Recommendation 12/2020. (XI.6.) of the Magyar Nemzeti Bank on the information security requirements of teleworking and remote access

TRANSLATION

I. Objective and scope of the recommendation

The rapid development of information and telecommunications technologies is giving more and more room to the spread of teleworking. Growing demands have been driven by economic and social considerations in addition to convenience, due to the movement restrictions caused by the pandemic situation, the mass demand for teleworking also appeared in institutions where this form of work had not been used before or only to a limited extent.

For this reason, the collaboration and video conferencing solutions that are often based on cloud services, and are implemented on infrastructures on which the institution has no full control gained more and more ground in.

The Magyar Nemzeti Bank (hereinafter: the "MNB"), acting in its role of responsibility for the supervision of the financial intermediary system, intends to ensure in accordance with the provisions of the relevant laws and regulations, that the institutions of the financial intermediary system make it possible to access and work remotely outside the office with the institution's internal network or sensitive data or systems (hereinafter: remote access) for employees and other contract workers (collectively: remote users) under adequate technical conditions taking into account security requirements, in compliance with the relevant legislation.

The objective of this recommendation is to define the expectations of the MNB pertaining to the IT security requirements for teleworking and remote access, and to facilitate the predictable application of the law, to promote the uniform application of relevant legislation and to support innovation.

This recommendation is addressed to the institutions and persons (henceforth together: institution) defined in article 39 of Act CXXXIX of 2013 on the Magyar Nemzeti Bank.

This guideline does not comprehensively refer to legal provisions when defining principles and expectations, but the addressees of the recommendation are of course still required to comply with relevant legal requirements.

This recommendation does not define guidance regarding the handling of data and data protection matters, does not contain any requirements regarding the handling of personal data, and the requirements contained therein shall in no way be understood as an authorisation for processing of personal data. Handling of data in relation to the fulfilment of supervisory requirements set out in these recommendations may be carried out exclusively in compliance with the legal provisions on data protection in force at any time.

II. General expectations, concepts

1. For the purposes of this Recommendation, teleworking means the regular or occasional performance of a task arising from an employment relationship or other contractual relationship at a place separate from the institution's premises, which is performed by computer means and the results transmitted electronically. Remote access is a broader, technical concept that means external access to the institution's internal network and IT resources (regardless of the user's legal relationship).

2. The institution is expected to pay special attention to the IT security risks related to teleworking and to the full protection of the data of the institution and its clients, in particular the risks of data handling and processing in teleworking.

3. The recommendation in the recent document should be applied together with the MNB recommendation 8/2020 (VI. 22) on the protection of the information system [hereinafter: MNB recommendation 8/2020 (VI. 22.)] and the MNB recommendation 4/2019 (IV.1.) on the usage of community and public cloud computing services [hereinafter: MNB recommendation 4/2019 (IV. 1.)].

III. Regulation of teleworking

4. The MNB expects the institution to have a document regulating teleworking and access to teleworking, which is an integral part of the institution's information security management system. The regulatory document is expected to include at least the following:
   a) a clear definition of the concept and conditions of teleworking;
   b) the range of processes, sub-processes and activities that can be performed in teleworking;
   c) a list of systems and data categories available in teleworking;
   d) a list of roles or jobs authorized for teleworking;
   e) a list of priority users or jobs for remote access in case of high system load;
   f) the procedure for ordering and revoking teleworking (request, approval, revocation, duration);
   g) the location of the registry of issued teleworking licenses;
   h) the identification and authentication procedures applied in teleworking[1];

[1] According to the institution's information security management system.

