its end users.</b></p> <p><i>For example, via a "View Privacy Statement" option under the help menu that presents the enterprise's privacy statement.</i></p>

### 9.2 Storage of User Data in an Enterprise

Category	Guidelines
Enterprise Controls	<p><b>9.2.1 Must identify or provide a mechanism that allows a System Administrator to restrict overall access to data stores, such as files, databases, or the registry, which contain User Data.</b></p>
	<p><b>9.2.2 Must identify or provide a mechanism that allows an Application Administrator to protect stored User Data from unauthorized Instance Administrators.</b></p> <p><i>For example, if data stored in a certain directory should only be accessible to one Instance Administrator, other Instance Administrators should not have access to that directory.</i></p>
	<p><b>9.2.3 Must identify or provide a mechanism for an Instance Administrator to protect stored User Data.</b></p> <p><i>For example, if data stored in a certain directory will be automatically indexed for search, the Instance Administrator should be given a means to prevent data on its site from being indexed.</i></p>
	<p><b>9.2.4 Should provide or identify a mechanism to help an Instance Administrator prevent disclosure of User Data.</b></p> <p><i>For example, providing the ability to set site permissions that prevent unauthorized access to User Data.</i></p>

### 9.3 Transfer User Data outside the Enterprise Firewall

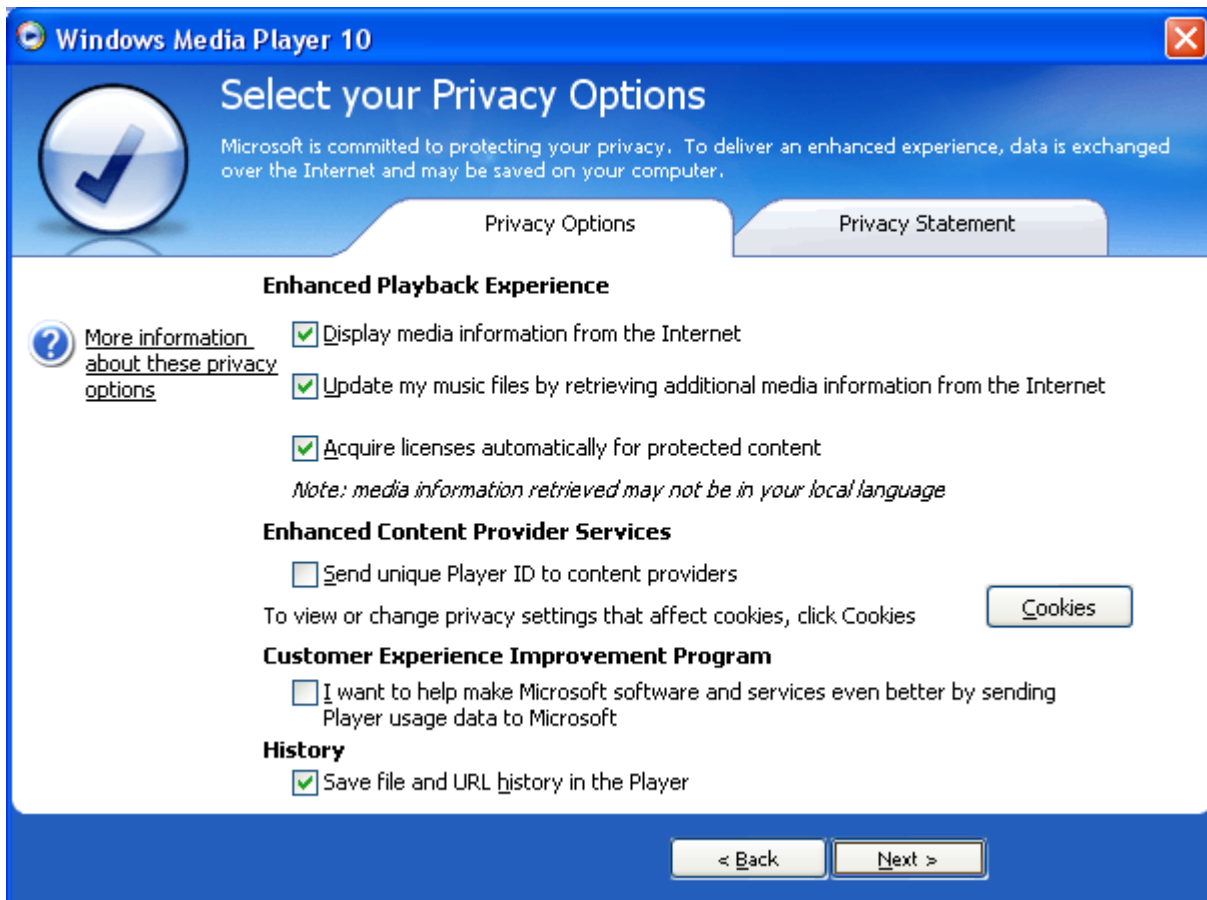
Category	Guidelines
Notice and Consent	<p><b>9.3.1 Must get Opt-In Explicit Consent from an Application or System Administrator prior to transfer of data from the server over the Internet.</b></p>

<sup>28</sup> Please note that Scenarios 1-9 also apply to server software. When applying those guidelines consider the case where the administrator is acting as the customer.

