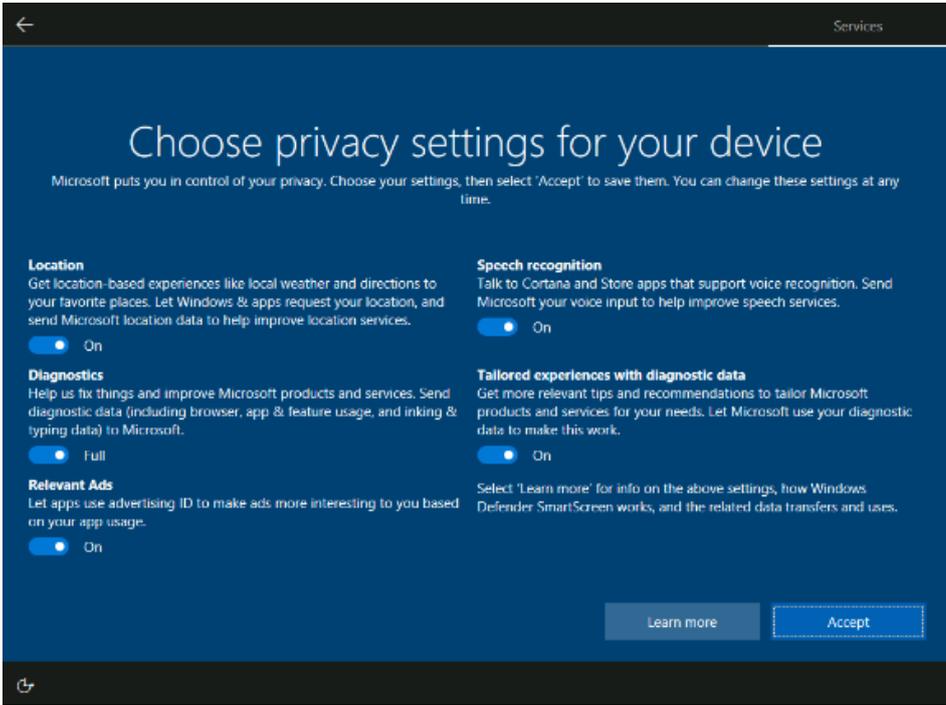
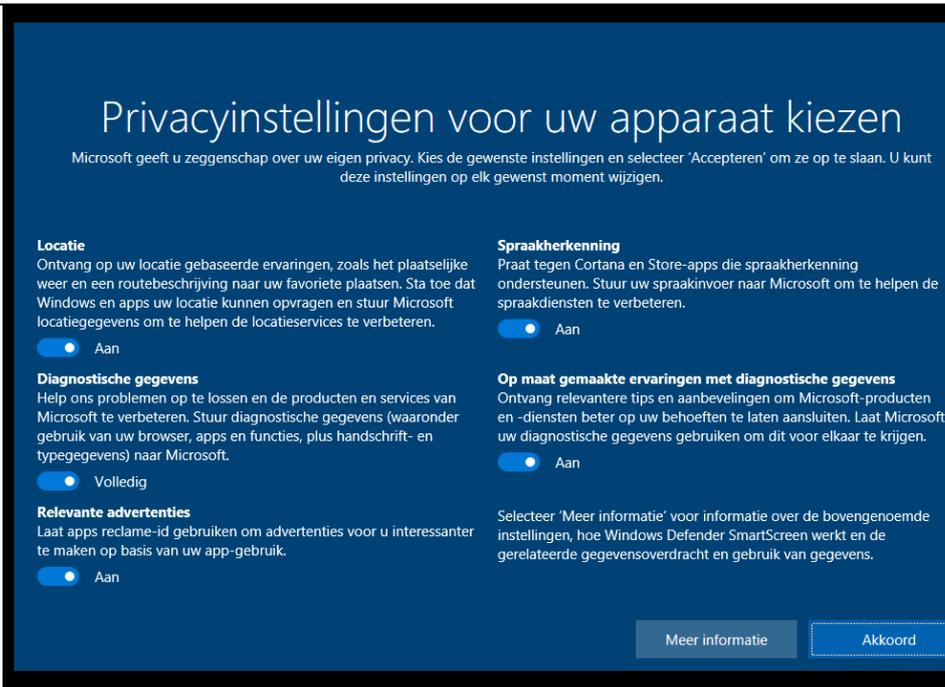
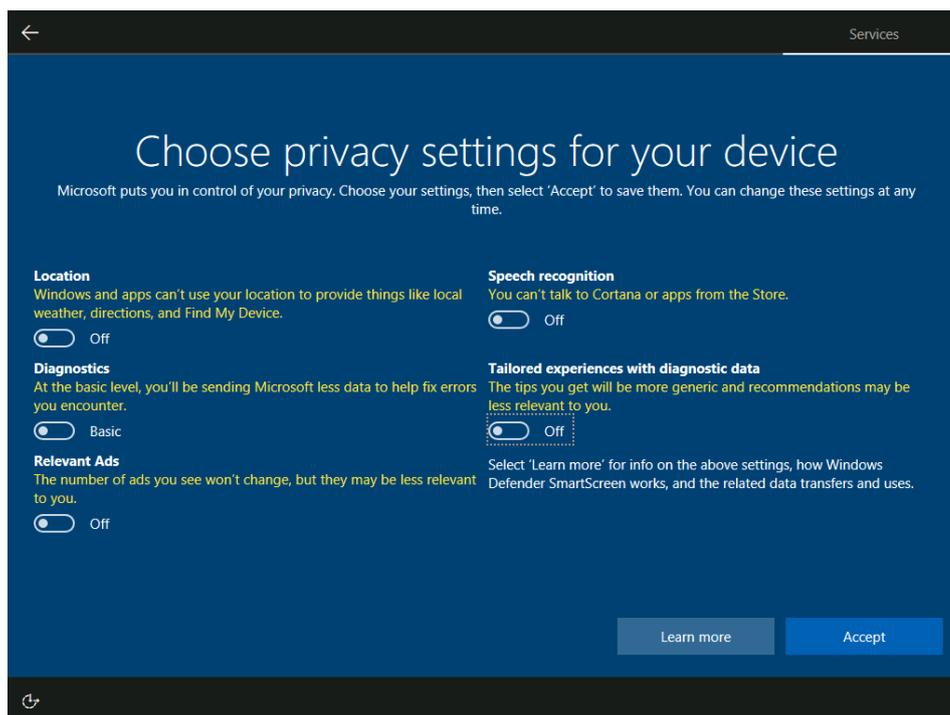