i) special data management and data processing rules to be observed in teleworking (access, storage, transmission, deletion, etc.);
j) special regulation of privileged user access (e.g., system administrator and application administrator) in teleworking[1];
k) in addition to the general logging requirements, log collection requirements arising from teleworking, the content of reports on log entries and the right of access to them[1];
l) a list of the types of devices permitted and required for teleworking;
m) identification of the organizational units and persons providing the devices used in teleworking (notebook, PC, smartphone, internet access, communication software, etc.), the procedure for requesting the devices;
n) a procedure for the handover of devices related to teleworking (e.g., token, certificate), which requires at least a written declaration of acknowledgement and acceptance from the remote user about the security rules for teleworking;
o) determination of the home IT and IT security conditions required for the use of teleworking;
p) special information security awareness behaviour required to perform the general and certain high security (e.g., treasury) tasks expected from the remote user in teleworking, as well as a list of the relevant rules and regulations and the rules for their training;
q) the procedure for completing teleworking and the rules for returning to the office;
r) rules and regulations for the maintenance and repair process of user equipment used in teleworking;
s) the procedure for the destruction of data media used in teleworking;
t) prohibition of the handling of paper-based documents and its special regulating in exceptional cases;
u) special technical conditions and security rules for teleworking of areas requiring special security (e.g., treasury); and
v) the procedure to be followed in the event of the loss, theft or compromise of equipment used in teleworking.

IV. IT security risk assessment of teleworking

5. The MNB expects the institution to address specific IT security risks arising from teleworking in the framework of its IT security risk assessment, and to ensure the development of risk mitigation action plans[2], the conditions for the implementation of measures, the implementation of measures and the review of measures taken. In the risk assessment, the institution shall cover at least the persons, processes and systems involved in teleworking (including data processing systems) as well as the data

[2] The requirements related to the action plans are defined in MNB recommendation 8/2020 (VI. 22.).

processed in these systems and the risks arising from the location of teleworking.

6. The MNB expects the institution to review its risk assessment related to teleworking on a regular basis[3], at least as often as required by law, and document the identified risks and the monitoring of their management.

V. Building teleworking infrastructure

7. Developing its IT infrastructure for teleworking, the institution may rely on its existing tools and systems, or expand them as needed, or build new ones.

8. In the acquisition, deployment and operations phases, the MNB expects the following:
   a) in teleworking, remote access must always be implemented via an encrypted channel;
   b) the institution shall ensure that an adequate number of remote access licenses are obtained for all systems used for teleworking and that the licenses are recorded;
   c) while developing the infrastructure required for teleworking, the institution shall determine the expected availability of the systems and the necessary capacity to provide them, as well as the alert and architectural expansion thresholds;
   d) the institution determines the type and manageability of the devices that can be used in teleworking based on a risk assessment (institutional, third party, remote user's own device);
   e) the institution determines how remotely connected devices can access resources on the internal network (e.g., terminal server, printers) – and, to the extent necessary, defines different security levels and connection types;
   f) the institution determines in advance and regularly reviews the parameters expected during operation (number of data connections, time and place of distribution of data connections, amount of data distributed, etc.);
   g) in case of using cloud-based services (team work platform, communication application, etc.) that support business processes in teleworking, ensures compliance with the MNB recommendation 4/2019. (IV. 1.);
   h) at the procurement process of the remote access services, the institution shall, as far as possible, choose a service provider or solution with references and international security certificates that is not included in either the institutional or the generally accepted blacklists available on the Internet; and
   i) to authenticate the remote user and device, the institution shall use multi-factor authentication, obtaining a strong authentication factor, such as a token, dynamic code, or certificate, from a trusted source.

[3] 3.4.2. of MNB recommendation 8/2020 (VI. 22.).

In case of dispute between the language versions, the Hungarian version shall prevail.

VI. Equipment used in teleworking

9. It is recommended that the institution provide and manage by the devices (notebook, smartphone, tablet, etc.) used for teleworking. If the institution is unable to provide a sufficient number and quality of devices for teleworking or these are not proportionate to the security risks depending on the type of access, the institution may allow remote users to use their own devices, subject to appropriate control measures, and the use of third party assets.

10. The MNB expects the institution to prohibit or prevent by technological means the use of publicly available computers and by technological and administrative means the use of publicly available wired and wireless networks (libraries, Internet cafes, etc.) for remote access.

