VANJA KORAĆ
Mathematical Institute SASA,
Kneza Mihaila 36/III,
Belgrade, Serbia,
e-mail: vanja@mi.sanu.ac.rs

MILAN TODOROVIĆ
Mathematical Institute SASA,
Kneza Mihaila 36/III, 11 000
Belgrade, Serbia,
E-mail: mtodorovic@mi.sanu.ac.rs

DRAGAN PRLJA
Institute for Comparative Law,
Terazije 41, Belgrade, Serbia,
e-mail: dprlja@yahoo.com

004.451.9WINDOWS
COBISS.SR-ID 228055308

Original research article
Received: April 17th 2016
Accepted: June 20th 2016

PRIVACY CONTROL ON WINDOWS 10

ABSTRACT

Just as with every information system, an organisation's policy focuses on the security questions of privacy control. This paper gives suggestions related to the information system of the archaeological site "Viminacium", necessary to the upgrade of its computer systems, in order to secure the demanded privacy of collecting data during the processing of digital archaeological data. Windows 10 contains complex settings regarding the privacy of its users. There will be information on settings recommendations regarding security on Windows 10 OS. Settings will be mentioned that can be chosen during installation, and further on there will be details regarding the switching off of certain hidden privacy settings, as well as a discussion about the advantages of using local accounts on Windows 10. There will also be mention made of Microsoft's use of users' Internet flow and ways of disabling it. At the end, there will be a section on the privacy problems related to the new features of Windows 10: the new Internet search-machine Edge and the personal assistant Cortana.

KEYWORDS: PRIVACY, PRIVACY CONTROL, WINDOWS 10 AND PRIVACY.

I INTRODUCTION[1]

When a new operating system is being installed, it is necessary to pay attention to privacy protection. In modern times, privacy can be defined as the right of a person to control information about him/her that is being collected, processed and given to third parties. Besides many positive effects, electronic communication has made it possible to observe people without them being aware of it and without their permission, following their activities and everything they type on the keyboard, again without their awareness or permission. Additionally, the storage and distribution of information collected about each person is possible, also without his/her awareness or permission. In such a way, an organisation or a person can find their privacy rights, guaranteed

[1] The article results from the project: *Viminacium, Roman city and military camp – research of material and non- material culture of inhabitants by using the modern technologies of remote detection, geophysics, GIS, digitalization and 3D visualization* (no 47018), funded by The Ministry of Education, Science and Technological Development of the Republic of Serbia.

under national and international law, endangered. Such rights specify that a person alone should determine when, how and in what quantity information about him/her, gained through electronic communication, will be accessible to others. This prerequisite for the gathering, processing and distribution of data about him/her is an explicit agreement in written, electronic or oral form. The latest legal regulation of the European Union, from May 2016, describes explicit, unambiguous, voluntary and special acceptance as a condition.[2] Privacy rights protect data and records connected to one's private life from being published, or from any kind of misuse (Vilić and Radenković 2015). On one hand, there are tendencies to protect one's privacy through national and international legislation as well as possible, but on the other hand, software producers and companies that earn money collecting, processing and distributing personal data, tend to collect as much data as possible, even when users do not give their unambiguous permission. The need for privacy protection is especially important for companies producing operating systems, since they are being used on a daily basis on every computer. The danger of collecting an owner's (private or legal entity) sensitive data, photos, codes and other information that he/she does not want to share, is always present with companies that produce Oss, and it is a very real danger. As a result of this, and in order to protect users, it is necessary to use all the possibilities offered by the OSs themselves, to protect privacy as well as possible from the very beginning, i.e. while the OS is being installed.

Further on in this paper, certain recommendations will be presented regarding privacy in Windows 10 OS, related to the information system of the archaeological site "Viminacium".

II RECOMMENDATIONS

1. Avoid using the express setting during installation

By choosing the express setting, the maximum sharing of users' information with Microsoft is enabled. Choosing the "custom install" option offers a larger number of keys for setting privacy in several sets. The first set, which enables the sending of personal data, should all be switched to "off".

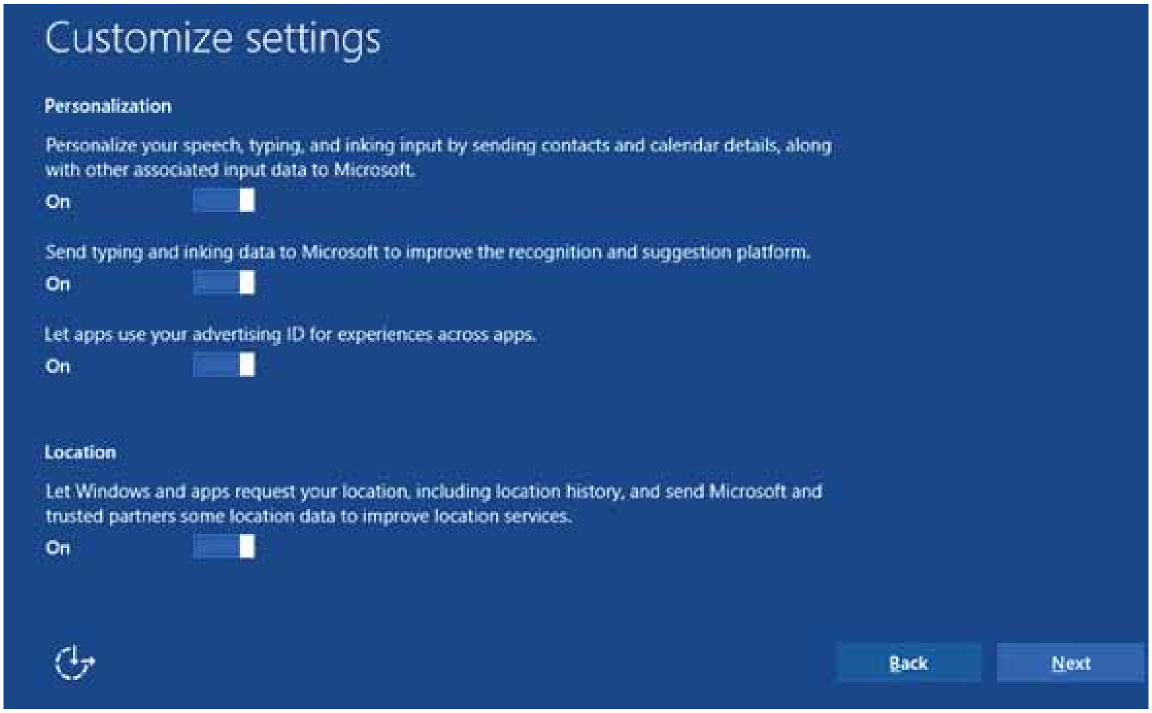
The second set of keys is more intriguing, but is rather important, so they should be switched off, in order to maintain privacy.