Dutch DPA Windows 10 Home/Pro Investigation: Microsoft Fact Sheet

The Dutch DPA's Announcement	Microsoft Comments
<p>Microsoft does not clearly inform users about the type of data it uses, and for which purpose.</p>	<p>➤ Microsoft informs Windows 10 users about the data we collect and how it is used in a variety of ways. For example, in the Creators Update and the upcoming Fall Creators Update Windows 10 users can learn about their privacy choices and controls through:</p> <ul style="list-style-type: none"> • The text and toggles in the user experience, which includes (i) the Privacy Choices Screen presented to users when they install or upgrade to the Creators Update or Fall Creators Update (see screen shot below) and (ii) the general Windows 10 Privacy Settings experience (see screen shot below). • The Learn more documents, which provide more detailed information about users' privacy choices and supplement the text provided in the user experience. These documents are available to users when they make privacy choices in Windows 10; • The Microsoft Privacy Statement, which provides more detail about Windows 10 privacy choices and controls, along with information about Microsoft's privacy practices, generally; and • Windows 10 in blogs and other documentation we publish. <p>➤ We publish a document which lists all types of data collected in Windows diagnostics (called telemetry data in the Dutch DPA's announcement), with comprehensive examples of each type on our Windows IT Pro site (available here).</p> <p>➤ We also publish an even more detailed list of every data item collected in Basic telemetry (available here).</p> <p>Privacy Choices Screen – On/Full (English & Dutch):</p> 



Privacy Choices Screen- Off/Basic (English & Dutch):



Privacyinstellingen voor uw apparaat kiezen

Microsoft geeft u zeggenschap over uw eigen privacy. Kies de gewenste instellingen en selecteer 'Accepteren' om ze op te slaan. U kunt deze instellingen op elk gewenst moment wijzigen.