VI.1. Working with the institution's computing equipment

VI.1.1. IT security recommendation for notebooks and workstations

11. In case of desktop and portable computers owned and provided by the institution, the institution is expected to provide, in proportion to the risks:
    a) centralized device management in directory services (e.g., LDAP, Active Directory) and authentication (e.g., Kerberos, RADIUS), and connecting them to IT security management systems;
    b) disabling the local admin rights for the remote users, with documented limited use and enhanced control where appropriate;
    c) that only and exclusively software approved by the institution may be installed on the devices;
    d) a centralized solution for the continuous security updates of device firmware, drivers, operating system, virus protection and virus definition database and applications;
    e) that the change of the security settings of devices and centrally managed software by the remote user be prohibited also by technical means;
    f) that direct access to an external network is only allowed for the duration of setting up the remote connection (e.g., in the case of access to a hotel or home WiFi network requiring authentication) or, where appropriate, the technical conditions required for remote access until the necessary connections are provided (e.g., to update in anti-malware protection system the virus definition files, download security patch);
    g) that the local firewall is running and the connection to the Internet is only possible after establishing a remote connection, through the institution's perimeter protection infrastructure (firewall, proxy, content filter);

h) encryption of the built-in storage of these devices and an additional end-to-end data loss protection (DLP) solution in risk-proportionate manner;
i) prohibition of the use of external storage devices (such as USB drives, external hard disks, CDs / DVDs, etc.) by default, and allow their use only in duly justified cases with distinct, documented approval; and that it only allows the use of external devices provided and managed by the institution and encrypted as needed;
j) the using of the local printers with special permission only; and
k) synchronization of the device clocks based on a central source.

VI.1.2. IT security recommendation for smartphones and tablets

12. For smartphones and tablets used in teleworking (hereinafter together: smart devices), the institution is expected to ensure:
a) the integration of smart devices into the existing IT and IT security systems, provided that the capabilities of the smart device allow it in a risk-proportionate way;
b) that only smart devices managed by the central Mobile Device Management (MDM) solution be issued to the remote user , under the conditions and settings defined in the information security management system;
c) risk-proportionate usage of additional mobile management solutions in addition to the MDM solution (e.g., unified endpoint management (UEM), mobile application management (MAM), Enterprise Mobility Management (EMM), etc.);
d) in addition to MDM solutions, the utilization of additional protection solutions on these smart devices in proportion to the risks (e.g., Mobile Threat Defense Solution, Mobile Threat Defense (MTD) solutions, etc.);
e) depending on the capabilities of the applied MDM solution, the use of a separate user profile or storage (container) to be able to separate the institution's sensitive data and the personal data of the remote user;
f) protection of data stored on the smart devices with appropriate encryption, authentication methods, passwords;
g) the restriction of application installation from unknown sources, and the detection ofcracked smart devices and, in that case, disabling the connection of the smart device and remotely securely wiping the data on it;
h) an unambiguous binding of remote users to their smart devices provided to them by the institution in the institution's remote access IT infrastructure, and that the remote user, in addition to the devices used under the notebook and workstation policies, can access the institution's network and resources only from registered smart device (s) provided to them by the institute.
i) that the purchased smart devices and their operating systems are compatible with the institution's encryption requirements;

j) to keep the smart device operating systems and applications up-to-date, in a risk-proportionate manner, and to specify the minimum expected operating system versions;
k) that security settings defined and set by the institution cannot be changed by remote users;
l) that internal network services (e.g., e-mail, calendar, file server access) accessed through the institution’s smart devices are provided to remote users only to the necessary extent;
m) that the smart devices provided by the institution are connected to the institution's internal network through the infrastructure for teleworking and remote access;
n) keeping an up-to-date and complete record of remote accesses, indicating the identity of the remote user and the type of smart device.

