Brandenburg Commissioner
for Data Protection and Access to Information

Final decision

national reference	136/20/0820
case register no.	Case 147873
Art. 56 procedure	143055
further references	61VMN 137770
draft decision	147910

I. Reason for the hearing

The reason for an investigation by the Brandenburg Commissioner for Data Protection and Access to Information was - in addition to a complaint we have received - the report on [redacted], which reported on the port scanning carried out on the website of [redacted] (see attachment).

According to the statement on [redacted], the Microsoft Windows IT systems of the website visitors of "[redacted]de" or "[redacted]com" would be scanned for open ports using the JavaScript program "check.js" using the network protocol "WebSockets". This concerned in particular the services or programs "Aeroadmin", "Ammy Admin", "AnyDesk", "Anyplace Control", "RDP", "Teamviewer" and "VNC" and their standard ports.

After analysis by the Brandenburg Commissioner for Data Protection and Access to Information, the facts described in the article by [redacted] of 25 May 2020 were verified.

II. Statement by [redacted]

[redacted] described that the "port enumeration technology" used, which is carried out in contrast to the port scanning mentioned in the article to determine open ports without directly sending data packets to the target object, processes the IP address of the user as a personal date in addition to the device-specific data. These data are linked to user data known to [redacted] [redacted].

According to the statement, the port enumeration method has been used since 2016/2017 for the EU/UK as well as for the US domain and targets Microsoft Windows systems. A Microsoft Windows system is the most widely used operating system in the use of remote desktop tools and is the operating system

with the greatest vulnerability and impact to malware. The test object is the open ports of the tools "Aeroadmin", "Ammy Admin", "AnyDesk", "Anyplace Control", "RDP", "TeamViewer" and "VNC".

The purpose of processing personal data via port enumeration is the identification of potentially compromised systems and the prevention, detection, mitigation and investigation of fraud attempts, security breaches and other prohibited or illegal activities in risk scenarios - such as at the time of user registration, login, bidding, purchase, voucher redemption, guest purchase and transaction execution.

As a legal basis for the processing of personal data using the port enumeration method and the device-specific data obtained and the user's IP address, [redacted] refers to Art. 6 para. 1 sentence 1 lit. f GDPR. [redacted] sees the legitimate interest in the processing of personal data by the port enumeration method on the one hand in the financial and data protection interests of the users of the [redacted] platform that are worthy of protection. It is in the interest of the user that his or her personal data be protected from unauthorised access.
On the other hand, [redacted] bases its legitimate interest on its own interest in using the port enumeration method as part of its IT security tools and to protect [redacted]'s own IT systems from external unauthorized attacks, in particular to meet the requirements of Art. 32 GDPR and § 13 para. 7 TMG. Furthermore, the method aims at preventing commercial damage, fraudulent activities on the website and damage to your reputation.
The necessity of the method is justified by the fact that no comparable, less invasive method exists to pursue and protect the interests described. To limit its use, the port enumeration method would only be used in identifiable high-risk scenarios and only for the most common and vulnerable operating systems.

[redacted] states that the interests you describe are not overriding the interests or fundamental rights and freedoms of users of the website. This is due to the fact that the date port collected by the port enumeration method has a lower sensitivity than the sensitivity of the collected data, which would have been accessible to unauthorised persons through a security incident without using the method. Furthermore, the risk arising from the measure and the collection of the date was considered to be low, as the date was only used as initial information and further measures, such as the "captcha", would only follow afterwards.