Locatie

Windows en apps kunnen uw locatie niet gebruiken om functies als het plaatselijke weer, routebeschrijvingen en Mijn apparaat zoeken te bieden.

Uit

Diagnostische gegevens

Op basisniveau zult u Microsoft minder gegevens toesturen om u te helpen fouten die u tegenkomt op te lossen.

Standaard

Relevante advertenties

U ziet hetzelfde aantal advertenties, maar ze zijn misschien minder relevant voor u.

Uit

Spraakherkenning

Vanuit de Store kunt u niet tegen Cortana of apps praten.

Uit

Op maat gemaakte ervaringen met diagnostische gegevens

De tips die u krijgt, zullen meer algemeen van aard zijn en de aanbevelingen kunnen minder relevant voor u zijn.

Uit

Selecteer 'Meer informatie' voor informatie over de bovengenoemde instellingen, hoe Windows Defender SmartScreen werkt en de gerelateerde gegevensoverdracht en gebruik van gegevens.

Meer informatie

Akkoord

General Privacy Settings Experience (English & Dutch). Note, this images do not show all the privacy choices users can make.

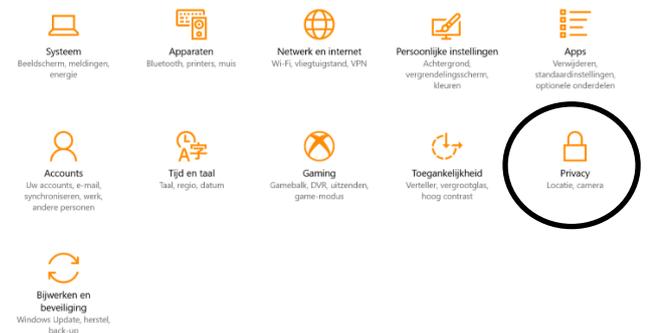
Windows Settings

Find a setting

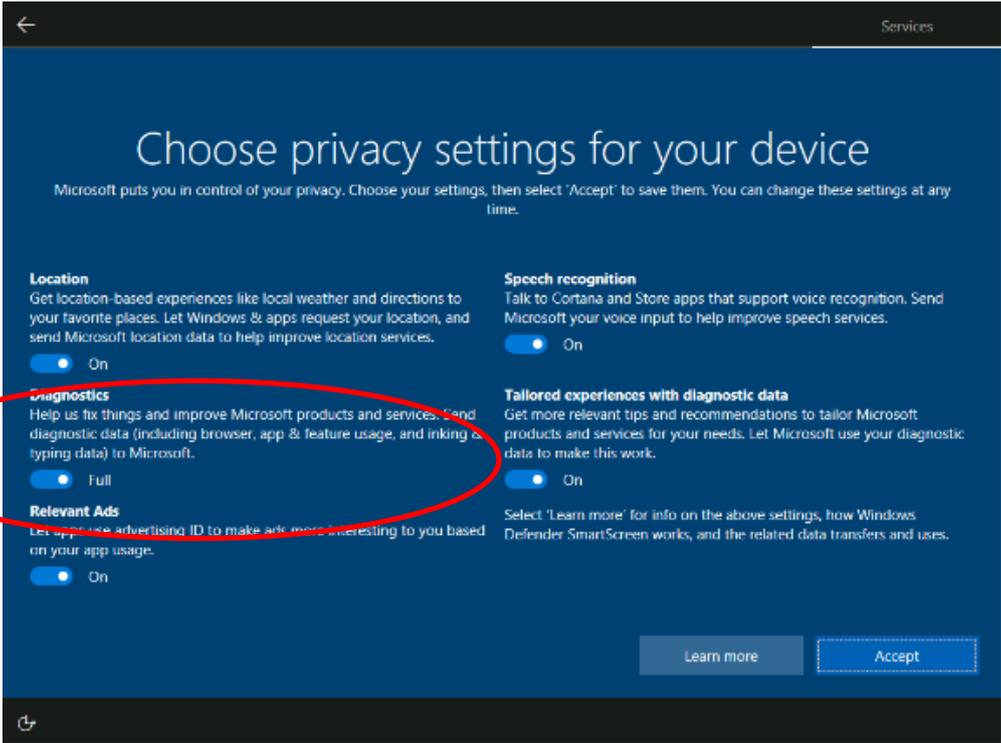


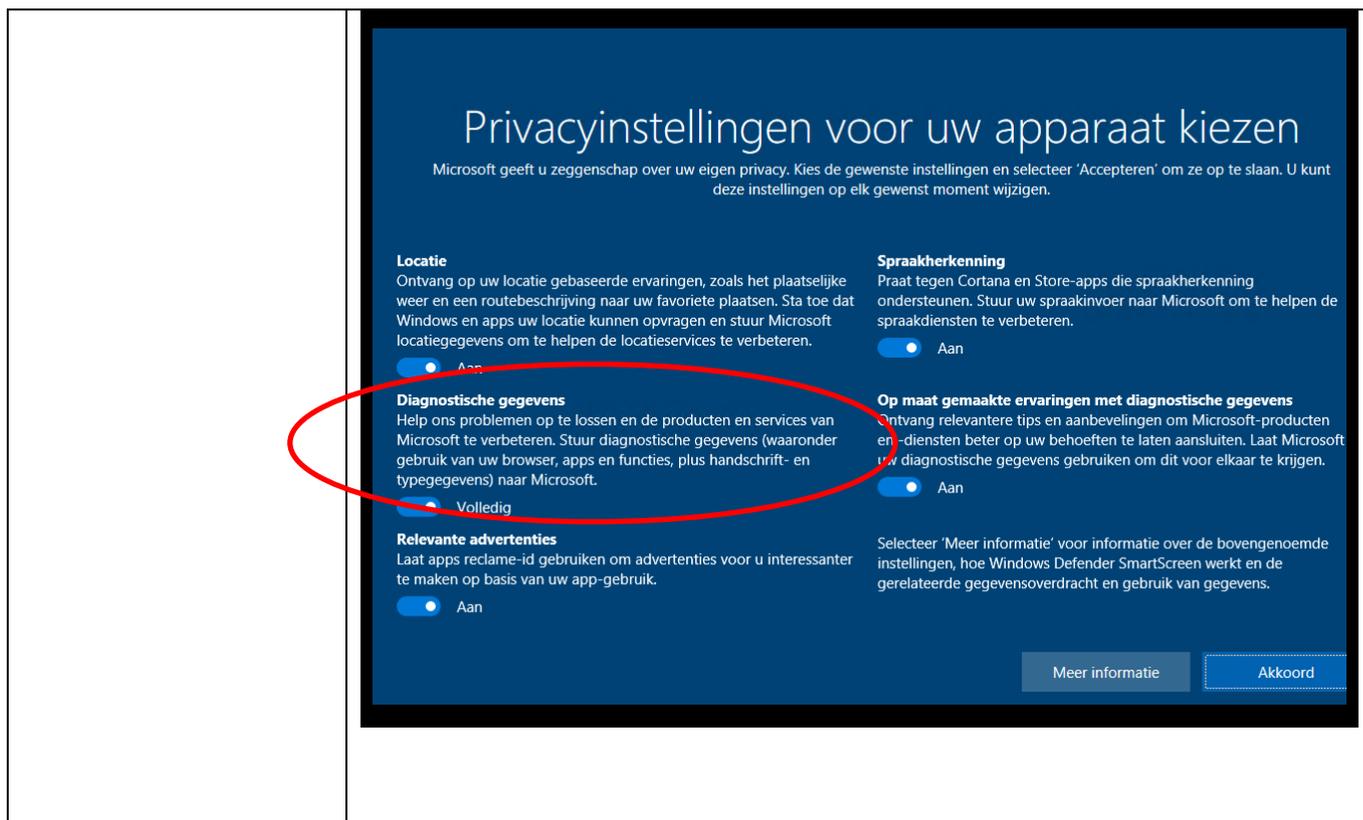
Windows-instellingen

Instelling zoeken



<p>[P]eople cannot provide valid consent for the processing of their personal data, because of the approach used by Microsoft..</p> <p>Due to Microsoft's approach users lack control of their data..</p>	<ul style="list-style-type: none"> ➤ When the Dutch DPA refers to the approach used by Microsoft they are referring to the operations and oversight of the Windows 10 diagnostics program. ➤ As we use diagnostics data to quickly respond to threats and performance issues, our engineers need the ability to gather data when investigating an issue impacting the Windows ecosystem. ➤ Today, Windows engineers who demonstrate a business need, consistent with legitimate uses of data, can collect new diagnostics data. These engineers have robust privacy and security training and must operate under rigorous controls. For example, engineers seeking to add any new types of data to telemetry must get approval from a cross group team, with privacy experts and lawyers. ➤ The Dutch DPA claims we cannot obtain lawful consent given the flexibility of our telemetry program, since the data we collect can change over time. Though we disagree with this, we plan to collaborate with the Dutch DPA to discuss key aspects of our data processing operations and implement improvements.