VI.1.3. IT security recommendation for external storage media

13. Throughout the usage of external storage media (USB drive or equivalent) in teleworking, the institution is expected to ensure:
    a) that storage media of unknown origin shall not be used, remote users shall only use media provided, managed and registered by the institution for teleworking in accordance with point 11. i);
    b) that storage media devices shall be used by remote users with a specific permission assigned to the user – and, assigned to the specific media device if possible;
    c) that non-public data shall be stored on storage media devices only in encrypted format;
    d) that the confidential information is stored on the storage medium only for as long as is strictly necessary, and the remote user must delete it from the storage media device immediately after use; and
    e) that the transport of storage media devices containing confidential information shall be prohibited by default, if the transport is justified by the maintenance of a business function, it is expected that the institution ensures the conditions and rules of secure transport.

VI.2. Working with the employee’s computing equipment

14. The MNB does not recommend allowing the use of the remote users' own devices, only in particularly justified cases with significantly reduced access compared to the access provided for the institution's own devices, or by applying additional control measures.

15. In such a case, the institution is expected to strive to enforce at least the institution’s

security policies to the assets, so the requirements listed in VI. 1. shall be enforced by administrative and technical measures, in a risk-proportionate manner.

16. Where the usage of the remote users' own devices is particularly justified, additional requirements are the following:
    a) the institution specifies in detail what types of the user’s own devices may be used (notebook, smartphone, tablet), with which systems (minimum requirements at the hardware and software level, versions, updates), what resources and data they can access, and what security settings must be applied;
    b) the institution makes the connection of devices owned by the remote user to the institutional network subject to a separate, documented authorization procedure;
    c) the institution informs the remote user in writing prior to the use of their own devices of the personal and device specific security requirements, the necessary technical conditions for the use of the device in teleworking, the institutional requirements, the relevant regulations and their content, as well as of the institution’s right to check the remote user’s devices so that the remote user declares in writing that they know and accept these conditions.
    d) before granting access, it shall be recorded and signed by the user that in the event of a change in the remote user's own device or in the event of termination of their employment, contract or assignment, they must present the device for inspection to the institution and enable the immediate deletion of institutional data and applications stored on it.
    e) allow the use of the remote user's own devices only by using the institution's central management solution for the institution's mobile devices, for which the institution shall define and technologically enforce appropriate individual, risk-proportionate security settings, ensuring that the security settings of the authorized devices may only be changed by the designated specialists of the institution;
    f) depending on the capabilities of the appliend MDM solution and the given smart device, the institution shall mandate the use of a separate user profile or storage (container) to be able to separate the institution’s sensitive data and the personal data of the remote user;
    g) the institution shall ensure the possibility to remotely delete (remote wipe) the institution’s sensitive data also on the user's own devices;
    h) the institution shall keep an up-to-date and complete records of which user and which user owned devices it provides remote access to;
    i) the institution's IT system must be able to clearly identify all remote access sessions (user, remote device);
    j) the institution shall also ensure with technical solutions that the connection providing access to the internal network or resources can only be established from a device approved and registered by the institution;

k) the institution should, as far as possible, prevent a user from accessing the institution's network and sensitive data from multiple user owned devices at the same time;
l) the institution shall require the remote user to copy sensitive data as soon as possible from their own devices to the server or storage provided to the remote user by the institution where the automatic data backup is implemented, and to securely delete the sensitive and non-public data from the user's devices that is no longer needed to perform his/her current task as soon as possible after the backup;
m) the institution shall prohibit the use of cracked (rooted and jailbroken) devices in teleworking;
n) the institution shall restrict the connection of devices with obsolete, vulnerable operating systems;
o) the institution shall ensure, if the technical conditions are met, that the remote user does not run any commands with local administrator privileges during the remote connection to the institution's system;
p) the institution shall require the remote user to install and run the latest version of malicious code protection software on his/her own device;
q) the institution shall ensure that during the remote connection to the institution's system, if the technical conditions are met, the Internet can be accessed via the institution's border protection infrastructure (firewall, proxy, content filter) only;
r) the institution shall also ensure that the remote user stores institutional data on his/her own device only in encrypted forms and in a place separated from personal data by re-authentication; and
s) the institution shall settle data traffic and fee issues in an internal regulation or in an agreement with the remote user.