	<p><i>Includes both ongoing and one-time transfers of data.</i></p> <p><i>If the System Administrator has consented to the transfer, Application Administrators do not need to Opt-In.</i></p> <p><i>Application Administrators may provide Opt-In Consent if the System Administrator has not blocked the transfer.</i></p> <p><i>Automated ongoing transfer does not require additional authorization from end users of the server software once an administrator has consented.</i></p>
<b>Enterprise Controls</b>	<p><b>9.3.2 Should provide or identify a mechanism such as group policy that allows an Application or System Administrator to manage distribution of data outside of the organization or firewall.</b></p>

# Appendix A

The following screen depicts the Windows Media Player 10 privacy experience that is presented to each customer the first time they run the player:



## **Appendix B**

# **Security and Data Protection<sup>29</sup>**

Every company should adopt a reasonable standard for protecting customer, employee, partner and proprietary information. Key factors to consider include the types of data the organization processes, legal and industry regulations, and customer expectations.

Data protection begins with understanding the data that the organization collects, stores, or transfers. The data should then be grouped into data categories (e.g., Sensitive PII, PII, or Anonymous)<sup>30</sup> and the data owners identified. The data owner is the person or people responsible for ensuring that the data protection standard is followed for each set of data.

Data protection should consider several areas including access controls, encryption in transfer and storage, physical security, disaster recovery, and auditing. We will look at each of these areas in more detail below.

### **Access Controls**

Access to data in an organization should be based on the specific job function and role of the individual. Individuals should only have access to the data needed to complete their business functions. For example, a market researcher may need access to demographic information stored on a CRM server, but likely does not need access to personal data records. Access can be controlled by limiting the information the market researcher can access, or by providing a tool on top of the database that provides access to only aggregate demographic data. Other access controls include requiring each individual user to have a unique account, disabling anonymous login, enforcing strong password requirements<sup>31</sup>, and following access review and revocation policies. Logging account access and usage, and conducting periodic audits also contribute to a strong access control policy.

### **Encryption in Transfer and Storage**

Encryption masks data in order to help prevent unauthorized visibility during transfer or in storage. The data is then only visible to authorized users who possess the decryption key. Whether to encrypt data in transfer and storage is a business decision that is influenced by various factors, legal and other. For example, if a privacy statement indicates that PII is safeguarded, PII should be encrypted when it is transferred over the Internet. Sensitive PII, such as credit card numbers, should always be encrypted when transferred over the Internet.

Whether to encrypt data in storage depends on the nature of the data and the potential consequences of a breach. Sensitive PII by its very nature needs to be handled more carefully than non-sensitive PII, including additional security precautions. For some Sensitive PII, there

---

<sup>29</sup> Last updated April 2007.

<sup>30</sup> Data protection standards and information security programs often cover additional confidential and proprietary information, in addition to protecting personal information of customers and employees. Full information security practices are beyond the scope of this document.

<sup>31</sup> An example of strong password criteria is requiring a combination of upper, lower, and special character, non-sequential passwords over 8 characters in length containing no personal information and changed every 60 days.

are legal consequences associated with a failure to encrypt. For example, a number of states currently require notification if a security breach occurs on a machine storing name in conjunction with U.S. Social Security Number or other enumerated Sensitive PII where either name or the Sensitive PII is unencrypted.<sup>32</sup> Additionally, recent FTC actions indicate there is an obligation to keep personal information secure.<sup>33</sup> Contractual obligations may also come into play. When displaying account numbers, Visa and MasterCard require their partners to mask all but the first 6 and last 4 digits unless there is a specific and immediate need to see the full credit card number.<sup>34</sup>

An organization's data protection standard should include a combination of encryption strategies. Some examples of encryption strategies are:

- Require encryption at an appropriate level for the contents of data on remote VPN access to your internal servers (e.g., 128-bit).
- Configure Secure Sockets Layer (SSL) security features on your Web server to encrypt network transmissions. SSL can also help users verify that they are connected to your site, not a spoofed site.
- Use the strongest encryption protocol available (e.g., using WPA instead of WEP)<sup>35</sup> to prevent eavesdropping on your Wireless network.
- Implement a policy to encrypt locally stored files or individual data fields containing high value or sensitive data, or require full volume encryption on laptops and desktops to protect against data loss if hardware is stolen.

## Physical Security

The physical security of data must also be considered. Locking workstations, building security, hardware reuse policies and paper and media shredders, are all important aspects of helping to ensure that data is not accessed by unauthorized individuals.