<p>They are not informed which data are being used for what purpose, neither that based on these data, personalised advertisements and recommendations can be presented, if those users have not opted out from these default settings on installation or afterwards.</p>	<ul style="list-style-type: none"> ➤ We tell users the purposes for which we process their data in the Windows 10 user interface (text/toggles), in the Learn more documents, in the Microsoft privacy statement and in other materials. ➤ We have been transparent about the fact that we do process diagnostic data for personalization (we want our users to get the best out of Windows 10 so they enjoy using it), depending on how a user configures her privacy settings. ➤ We have worked hard to make it easy for a user to make choices about personalization in Windows 10. For example, we've updated the privacy settings experience to provide the Privacy Choices Screen for the Creators Update and Fall Creators Update, which simplifies users privacy choices.

	<ul style="list-style-type: none"> ➤ Starting with the Creators Update, users can choose to receive Tailored Experiences. If users enable Tailored Experiences, Microsoft will use their diagnostic data (whether that is Basic or Full) to personalize their Windows 10 experience. For example, we may use the data to provide recommendations. ➤ Starting with the Creators Update, users can choose to receive Relevant Ads. If users enable Relevant Ads, which activates the Advertising ID, apps can use the Advertising ID to provide personalized ads in apps. If users disable Relevant ads, the user will still see advertising in apps; those ads, though, will not be personalized. This setting does not control the collection or use of Windows diagnostic data in any way. Turning this setting on does not enable the use of Windows diagnostics for advertising in apps.
<p>The company does not clearly inform users that it continuously collects personal data about the usage of apps and web surfing behaviour through its web browser Edge, when the default settings are used..</p>	<ul style="list-style-type: none"> ➤ We inform users in the Privacy Choices Screen about this data collection, as described above. If the user does not interact with the toggles on the Privacy Choices Screen (see below), for diagnostic data it reads: "Help us fix things and improve Microsoft products and services; send diagnostic data (including browser, app and feature usage, and inking & typing data) to Microsoft." If the user selects "Accept" on this screen, Microsoft will collect data about the use of apps and surfing behavior through the Microsoft Edge browser. ➤ Users can change their privacy settings at any time when using Windows 10. 