The first two options send additional activities to Microsoft, while the following two options are more subtle. These options enable automatic connections to open Hotspots and networks comprising the users' contacts!? The last option, for sending diagnostic information and error information, can be described as harmless. However, if a problem occurs, like a system crash, "information" that is sent could contain a large amount of sensitive data (if the user's computer broke down while working in Word or Excel, which could include confidential date, this would be uploaded onto the Microsoft server, along with error and diagnostic information).

2. Switching off hidden settings

Settings made while installing are just a subgroup of the privacy settings on the Windows 10 system, which contain a rather large number of pages and dialogues on the user interface that are not very visible. According to Auerbach (Auerbach 2015), in one of the dialogues during settings, Microsoft reveals its insincerity. Actually, when the user decides to switch off the options

[2] *Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data to the European Parliament and the European Council*, 2016/679, and *Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the prevention, investigation, detection, criminal offenses or the execution of criminal sanctions and on the free movement of such data to the European Parliament and the European Council*, 2016/680, http://ec.europa.eu/justice/data-protection/



Customize settings

Personalization

Personalize your speech, typing, and inking input by sending contacts and calendar details, along with other associated input data to Microsoft.

On

Send typing and inking data to Microsoft to improve the recognition and suggestion platform.

On

Let apps use your advertising ID for experiences across apps.

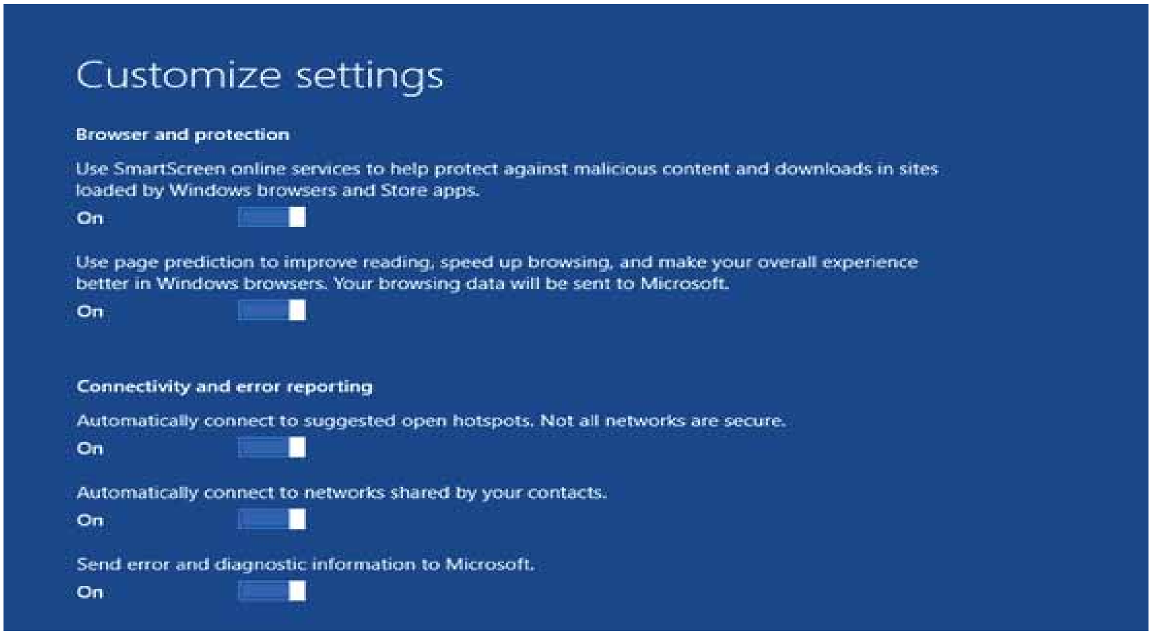
On

Location

Let Windows and apps request your location, including location history, and send Microsoft and trusted partners some location data to improve location services.

On

Fig. 1 The first set of keys that enable the sending of personal data



Customize settings

Browser and protection

Use SmartScreen online services to help protect against malicious content and downloads in sites loaded by Windows browsers and Store apps.

On

Use page prediction to improve reading, speed up browsing, and make your overall experience better in Windows browsers. Your browsing data will be sent to Microsoft.

On

Connectivity and error reporting

Automatically connect to suggested open hotspots. Not all networks are secure.

On

Automatically connect to networks shared by your contacts.