VI.3. Working with the third party's computing equipment

17. The MNB expects the institution to avoid the use of assets owned by third parties as far as possible, provide them only to a limited extent, subject to a separate permit. Allow the connection with these devices to the institution's network only if:

a) they meet at least the requirements for the institution's assets and the details of the cooperation have been agreed with the third party and the third party makes a confidentiality statement;
b) the institution shall appoint a responsible person or contact person within the institution for the management of third party access;
c) the third party access shall be granted by the institution only for a specified period of time and shall be automatically revoked upon expiry;

d) before connecting third party devices to the institution's network, the institution shall verify that the connecting device has protection (such as a malicious code protection client) of at least the same level as that used by the institution;

e) third party's security software meets the institution's security requirements; in the absence of that, the institution is expected to require the third party to take the necessary measures to fulfil them or to withdraw its intention to join; the institution shall provide support for the deployment of the necessary software (e.g., VPN client, encryption software, service, anti-malware protection system) or, depending on the agreement, ensure their deployment; and

f) the third party agrees in the contract not to perform any activity other than the performance of the work included therein, even if it has technically more extensive rights.

VII. Operations and protection of the teleworking infrastructure

VII.1. Security of the teleworking location

18. The MNB recommends that, to secure the workplace at home, the institution provide guidance to the remote user at least on the secure design of the home environment and network, the configuration and security settings of the operating system and the remote connection. In teleworking, the remote user does not use the protected office environment, therefore the confidentiality of their telephone conversations and work materials require enhanced protection. The MNB expects the institution to determine the minimum physical and logical protection measures required from the location of teleworking (location, size, infrastructure, physical protection, etc. of the workplace). It is also expected that the authorization of remote access shall include the consent of the remote user to the security check of the teleworking workplace as required. The MNB expects that the security guidelines for the workplace of teleworking and the conditions for its checking will be laid down in a contract concluded with any third party, and the observance of it is guaranteed by the third party.

19. The institution is expected to assess and provide, in a risk-proportionate manner, tools and services needed to conduct business workflows securily and continuously, such as:

a) computer devices (notebook, PC, smartphone, etc.);

b) computer accessories (headsets, webcam, SIM card, token, smartcard, card reader, etc.);

c) tools of protection against physical theft (e.g., Kensington lock, safebox for lockup, etc.);

d) where appropriate, the equipment needed to process the paper documents generated while teleworking (scanner, shredder, security envelope, etc.);

e) if necessary, a privacy screen filter or foil; and

f) if necessary, data connection subscription (e.g., internet subscription, managed mobile internet).

20. The MNB expects the institution to prepare IT security awareness material on the conditions and risks of using teleworking, within the framework of which the institution draws the attention of the remote user to at least the following:

a) the devices used for remote access must not be left unattended by the remote user, the screen must be locked, or the password-protected screen saver must be activated in the event of a shorter absence;

b) the institutional tools used in teleworking are used only by those competent to do so (not family members);

c) the remote user shall keep the devices used for authentication (e.g., token, smartcard) in a secure place, should not leave them connected to the machine when not in use, should not share or and give them to anyone;

d) to make the remote user's own home WiFi network more secure in teleworking (changing the default administrator password of the WiFi router and setting up the firewall securely, connecting to the WiFi network only with password with proper encryption, disabling WEP and WPS, etc.);

e) the remote user must ensure the secure storage of devices used in teleworking in the event of interruption or finishing of work, so that the devices do not remain in a "sleeping" or "hibernating" state for a long time;

f) do not leave the devices unattended, especially in a car, car trunk, hotel room, ensure that the devices are stored in a locker;

g) in case of travel, carry the equipment as hand luggage and pay particular attention to its protection;

h) ensure that the data storage media containing the data are stored securely (e.g., safebox, etc.) in accordance with their security class and that unauthorized access to the data is prevented or detected (e.g., storage in a tamper evident envelope, etc.);

i) the passwords required for the institution's network and applications should not be used by the remote user for private purposes;

j) avoid using the devices in a public place as much as possible, do not allow an unauthorized person to gain access to your screen; and

k) report any IT security incident and compromise, loss or theft of the teleworking devices to the institution without delay.

