DPA: Commission Nationale de l’Informatique et des Libertés (CNIL). France

TITLE: Rules for the use of personal data in electoral campaigns

DATE: November 2016

KEY WORDS: Microsoft, cooperation, tracking, privacy policy, consent, cookies, safe harbor

WEBSITE: https://www.cnil.fr/fr/windows-10-la-cnil-met-publiquement-en-demeure-microsoft-corporation-de-se-conformer-dans-un-delai

ABSTRACT:

On July 2016, the France’s National Data Protection Commission (CNIL) issued a formal notice to Microsoft Cooperation urging Microsoft to make Windows 10 to comply with French data protection law. The CNIL criticized the company for three actions:

a) tracking its users web browsing habits without their consent,

b) failing to offer proper security protections, and

c) delivering targeted advertising materials without the user’s consent.

This notification does not seek to prohibit Microsoft from using its services to advertise but seeks to enable users to make their choice freely, having been properly informed of their rights.

Consequently, the CNIL gave the company three months to comply with its orders to stop collecting personal data without the consent of those users concerned. Otherwise, the company may impose any applicable sanctions of up to 150,000 euros.

ASSESSMENT

Microsoft's practices have been questioned during the last year by the CNIL. In September 2015, the company said that Windows 10 collected personal data in order to improve user’s experience as well as to help Microsoft understand how consumers are using the new Windows 10.

As a consequence, the CNIL carried out an investigation between April and June 2016 and conclude that the telemetric service used for the purpose of diagnosing issues and improving the services was unnecessary for the relevant purpose and therefore excessive and also stressed that the collection of personal data through advertising used to be activated automatically and user consent was required. In addition, the CNIL considered that the pin code system did not offer adequate security.
In this regard, the formal notice might be considered as a high efficient initiative as Microsoft data was being transferred outside the EU on a “safe harbor” basis despite it was invalidated by a decision issued by the European Union’s Court of Justice back in October 2015\(^1\). However, it seems that the company aims at working closely with the CNIL to implement those changes and resolve the illegal situation as the vice president of the Regulatory Affairs team at Microsoft, David Heiner, has promised to address privacy and security concerns.

So far, the company has continually focused on meeting high standards of EU privacy law. On 2 April 2014, the Article 29 Working Party (WP 29) approved Microsoft’s cloud commitments and stated that the personal data stored in Microsoft’s enterprise cloud was subject to Europe’s rigorous privacy standards no matter where that data is located. Specifically, the WP 29 stated the following: "Importantly, Microsoft is the first – and so far the only – company to receive this approval. This recognition applies to Microsoft’s enterprise cloud services – in particular, Microsoft Azure, Office 365, Microsoft Dynamics CRM and Windows Intune."\(^2\)

Ultimately, it is important to mention that the CNIL has been the only authority that has formally investigated the lack of security and data breaches performed by Microsoft. Thanks to this efficient and effective way to proceed to investigate the computer and software giant, the Spanish Data Protection Agency (AEPD) has started to analyse whether Microsoft complies with the Spanish Data Protection Law (in this sense, both French and Spanish legislation are governed by the principle of the quality of the data, which is also related to the user's consent).

Therefore, it will be important that European authorities work closely to guarantee uniform interpretation of cross border legal affairs. As a starting point, the active communication between European authorities and Microsoft is needed to increase legal certainty within the EU since the new GDPR will become law in 2018 across all 28 EU member states and will impact every organisation that holds or uses personal data both inside and outside of Europ

\(^1\) For further information about the Safe Harbor, visit:

Unofficial translation

Windows 10: the CNIL publicly informs MICROSOFT CORPORATION to comply, within a period of three months, with the French law Informatique et Libertés (Computer Technology and Freedoms).

The President of the CNIL warns MICROSOFT CORPORATION to stop the excessive collection of data and the monitoring of users' navigation without their consent. It also asks it to satisfactorily ensure the security and confidentiality of users' data.

Following the launch of the new Windows 10 operating system in July 2015, the CNIL's attention was drawn to the press and to political party letters on the potential for excessive collection of personal data by MICROSOFT CORPORATION.

At the same time, within the G29 (a group of European CNILs), a group of several protection authorities has been set up (Contact Group) to investigate this issue and carry out investigations in the various Member States involved.

It is in this context that the CNIL carried out 7 online checks in April and June 2016 and questioned MICROSOFT CORPORATION on certain points set out in its privacy policy in order to verify the compliance of Windows 10 with the law Informatique et Libertés.

These audits identified numerous breaches of the Act, including:

**Collected irrelevant or excessive data**

The CNIL has found that the company collects diagnostic and usage data as part of its "telemetry" service. This service allows, on the basis of diagnostic or usage data, to identify problems, solve them and improve products. For this purpose, MICROSOFT CORPORATION deals, for example, with usage data of the Windows applications and the Windows Store, which make it possible to be aware of all the applications downloaded and installed on the system by a user and the time spent on each of them, they. In doing so, it engages in excessive collection, which data is not necessary for the functioning of the service.

**A safety fault**

The company allows users to choose a 4-digit PIN to authenticate for all its online services, including access to their Microsoft account, which lists purchases made on the store and means of payment Used. However, the number of attempts to enter this PIN is not limited, which does not ensure the security and confidentiality of user data.

**Lack of consent**
It also appears that an ad identifier is enabled by default when installing Windows 10. It allows Windows applications and third-party applications to track users' browsing and offer them targeted ads without user consent.

**A lack of information and the possibility of opposing the deposit of cookies**

The company deposits on the users' terminals advertising cookies, without first having correctly informed them or being able to oppose them.

**The persistence of international transfers on the basis of the Safe Harbor**

The company transfers the personal data of its members to the United States on the basis of the Safe Harbor, which is no longer possible since the decision of the Court of Justice of the European Union of 6 October 2015.

**The President of the CNIL therefore decided to give notice to MICROSOFT CORPORATION to comply with the law within a period of 3 months.** This procedure and the legal analysis of the CNIL are the sole responsibility of the French authorities, the other Member States of the Contact group continuing their investigations on their territory.

Update: MICROSOFT asked the President of the CNIL to benefit from an additional period of 3 months. This renewal was granted and therefore postponed the deadline to 20 January 2016.

The purpose of this notice is not to prohibit all advertising on the services of the company but to allow users to exercise their choice freely by being properly informed of their rights.

It was decided to publish this notice, in particular because of the seriousness of the shortcomings and the number of people involved (more than ten million users of Windows 10 on the national territory).

The CNIL recalls that this demand is not a sanction. No action will be taken if the company complies with the law within the time limit. In this case, the closure of the procedure will also be publicized.

If MICROSOFT CORPORATION fails to comply with this formal notice within the prescribed time limit, the Chairperson may designate a rapporteur who may, if necessary, prepare a report proposing to the CNIL’s restricted committee responsible for sanctioning breaches of the law Informatique et Libertés, to impose a sanction against society.