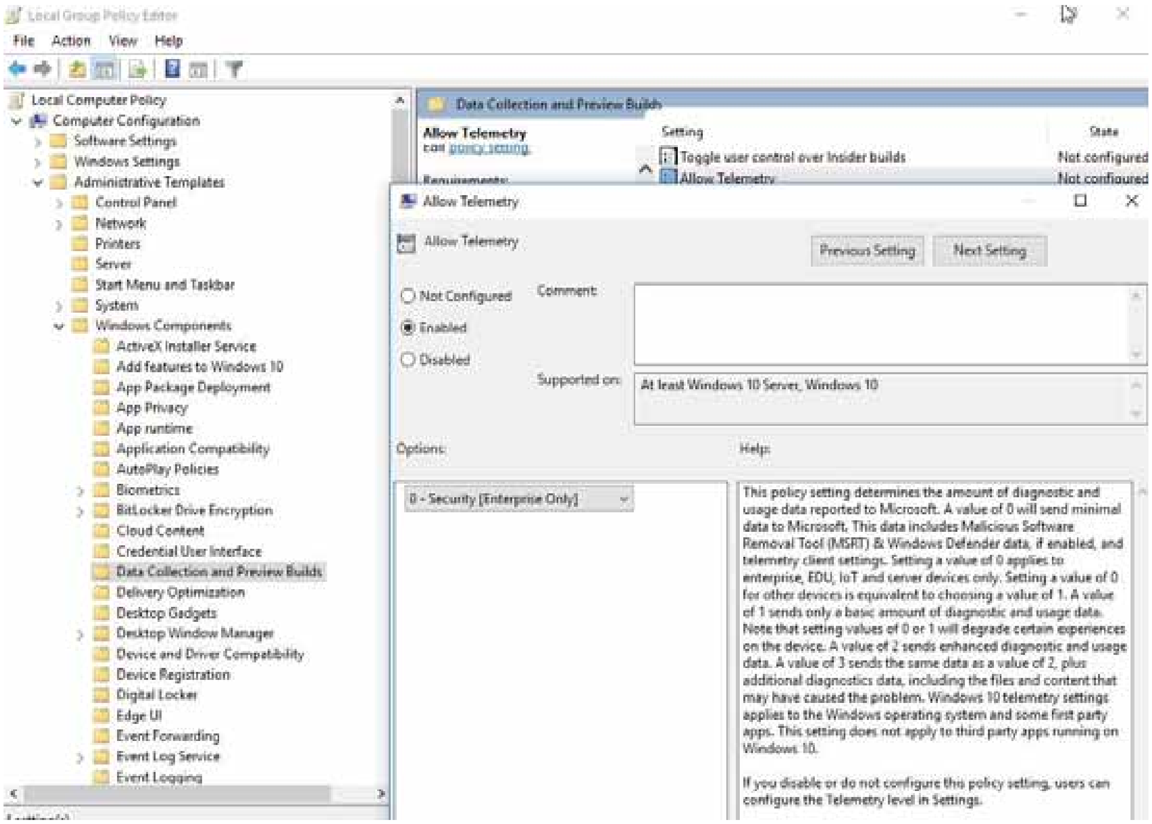
On

Send error and diagnostic information to Microsoft.

On

Fig. 2 The first set of keys that enable the sending of personal data

"sending diagnostic information and error information", the system limited sending information from FULL to enhanced. In order to truly reduce the sending of such information, it is necessary to go to Start menu- Settings, Privacy-Feedback and Diagnostics and choose the "Basic" option and reduce the sending of random data to Microsoft to a minimum (Fig. 4). Also set "Feedback frequency" to "never". It is necessary to mention that, apart from the "full, enhanced and basic" options, there is a fourth, hidden, option named "security". Of all the options, this sends the least data to Micro-



Allow Telemetry

Setting	State
Toggle user control over Insider builds	Not configured
Allow Telemetry	Not configured

Allow Telemetry

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 10 Server, Windows 10

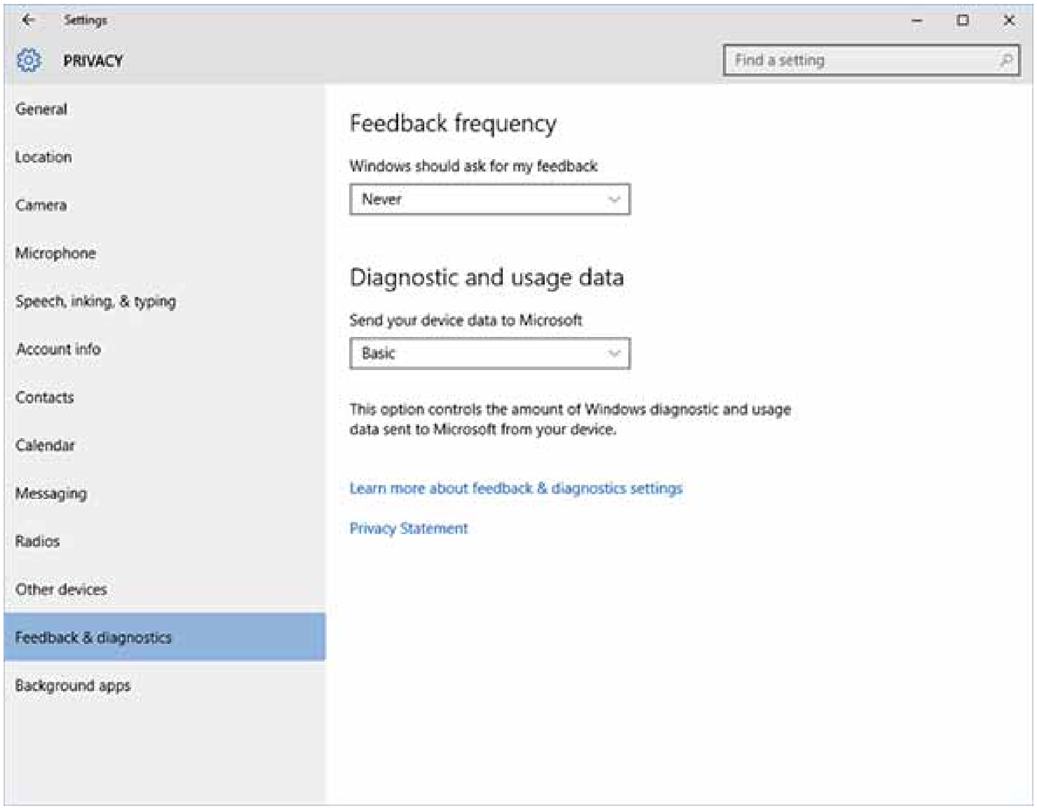
Options: 0 - Security [Enterprise Only]