VII.2. Network security

21. In teleworking the MNB expects the institution to:

a) ensure and verify that only verified and authorized devices that comply with IT security standards, have up-to-date security updates and protection tools (e.g., malware protection) can connect to the institution's network;

b) ensure and verify that smart devices managed by the institution can only be connected to the institution's infrastructure if the security settings of the devices meet the criteria of the mobile device protection system;

c) always check the network traffic of the connected device during the remote access connection by the institution's perimeter protection solutions (firewall, IDS / IPS, webgateway, data leakage protection system, etc.);

d) pay special attention to the prevention of data leakage in teleworking;

e) seek to use recent and more secure solutions in the implementation of remote access, with strong and secure protocols and algorithms in a risk-proportionate manner;

f) avoid technologies that provide remote access that is considered less secure, such as remote desktop, file sharing (despite their encrypted authentication and data transfer), use these connections only in particularly justified cases, with additional network encryption;

g) terminate remote access in a network segment separated by firewall from of the institution's internal, protected networks, use a technical solution to ensure that in the event of a compromise of the remote access terminating device (e.g., VPN gateway), the attacker cannot access the internal, protected networks;

h) ensure that access to sites and services that pose a risk of data leakage, such as, but not limited to, social media, public cloud storage, file sharing and webmail, is prohibited or in particularly justified cases is restricted in proportion to the risks, and their use for work purposes (for storing and sharing institutional data, images, information) is subject to a specific permit;

i) prohibit, in justified cases strictly regulate or restrict the transmission of confidential materials via public e-mail service; and

j) ensure the confidentiality and integrity of emails containing tax, business, banking, securities, cash, payment, insurance or occupational pension secrets or personal data.

VII.3. Daily operations and services in teleworking

22. The MNB expects the institution to maintain the necessary and sufficient IT services in teleworking, that ensure the continuous operation of IT tools and systems. Within this framework, the MNB expects the institution to:

a) employ an adequate number of qualified professionals for user support (helpdesk);

b) ensure that remote user requests are securely delivered to the customer service;

c) ensure the availability and proper functioning of the user support in teleworking and emergency events (e.g., pandemic situations);
d) assess and determine the institution’s office-specific job roles and work processes;
e) in the office, ensure an adequate number of qualified staff and a safe working environment to carry out the on-premises jobs and work processes;
f) ensure that the necessary daily operational activities are always carried out (backups, checking the logging and monitoring systems, reporting, etc.); and
g) ensure the detection and investigation of the IT security incidents and execution of the necessary actions.

VII.4. Security of fax, phone-, tele-, video conferencing calls and other communication channels

23. In teleworking, users working at the office and remotely can communicate with each other and with third parties by telephone teleconferencing or video conferencing. The confidentiality, integrity and authenticity of data and information travelling on these and other (fax, online chat, other) communication channels must be ensured at all times.

24. In order to reduce risks and protect data, the MNB expects the institution to provide technical and administrative controls, depending on the given communication solution, and to ensure:

a) the encryption of data connections and encrypted transmission of authentication data for all online conference / collaboration services (video, audio, chat, other);
b) the use of standard encryption algorithms and procedures;
c) the exclusion of the possibility of disabling the encryption (even for the administrator);
d) the limitation of the handling of non-public information by telephone, fax, video conferencing, online chat and similar platforms by technical or administrative controls;
e) that the persons invited have the necessary authorization to access information provided during the calls;
f) the prohibition of conversations sharing confidential information in public places used also by unauthorized persons;
g) that only persons invited by the meeting organizer can join the calls;
h) the authentication enforcement at login;
i) the use of the "waiting room" on joining, if possible;
j) the license for the required number of participants;
k) that audio and video contents of the call only be recorded in justified and pre-approved cases, of which all participants are informed in advance; the conversation or conference must be recorded exclusively on the lines designated for that purpose, by the tools designated for that purpose;