<p>Microsoft has indicated that it wants to end all violations</p>	<ul style="list-style-type: none"> ➤ We look forward to an opportunity to discuss with the Dutch DPA potential solutions to address their concerns.
<p>Microsoft continuously collects technical performance and user data (e.g. which apps are installed and, if the user has not changed the default settings, how often apps are used, as well as data on web surfing behaviour) from these devices. These data are called 'telemetry data'.</p>	<ul style="list-style-type: none"> ➤ Windows 10 is a uniquely diverse ecosystem. There are many millions of combinations of hardware devices, peripherals and drivers that operate on Windows devices, providing core functionality for hundreds of millions of people. There are also more than 20 million software applications that operate on Windows 10. And this number is growing as more software apps continue to be developed. ➤ Microsoft collects diagnostic data to understand how Windows 10 devices are performing and how they are used. Without the ability to “see” all these combinations, through the collection of diagnostic data, Microsoft would not be able to discern that a particular operating system update could be deployed without creating a compatibility issue for computers with unique combinations of hardware and software. For this reason, Microsoft collects information about each device. Knowing this information enables Microsoft to successfully provide a modern Windows computing experience to all customers and for all types and configurations of Windows devices. ➤ Microsoft needs to collect information on users devices to provide a secure computing environment. <ul style="list-style-type: none"> ○ An important reason Microsoft collects reliability data from the operating system and all Windows apps (not just apps we ship with the operating system) is that crashing apps are often an indicator of a security breach or attempted security breach as malicious software attempts to inject itself into running processes. ○ Understanding which apps are installed and used on Windows devices enables the ability to assess potential impact and to address vulnerable devices quickly, protecting individual Windows devices and the broader network, including the public internet from harm and malicious intent.