Help:

This policy setting determines the amount of diagnostic and usage data reported to Microsoft. A value of 0 will send minimal data to Microsoft. This data includes Malicious Software Removal Tool (MSRT) & Windows Defender data, if enabled, and telemetry client settings. Setting a value of 0 applies to enterprise, EDU, IoT and server devices only. Setting a value of 0 for other devices is equivalent to choosing a value of 1. A value of 1 sends only a basic amount of diagnostic and usage data. Note that setting values of 0 or 1 will degrade certain experiences on the device. A value of 2 sends enhanced diagnostic and usage data. A value of 3 sends the same data as a value of 2, plus additional diagnostics data, including the files and content that may have caused the problem. Windows 10 telemetry settings applies to the Windows operating system and some first party apps. This setting does not apply to third party apps running on Windows 10.

If you disable or do not configure this policy setting, users can configure the Telemetry level in Settings.

Fig. 3 Allow Telemetry dialogue



Feedback frequency

Windows should ask for my feedback: Never

Diagnostic and usage data

Send your device data to Microsoft: Basic

This option controls the amount of Windows diagnostic and usage data sent to Microsoft from your device.

Learn more about feedback & diagnostics settings

Privacy Statement

Fig. 4 Section of the privacy dialogue for switching off the sending of diagnostic information and error information

soft (AskVG 2016). Nevertheless, choosing this option is not possible from any standard settings dialogue, but it is necessary to do it through the editor for policies of local groups. This editor is easily activated from the RUN dialogue (the easiest way to reach this is by using a combination of the WIN + R keys), then enter “gpedit.msc” and press “enter”. In this editor, it is necessary to find the “Allow Telemetry” option, which is on the following path: Computer Configuration → Administrative Templates → Windows Components → Data Collection and Preview Builds. From there, it is necessary to choose “Allow Telemetry”, obtaining the dialogue as shown in Fig. 3.

With the use of this dialogue, it is possible to choose the hidden “Security” option. Nevertheless, it needs to be said that choosing such an option makes sense only for Enterprise, EDU, IoT and server versions of Windows 10. With other versions (Core/Home and pro), this option behaves the same as the “Basic” option, so choosing the “Security” option would be pointless.

The dialogue shown in Fig. 4 contains a total of 13 sections related to privacy (Epstein 2015). It is necessary to dedicate special attention to each one of them in order to establish the users’ need to share certain information or not.

Account info is a very important sub-section of privacy. In it, it is defined that each and every application installed has access to data about a user’s account. This needs to be switched off. In Fig. 5, a dialogue is shown in which it is possible to deny applications access to data related to the user’s account.

3. Using local account only

Microsoft, as well as Apple, encourages users to create their accounts, such as a Microsoft Live account, by integrating the OS with the user’s account. When it comes to privacy, this actually represents one of the most disputed elements. As long as the user is logged into the system, Microsoft can upload any user profile data from the OS to the server without the user’s knowledge. Basically, logging in with a Microsoft account initiates the synchronisation of settings and data, including internet search history, favourites, currently opened applications and recorded applications. In addition, coded information from websites and mobile hot-spots, as well as Wi-Fi network names and their codes are transferred (Wright 2015). Without a Microsoft account, it is rather difficult, almost impossible in fact, to upload this data. In addition, without a Microsoft account, the problematic Wi-Fi sense function is disabled. By not using a Microsoft account, users protect themselves from numerous Microsoft attempts at collecting data through their offered privacy policy. It is recommended to use local accounts, while for email communication, alternatives should be used (Gmail, Yahoo and others).

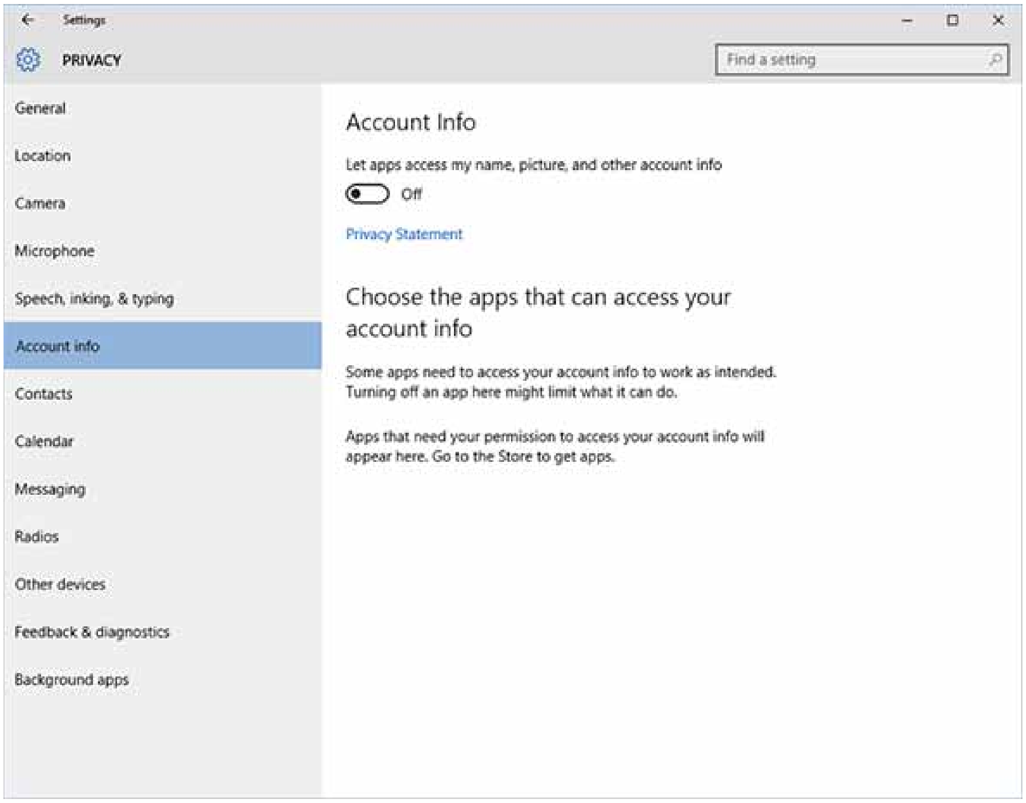
4. Microsoft’s use of users’ internet flow

