Genuine Microsoft Software Program Privacy Statement

Last updated: February 2010

Microsoft is committed to protecting your privacy and helping protect its customers and partners from counterfeit software. Using a properly licensed, genuine copy of Microsoft software helps to ensure you will have access to all the latest features and updates from Microsoft.

The Genuine Microsoft Software program (referred to as “Windows Genuine Advantage” in Windows XP and “Windows Activation Technologies” in Windows Vista and Windows 7) tools include:

■Validation, which determines whether you are running a properly licensed copy of Microsoft software. Validation will detect and may disable "activation exploits", which is software that circumvents or bypasses Microsoft product activation, validation, or licensing components. The presence of activation exploits indicates that a software or hardware vendor may have tampered with genuine Microsoft software to enable the sale of counterfeit software. Activation exploits may interfere with the normal operation of your software.

■Notifications, which display periodic reminders such as whether there is a problem with your Windows license components or whether a more recent service pack is available for your Windows software. At this time, the Notifications component is offered on Windows XP, Windows Vista, and Windows 7, and in select countries, on Office XP, Office 2003 and Office 2007.

■The Windows Activation Exploit Detection Update for Windows Vista and the Update to Activation Technologies for Windows 7 are used to detect activation exploits. These updates check your computer for known activation exploits and notify you if any activation exploits are found.

To effectively encourage the use of properly licensed software, these tools are designed to be a permanent part of the Microsoft software.

What data is collected?

To help you validate your software, Genuine Microsoft Software tools must collect a certain amount of configuration and status information from your computer. The tools do not collect your name, address, e-mail address, or any other information that Microsoft will use to identify you or contact you.

The tools collect information such as:

■Computer make and model

■Version information for the operating system and software

■Region and language settings

■A unique number assigned to your computer by the tools (Globally Unique Identifier or GUID)

■Product Key (hashed) and Product ID

■BIOS name, revision number, and revision date

■Hard drive volume serial number (hashed)

■Whether the installation was successful if one was performed

■The result of the validation check, including error codes and information about any activation exploits and any related malicious or unauthorized software found or disabled, including:

◦The activation exploit’s identifier

◦The activation exploit's current state, such as cleaned or quarantined

◦Original equipment manufacturer identification

◦The activation exploit’s file name and hash of the file, as well as a hash of related software components that may indicate the presence of an activation exploit

■The name and a hash of the contents of the computer's start-up instructions file (commonly called the boot file) to help us discover activation exploits that modify this file.

As standard procedure, your Internet Protocol (IP) address is temporarily logged when your computer connects to a Genuine Microsoft Software website or server. These logs are routinely deleted.

Software piracy is a worldwide problem. To help spot possible systematic abuse of product licenses, certain information about the computer being validated is derived from its IP address. This information includes geographical location, ISP (Internet service provider) and domain name. The smallest geographical unit that can be resolved is a city. This resolution is done using data provided from a third party.

When is data collected?

Genuine Microsoft Software tools collect the configuration and status data described above at the following intervals:

■For machines running Windows Vista SP1 and later service packs, data is collected after the Windows Activation Exploit Detection Update for Windows Vista is installed. In addition, data is collected and sent to Microsoft every 30 days even if no activation exploit is detected; no data is sent from Windows Vista RTM.

■For machines running Windows 7, data is collected after the Update to Windows Activation Technologies for Windows 7 has been installed. In addition, data is collected and sent to Microsoft every 90 days even if no activation exploit is detected. However, if the Update to Windows Activation Technologies for Windows 7 finds that essential Windows files have been tampered with, then data collected from that machine will be sent every 7 days until Windows becomes genuine.

Note: Details about data collected during activation of Microsoft software can be found in the privacy statement for that product.

How is this data used?

We use the information to:

■Help prevent improperly licensed use of the software

■Improve our software and services

■Develop aggregate statistics.

We may also share aggregate data with others, such as hardware and software vendors and volume licensees to help protect their license keys.

What controls are available?

Users may customize some aspects of the Notifications component on Windows XP. If the component is installed, right-click the Notifications icon in the system tray for more information on available controls.

Changes to the Privacy Statement

We may occasionally update this privacy statement. When we do, we will revise the "last updated" date at the top of the privacy statement. We encourage you to periodically review this privacy statement to be informed of how Microsoft is protecting your information.

For More Information

If you have questions about this privacy statement, please contact us by using our web form at <http://go.microsoft.com/fwlink/?LinkId=83260>.

Microsoft Privacy

Microsoft Corporation

One Microsoft Way

Redmond, Washington 98052