	<ul style="list-style-type: none"> ➤ If the user does not interact with the toggles on the Privacy Choices Screen (see below), for diagnostic data it reads: “Help us fix things and improve Microsoft products and services; send diagnostic data (including browser, app and feature usage, and inking & typing data) to Microsoft.” If the user selects “Accept” on this screen, it’s true that we will collect data about the use of apps and surfing behavior through the browser Edge. ➤ Users can change their privacy settings at any time when using Windows 10.
<p>With telemetry Microsoft – as it were – takes pictures of the behaviour of Windows users, and continuously sends these pictures to itself.</p>	<ul style="list-style-type: none"> ➤ Windows 10 diagnostic data is primarily highly technical data about a product or service - data that in many cases is not interesting to the user and reveals very little or nothing about her. ➤ Diagnostic data is, by its nature, data about a thing: data about a driver, a device, software, or an app. ➤ This kind of device-based data is precisely the data required by Windows 10 to keep Windows 10 running properly, secure, and up-to-date in a diverse ecosystem. ➤ Even where diagnostic data can be linked back to an identified or identifiable individual, the data is usually not particularly revealing or private. Indeed, most of data collected by Windows 10 is very detailed and technical, and frankly quite boring. We collect data to learn, for example, that device XYZ123 is pen-enabled (meaning that the device has functionality which enables a user to input data with a digital “pen” or stylus), what driver a device has, or whether a device has a certain processor. ➤ While we understand that at least some of this data would be considered personal data under the data protection laws, we emphasize that most diagnostic data events are not designed to gather personal data. To the extent we do process personal data, we seek to treat such data properly under all applicable data protection laws. ➤ The documentation about diagnostics that we have provided to the public shows that most diagnostic data is device-based, highly technical, and largely mundane. <ul style="list-style-type: none"> ○ See the list of all the types of data we collect in Windows diagnostics on our Windows IT Pro site (available here). ○ And find an even more detailed listing of every data item we collect at Basic diagnostics (available here).
<p>It turns out that Microsoft’s operating system follows about every step you take on your computer. That results in an intrusive profile of yourself”, according to Wilbert Tomesen, vice-chairman of the Dutch DPA. “What does that mean? Do people know about this, do they want this? Microsoft needs to give users a fair opportunity to decide about this themselves.</p>	<p>See points above that describe the technical nature of diagnostic data.</p> <ul style="list-style-type: none"> ➤ Users can change their privacy settings at any time when using Windows 10. ➤ We provide users with the opportunity to make choices on five key privacy settings when the user upgrades or installs Windows 10 Creators Update or Fall Creators Update. ➤ (see screenshot above). Users are provided layers of information, accessed from the Privacy Choices Screen to inform their selections. ➤ For other privacy choices, users are given an opportunity to make choices in context. For example, when the user first uses the Camera app, she will be prompted to make choices about the collection and use of data associated with the camera functionality.