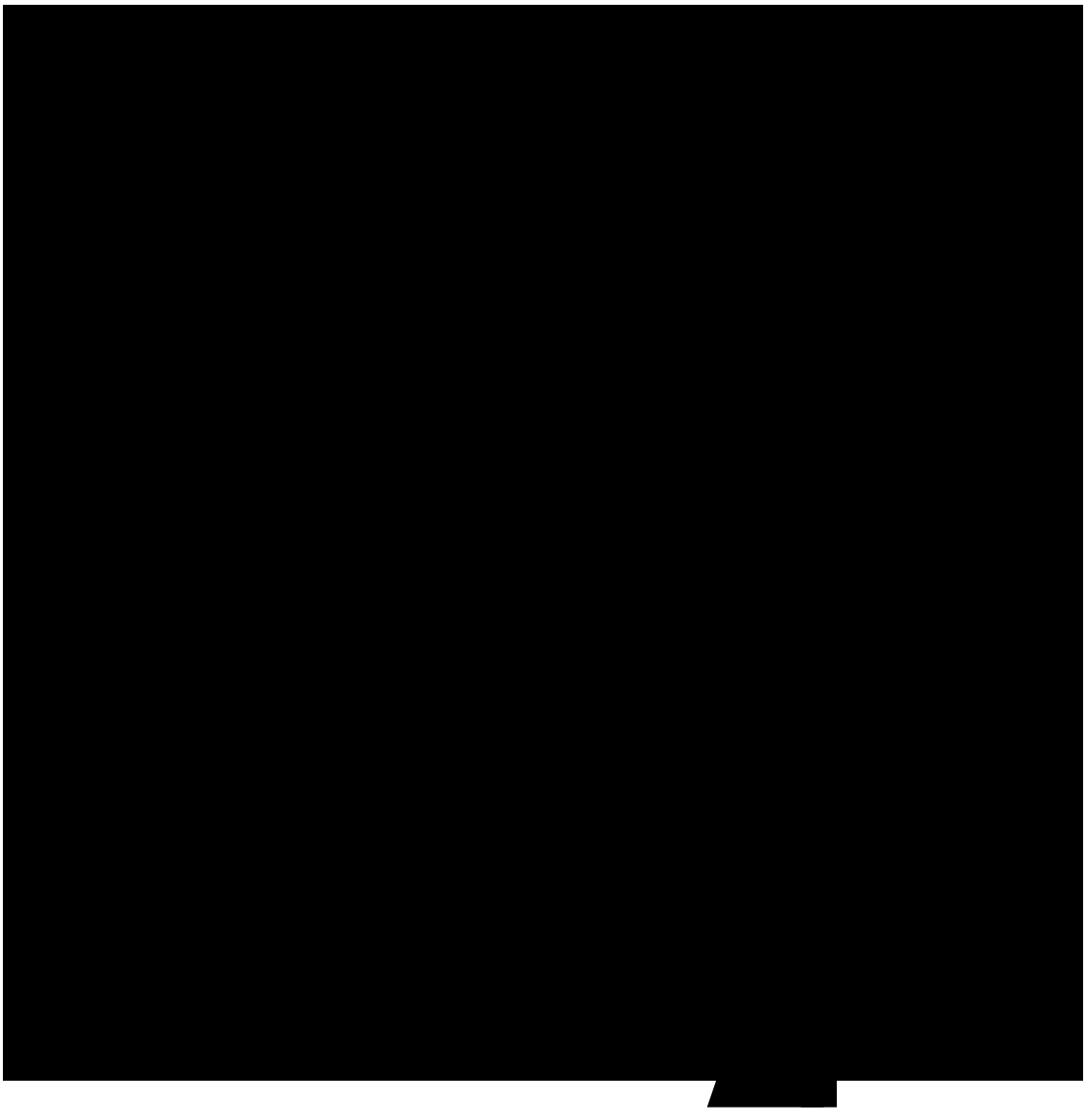
The user of the website of [redacted] would be informed in section 5.4. of the privacy policy that personal data is processed for the "prevention, detection, containment and investigation of fraud, security breaches and other prohibited or unlawful activities, including the assessment of relevant risks" in the sense of Art. 6 para. 1 sentence 1 lit. f GDPR.

III. Legal assessment

The Brandenburg Commissioner for Data Protection and Access to Information agrees that the present case constitutes processing of personal data within the meaning of Article 4(1) of the GDPR.

The Brandenburg Commissioner for Data Protection and Access to Information considers the legal basis used by [redacted], Art. 6 para. 1 sentence 1 lit. f GDPR, and the weighing of interests described above to be justified and comprehensible, so that there are no data protection concerns.

However, we would like to point out to those responsible that the port enumeration method is carried out during a mere visit to the website (see Figure 1: Port enumeration during a visit to [redacted].de) and not only, as described in the statement, in every risk scenario.



In addition, we recommend that the person responsible extends the information in the data protection statement (Section 5.4., point 3) relating to the facts

presented here to include the information in the port enumeration in the sense of Art. 12 Para. 1 sentence 1 GDPR and Art. 13 Para. 1 lit. c GDPR, since such a method is not expected by an ordinary user of the website and is not intuitive.

For this reason and due tot he fact, that there are no objections by other European authorities (via IMI, DD 149710), the Brandenburg Commissioner for Data Protection and Access to Information considers the matter to be closed.

On behalf of the Brandenburg Commissioner for Data Protection and Access to Information,
October 13, 2020
Kleinmachnow, Germany