By default, Microsoft turns the user’s computer into a peer-to-peer node for distributing Windows 10 OS corrections, aimed at saving the flow costs of the Microsoft server. In Microsoft terminology, this is called WUDO or Windows Update Delivery Optimization (Microsoft 2016). WUDO should be switched off by default, since it can slow down the user’s internet connection, but it can also increase the user’s internet expenses in cases when it is paid according to flow. In order to switch off WUDO, it is necessary to go through four rather unclear screens.

Step 1: Settings -Update & security.

According to what is stated in Microsoft’s updated users’ terms, Microsoft will always know what you are currently doing on your computer: “*Micrososft will collect information from you and your devices, including for example ‘app use data for apps that run on Windows’ and ‘data about the networks you connect to‘.*”(Microsoft 2015a)

Step 2: Update & security - Advanced op-



Account Info

Let apps access my name, picture, and other account info

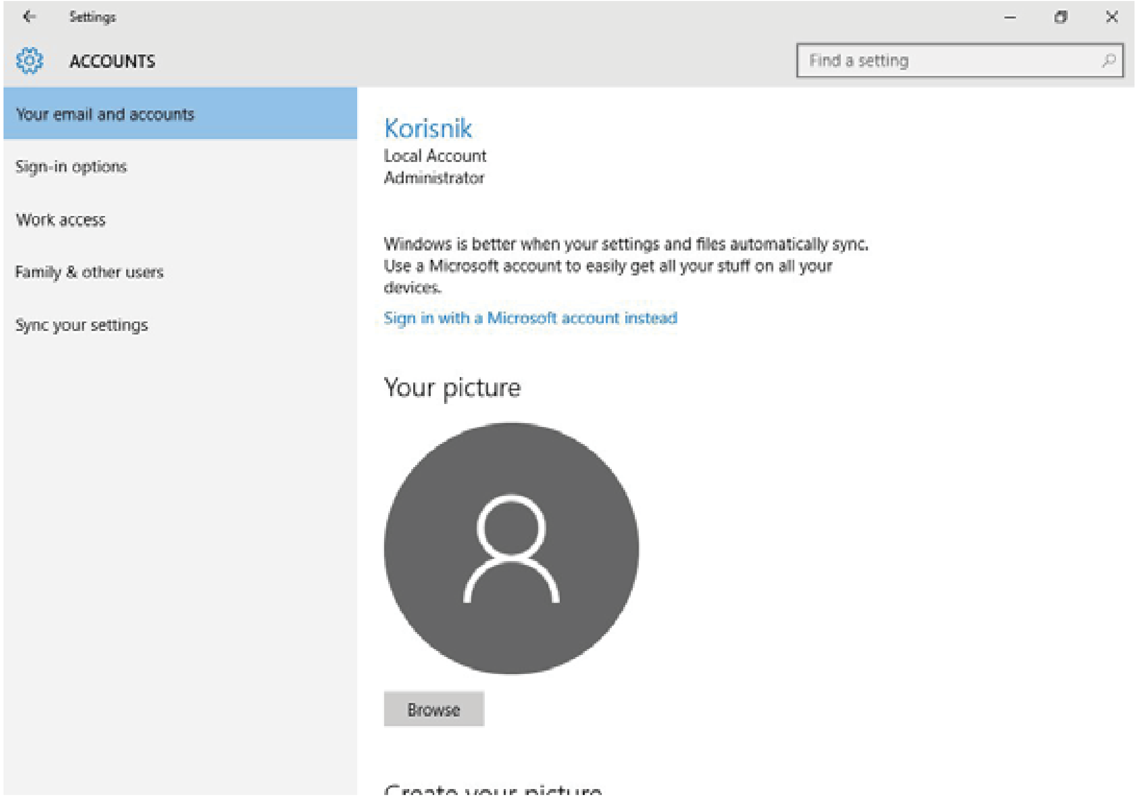
Off

Choose the apps that can access your account info

Some apps need to access your account info to work as intended. Turning off an app here might limit what it can do.

Apps that need your permission to access your account info will appear here. Go to the Store to get apps.

Fig. 5 Privacy dialogue section for denying applications access to the user's account



Korisnik
Local Account
Administrator

Windows is better when your settings and files automatically sync. Use a Microsoft account to easily get all your stuff on all your devices.