## Disaster Recovery

Protecting against data loss and loss of data integrity by ensuring the ability to recover from system failure, natural disasters, or other emergencies is another aspect of data protection. Guidelines for scheduling and maintaining system and application backups, replicating data across multiple drives (e.g., implementing RAID Level 5)<sup>36</sup>, incident response planning, and a data retention policy are key aspects of disaster recovery. Physical and electronic access to backups must also be considered. The disaster recovery measures implemented should be appropriate for the value of the data stored. See [Additional Resources](#) for links to more information.

---

<sup>32</sup> California Civil Code Section 1798.29

<sup>33</sup> The Federal Trade Commission's Privacy Initiatives Unfairness & Deception Enforcement page outlines a number of cases: [http://www.ftc.gov/privacy/privacyinitiatives/promises\\_enf.html](http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html).

<sup>34</sup> From the [Visa Payment Card Industry Security Audit Procedures](#).

<sup>35</sup> Wi-Fi Protected Access (WPA) uses a 128-bit key and a 48-bit initialization vector (IV) to form the RC4 traffic key. Wired Equivalent Privacy (WEP) uses a 40 bit key and a 24-bit IV. One crucial improvement in WPA is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used. With the much larger IV, this defeats key recovery attacks on WEP.

<sup>36</sup> Redundant Array of Independent Disks (RAID) Level 5 uses block-level striping with parity data distributed across all disks. A minimum of 3 drives are required to implement.

## **Auditing**

It is important to note that industry standard security practices are continually updated based on changes in technology and in methods of attack. A robust plan must contain guidelines for regular review and audit of the standard and its implementation. Part of updating the standard is also updating software and technologies in order to stay ahead of evolving threats.

## **Conclusion**

A security standard that helps to protect data must consider all aspects of data protection, including, but not limited to, access controls, data encryption in transfer and storage, physical security, disaster recovery, and auditing. Implementing a security standard that considers data protection from all angles is essential to protecting critical business data from compromise and loss.

## **Additional Resources:**

- Microsoft Security Home Page:
  - <http://www.microsoft.com/security/guidance/default.aspx>
- Microsoft Small Business Security Guidance Center
  - <http://www.microsoft.com/smallbusiness/support/computer-security.aspx>
- National Institute of Standards and Technology (NIST)
  - <http://www.nist.gov>
- Forum of Incident Response and Security Teams (FIRST)
  - <http://www.first.org/>

## Appendix C

### User Data Examples

Examples of User Data are summarized in the table below:

<b>Anonymous Data</b>	<p>Any User Data that:</p> <p>(a) Is not unique or tied to a specific person (i.e. cannot be traced back) such as:</p> <ul style="list-style-type: none"> <li>• Hair color</li> <li>• System configuration</li> <li>• Method by which product was purchased (retail, online, etc)</li> <li>• Usage statistics distilled from a large collection of customers</li> </ul> <p><b>Note that if this information is associated with PII, it must also be treated like PII</b></p>
<b>Pseudonymous Data</b>	<p>Any User Data that:</p> <p>(a) identifier that is not tied to PII, but is being used as a means to identify distinct users, such as:</p> <ul style="list-style-type: none"> <li>• GUIDs</li> </ul> <p><b>Note that if this information is associated with PII, it must also be treated like PII</b></p>
<b>PII</b>	<p>Any User Data that:</p> <p>(a) Uniquely identifies a customer such as:</p> <ul style="list-style-type: none"> <li>• Contact information (e.g., name, address, phone number, e-mail address)</li> </ul> <p>(b) Is commingled or correlated with the customer’s PII. For example, demographics stored with the customer’s PII or with a unique ID that can be linked to the customer’s PII</p> <p>(c) Is Sensitive PII as described below</p>
<b>Sensitive PII</b>	<p>Any User Data that:</p> <p>(a) Identifies an individual and could facilitate identity theft or fraud, such as:</p> <ul style="list-style-type: none"> <li>• Some government issued ID numbers (e.g., Social Security Number)</li> <li>• Credit card numbers</li> <li>• Bank account numbers</li> </ul> <p>(b) Is commingled or correlated with PII and used as a credential, such as:</p> <ul style="list-style-type: none"> <li>• Passwords and PINs</li> <li>• Biometrics (when used to authenticate)</li> <li>• Mother’s maiden name</li> </ul> <p>(c) Is commingled or correlated with PII and could be used to discriminate or is legally defined as sensitive<sup>37</sup> such as:</p> <ul style="list-style-type: none"> <li>• Sexual preference/sexual lifestyle</li> <li>• Beliefs (e.g., political, religious, or philosophical)</li> <li>• Ethnicity and race</li> <li>• Trade union membership</li> <li>• Medical history or health records</li> <li>• Financial information</li> </ul> <p>(d) Is collected by the system and could hold Sensitive PII, such as:</p> <ul style="list-style-type: none"> <li>• A raw memory dump</li> </ul>

<sup>37</sup> For example, as indicated by Article 8 of the EU Data Protection Directive (95/46/EC).