<p>With full telemetry also detailed data on app usage are processed as well as data about web surfing behaviour through Edge and (parts of) the content of handwritten documents via an inkpad.</p>	<p>With respect to the “content of handwritten documents”:</p> <ul style="list-style-type: none"> ➤ With Full diagnostic data, Microsoft collects small samples of inking and typing input, which is processed to remove identifiers, sequencing information, and other data (such as names, email addresses, and numeric values) which could be used to reconstruct the original content or associate the input to the user. In other words, Microsoft processes this data to enable us to use the information to improve input recognition but avoids retaining data that is personal or can be associated with a particular user. This data is never used for Tailored Experiences.
<p>If users have not opted out for these purposes upon installation or afterwards, then Microsoft also uses data from both the basic and the full telemetry level to show personalised advertisements in Windows and Edge (including all apps for sale in the Windows store)and is the Advertising ID used to show personalised advertisements in other apps.</p>	<ul style="list-style-type: none"> ➤ This is incorrect, as the Dutch DPA is mixing two separate privacy settings. ➤ If the user chooses to enable Tailored Experiences, Microsoft uses diagnostic data collected, whether Basic or Full, to personalize her experience in the Windows experience. ➤ If the user chooses to enable Relevant Ads, which means turning on use of the Advertising ID, personalized advertising will be shown in apps. This setting does not impact the collection or use of Windows diagnostics data in any way. ➤ When the Advertising ID is enabled, apps can access and use the advertising ID in much the same way that websites can access and use a unique identifier stored in a cookie. ➤ Turning on the Relevant Ads setting does not enable to use of Windows diagnostics data in connection with advertising in apps.
<p>Microsoft can use the collected data for the various purposes, described in a very general way. Through this combination of purposes and the lack of transparency Microsoft cannot obtain a legal ground, such as consent, for the processing of data.</p>	<ul style="list-style-type: none"> ➤ Microsoft is transparent about its uses of the diagnostic data it collects: Microsoft collects Windows diagnostic data to keep Windows up-to-date, secure, and operating properly. It also helps us improve Windows and, for users who have turned on “tailored experiences”, can be used to provide more relevant tips and recommendations to tailor Microsoft products to the user’s needs. ➤ Microsoft uses the collected data for more than one of the purposes we specify, when such use is compatible with the purpose for which the data was collected. For example, we may collect data to troubleshoot a reliability issues with Windows 10. If that data can also be used to improve a security feature of Windows, we may use it for that purpose as well.
<p>Microsoft offers users an overview of the categories of data that it collects through basic telemetry, but only informs people in a general way, with examples, about the categories of personal data it collects through full telemetry.</p>	<ul style="list-style-type: none"> ➤ In addition to information in the Privacy Statement, user settings and Learn More documents described above, we provided an exhaustive list of all the types of data we collect in Windows diagnostics, including at the Full level, on our Windows IT Pro site (available here).
<p>It is not made sufficiently clear that at the full telemetry level, Microsoft continuously collects data about the usage of apps and web surfing behaviour through Edge, including for example news articles that</p>	<ul style="list-style-type: none"> ➤ We disagree. A user can learn what is collected with Full telemetry by reading the text on the Privacy Choices screen, and reading information provided in the Learn more document easily accessible to the user when she makes her selections. ➤ If the user does not interact with the toggles on the Privacy Choices Screen (see below), for diagnostic data it reads: “Help us fix things and improve Microsoft products and services; send diagnostic data (including browser, app and feature usage, and

<p>have been read and locations entered into apps.</p>	<p>inking & typing data) to Microsoft.” To supplement the information on the screen, users can select “Learn More” to read more about what Microsoft collects with Full telemetry.</p> <ul style="list-style-type: none"> ➤ Users can change their privacy settings at any time when using Windows 10.
<p>Additionally, the Dutch DPA has established that Microsoft has not respected existing privacy choices from some users when they upgraded to the Creators Update. This applies to the people who downloaded the operating system themselves. If they had previously selected basic telemetry in a prior Windows version and did not actively change the privacy settings upon installation of the Creators Update, the settings were switched to full telemetry level.</p>	<ul style="list-style-type: none"> ➤ The majority of Windows 10 users who upgraded were prompted to choose settings for the Creators Update based on their existing privacy settings. These users waited to be offered the Creators Upgrade through the regular upgrade experience. ➤ A small minority of Windows 10 users who affirmatively sought out the new version with the Media Creation Tool, were prompted to choose settings based on the Microsoft’s standard defaults rather than their existing settings. . The Media Creation Tool is intended for tech-savvy users and is not the expected upgrade path for the average user. ➤ In either case, users were shown a consent dialogue with information about their choices regarding the same five settings and those choices were honored.