Your picture

Create your picture

Fig. 6 Dialogue for account settings

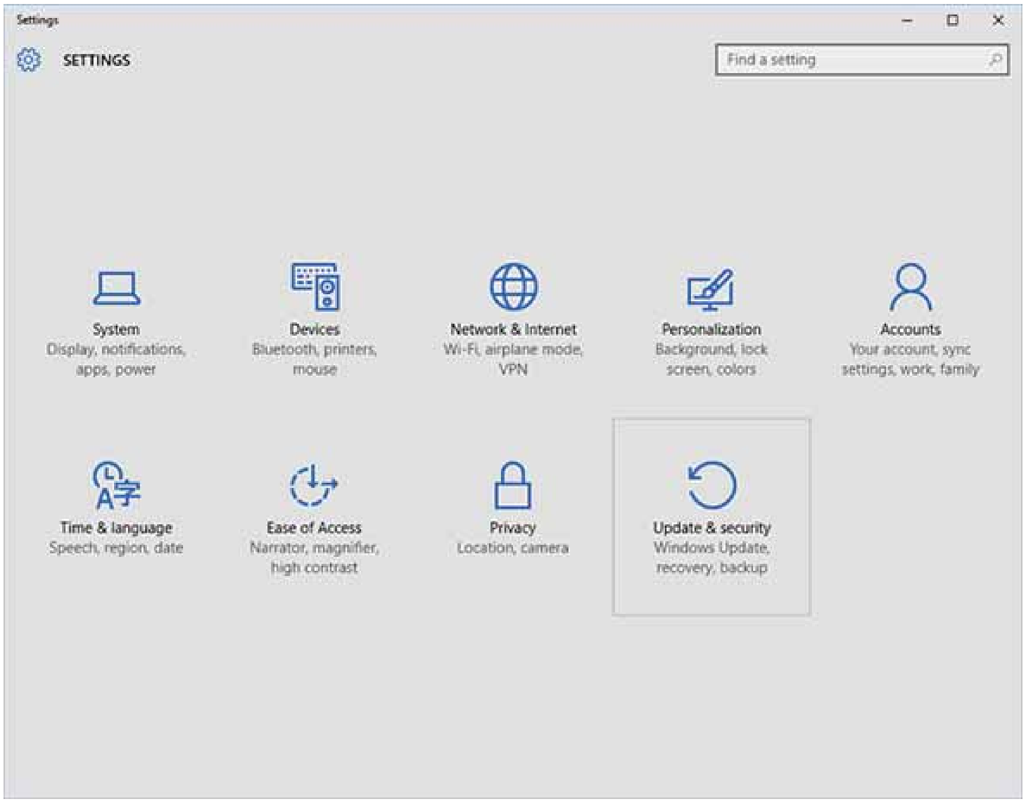
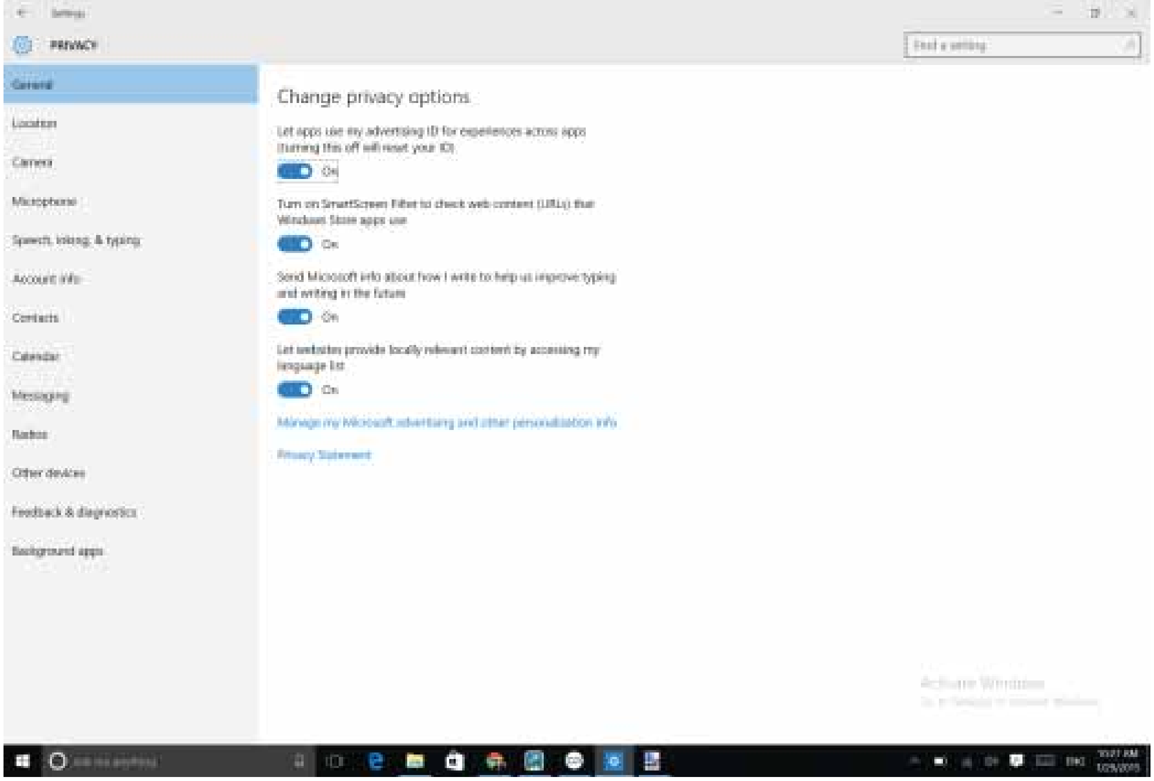

Settings
SETTINGS
Find a setting
System
Display, notifications, apps, power
Devices
Bluetooth, printers, mouse
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Accounts
Your account, sync settings, work, family
Time & language
Speech, region, date
Ease of Access
Narrator, magnifier, high contrast
Privacy
Location, camera
Update & security
Windows Update, recovery, backup

Fig. 7 Dialogue in which the Update & Security dialogue appears



Change privacy options

Let apps use my advertising ID for experiences across apps (turning this off will reset your ID)

On

Turn on SmartScreen Filter to check web content (URLs) that Windows Store apps use

On

Send Microsoft info about how I write to help us improve typing and writing in the future

On

Let websites provide locally relevant content by accessing my language list

On

Manage my Microsoft advertising and other personalization info

Privacy Statement

Fig. 8 Update & Security dialogue, with advanced options for Windows Update

tions

Step 3: In the Advanced options choose "*Choose how updates are delivered"***.** Choose the option **"***Notify to schedule restart***"** in order to avoid automatic restarting of the PC by Windows after updating, and to require permission to perform this action.

Step 4: Switching off peer-to-peer correction distribution.

5. Disabling the monitoring of advertising IDs

Windows 10 generates unique advertising IDs for every user on every PC (Microsoft 2015b). This can be misused by programmers and ad networks for profiling users. These options can be switched off, but one needs to know where:

6. Do not use Edge or Cortana

Microsoft's personal assistant Cortana and the new Edge browser are designed to take advantage of as much personal information as possible, in order to customise the user experience, take annotations, and learn all about the user (Auerbach 2015) (RT 2015). Until Microsoft clarifies or revises its privacy policy, it is better not to use any options that go into users' privacy. Regarding privacy, Firefox, Chrome or the latest version of Internet Explorer are better alternatives to Edge.

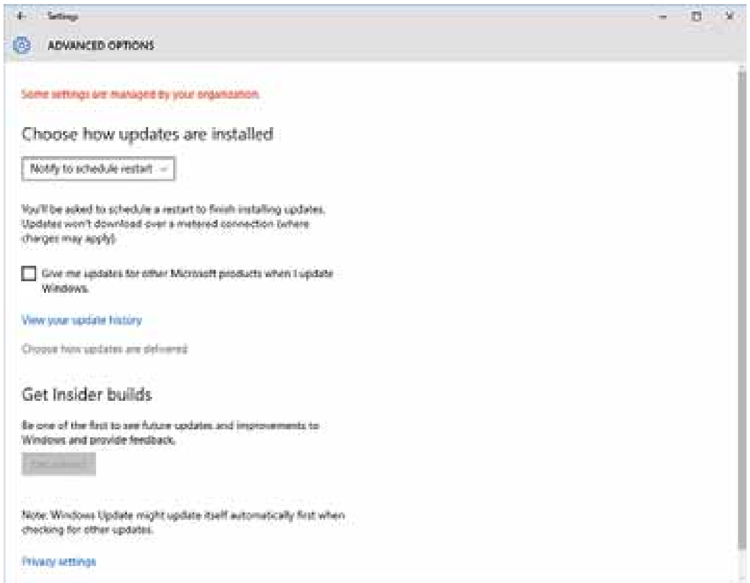
By switching on the Cortana virtual assistant, the system is allowed to provide personalised speech recognition, collect your voice input, as well your name and nickname, access your recent calendar events and the names of the people in your appointments, as well as information about your contacts, including their names and nicknames. This additional data enables the system to better recognise people and events when you dictate messages or documents (Microsoft 2015c).[3]

This is not a complete list, but only the most important items are highlighted, in which Microsoft encroaches into user privacy. Microsoft should centralise options regarding user privacy in a much more transparent way and explain all the implications of their usage. Obviously, however, the "free" Windows 10 update is actually paid for through the exchange of the user's personal data on the OS.

III CONCLUSION

While installing a new Operating system, it is necessary to pay attention to the protection of privacy, since modern computers contain sensitive data that users are not willing to share. Windows 10 really does represent a considerable improvement compared to previous versions of this operating system (8 and 8.1) in different fields, and it can be considered a good operating system. However, Windows 10 has a certain number of settings which are switched on by default and that can encroach into user privacy. In modern times, user privacy is very important. Confidential data that can be found on a computer, the use of computers for electronic transactions and access to different web portals from a PC with the user's name and password are only some examples where user privacy is so important. As a result, it is necessary for a PC user with the Windows 10 operating system, either as a private user or a legal entity, to make certain system adjustments according to his/her needs, regarding data protection and privacy rights. This paper contains an overview of settings regarding privacy on Windows 10, as well as recommended values for these settings that offer adequate privacy regarding the information system at the archaeological site of "Viminacium". Furthermore, in this paper, methods of adjusting these settings are mentioned, which are, in some cases, not particularly intuitive for the average operating system user.

[3] https://privacy.microsoft.com/en-us/privacystatement/



Some settings are managed by your organization.

Choose how updates are installed

Notify to schedule restart

You'll be asked to schedule a restart to finish installing updates. Updates won't download over a metered connection (where charges may apply).

□ Give me updates for other Microsoft products when I update Windows.

View your update history

Choose how updates are delivered

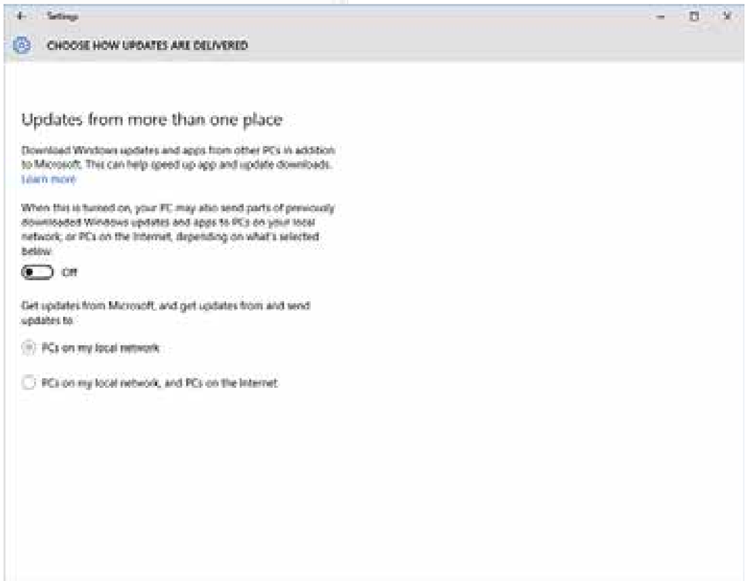
Get Insider builds

Be one of the first to see future updates and improvements to Windows and provide feedback.

Note: Windows Update might update itself automatically first when checking for other updates.

Privacy settings

Fig. 9 Dialogue with advanced options for Windows Update – choosing how to install updates



Updates from more than one place

Download Windows updates and apps from other PCs in addition to Microsoft. This can help speed up app and update downloads. Learn more

When this is turned on, your PC may also send parts of previously downloaded Windows updates and apps to PCs on your local network, or PCs on the Internet, depending on what's selected below:

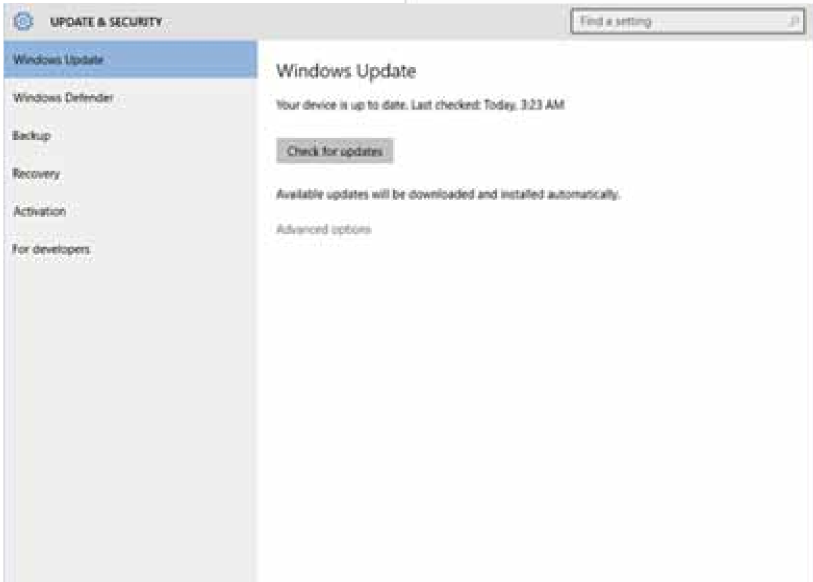
Off

Get updates from Microsoft, and get updates from and send updates to

○ PCs on my local network

○ PCs on my local network, and PCs on the Internet

Fig. 10 Dialogue for switching off peer-to-peer correction distribution



Windows Update

Your device is up to date. Last checked: Today, 3:23 AM

Available updates will be downloaded and installed automatically.

Fig. 11. Dialogue for disabling the monitoring of advertising IDs

BIBLIOGRAPHY

AskVG, 2016
Truth Behind Disallowing Telemetry and Data Collection Trick in Windows 10, [e-book], AskVG,
http://www.askvg.com/truth-behind-disallowing-telemetry-and-data-collection-trick-in-windows-10/
[accessed May 29th, 2016].

Auerbach, D. 2015
Broken Windows Theory, [e-book], Slate Magazine.
http://www.slate.com/articles/technology/bitwise/2015/08/windows_10_privacy_problems_here_s_how_bad_they_are_and_how_to_plug_them.html
[accessed March 15th, 2016].

Epstein, Z. 2015
Windows 10 is spying on almost everything you do – here's how to opt out, [e-book], BGR,
http://bgr.com/2015/07/31/windows-10-upgrade-spying-how-to-opt-out/
[accessed May 15th, 2016].

Microsoft 2015a
Microsoft Privacy Statement, Telemetry & Error Reporting Section, [e-book], Microsoft,
https://www.microsoft.com/en-us/privacystatement/default.aspx?Componentid=pspMainSyncSettingsModule&View=Summary
[accessed February 5th, 2016].

Microsoft 2015b
Microsoft Privacy Statement, Advertising ID Section, [e-book], Microsoft,
https://www.microsoft.com/en-us/privacystatement/default.aspx?Componentid=pspMainSyncSettingsModule&View=Summary
[accessed March 24th, 2016].

Microsoft 2015c
Microsoft Privacy Statement, Input Personalization Section, [e-book], Microsoft,
https://www.microsoft.com/en-us/privacystatement/default.aspx?Componentid=pspMainSyncSettingsModule&View=Summary
[accessed April 4th, 2016].

Microsoft 2016
Windows Update Delivery Optimization: FAQ, [e-book], Microsoft,
http://windows.microsoft.com/en-us/windows-10/windows-update-delivery-optimization-faq
[accessed March 27th, 2016].

RT 2015
'Incredibly intrusive': Windows 10 spies on you by default, [e-book], RT,
http://www.rt.com/usa/311304-new-windows-privacy-issues/
[accessed May 27th, 2016].

Vilić, V. and Radenković, I. 2015
Pravo na privatnost u svetlu Zakona o zaštiti podataka o ličnosti, Pravni život, nr. 10/2015, pp. 331-341.

Wright, M. 2015
The Windows 10 privacy issues you should know about, [e-book], Thenextweb,
http://thenextweb.com/microsoft/2015/07/29/wind-nos/
[accessed March 20th, 2016].

REZIME
KONTROLA PRIVATNOSTI NA WINDOWS 10 OS

KLJUČNE REČI: PRIVATNOST, KONTROLA PRIVATNOSTI, PRIVATNOST I WINDOWS 10.

Kao i kod svakog informacionog sistema pitanje zaštite privatnosti je u fokusu politike bezbednosti organizacije. Ovim radom date su smernice koje se odnose na informacioni sistem na arheološkom lokalitetu „Viminacium“ koje su neophodne pri nadogradnji računarskih sistema, da bi se obezbedila zahtevana privatnost prikupljenih informacija u toku obrade digitalne arheološke građe. Windows 10 sadrži složena podešavanja koja se tiču privatnosti korisnika ovog operativnog sistema, i u nastavku radaće biti reči o preporukama za podešavanja koja se tiču bezbednosti na Windows 10 OS. Biće reči o podešavanjima koja se mogu odabrati tokom same instalacije, zatim o isključivanju određenih skrivenih podešavanja privatnosti kao i o prednosti korisćenja lokalnog naloga na Windows-u 10. Takođe ce biti reći o iskorišćavanju korisničkog Internet protoka od strane Microsofta i o tome na koji se način ono onemogućuje. Na samom kraju će biti reči i o problemima privatnosti koje donose novi sastavni delovi Windows-a 10: novi Internet pretraživač Edge i personalni asistent Cortana.