l) the secure and lawful storage and use of audio and video recordings and their immediate deletion when the purpose ceases;

m) the supervision of screen sharing, file sharing and file transfer during the calls by the meeting organizer;

n) the use of an additional encrypted channel over the conference service connection in proportion to the risks (this may result in a higher voice and data network traffic);

o) that the sending or receiving of confidential data by fax is prohibited by default, and is allowed only in duly justified cases, with appropriate controls in place, with the prior notification and approval of the receiving party;

p) that during the live speaking conversation and telecommunication unauthorized persons within hearing or sight shall not gain possession of confidential information; and

q) the confidentiality of conference calls with appropriate microphone headphones provided to remote users as needed.

VII.5. Management of recorded telephone conversations

25. In relation to the recording of telephone calls, the MNB expects the institution, in accordance with the relevant statement[4] of the European Securities and Markets Authority (ESMA), to:

a) pay special attention in teleworking to the compliance with relevant legislation during the recording and storage of telephone conversations or electronic communications (voice, e-mail, chat, video) concerning client orders;

b) if electronic data recording is not possible for any reason, ensure that the data is recorded in an alternative way, and the change and the new method are communicated to the customer before starting the phone call[5];

c) ensure enhanced monitoring and ex-post review of relevant orders recorded by alternative way (paper or electronic record, dictaphone, clerk's mobile phone, personal telephone voice recorder, etc.) and the fulfilment of these orders[6];

d) not to leave in outgoing call any messages containing confidential data on the called party's answering machine; and

e) make all possible efforts to return to the original state from the alternative recording method as soon as possible[7].

[4] ESMA Statement on COVID-19 telephone recording (hereinafter: ESMA35-43-2348)

[5] Paragraph 6. of ESMA35-43-2348

[6] Paragraph 6. of ESMA35-43-2348

[7] Paragraph 7. of ESMA35-43-2348

VII.6. User identification and authentication in remote access

26. In remote access, the MNB expects the institution to:

a) use multi-factor authentication to authenticate the remote user;
b) use standard, strong cryptographic algorithms for encryption and authentication;
c) uniquely identify remote users, their devices and connections;
d) determine the maximum number of remote connections allowed to the same remote user at a time;
e) regulate and document the end-user access;
f) ensure that the strength and complexity of the passwords used in teleworking meet or exceed the requirements for accessing the institution's internal network;
g) determine a secure process for issuing, renewing and revoking the second factor used for authentication so that it can be provided even remotely;
h) ensure the possibility of the immediate termination of an established connection by the institution; and
i) authenticate the remote devices as well for the more reliable authentication in proportion to the risks.

VII.7. Access to data

27. The institution must provide teleworkers while teleworking with necessary and sufficient conditions for accessing the data, keeping in mind the principle of least privilege. To this end, the MNB expects the institution to:

a) determine adequate remote access groups and personalize their access rights to institutional data, following the "least privilege" principle;
b) separate the data access to the production, test, training and development environments;
c) regulate and separate the privileged users' (e.g., application and operation system administrators) access according to their roles;
d) disable the printing in teleworking by default, regulate it in justified cases;
e) control the downloading of institutional data to the local machine in teleworking;
f) ensure the off-device backup of institutional data generated on local devices.

VIII. Remote access control

28. The increased number and traffic of network connections required for remote access and data traffic flowing through these in teleworking need to be managed in a risk-proportionate manner. To this end, the MNB expects the institution to:

a) continuously monitor the remote access network connections and data transferred through them;
b) define the logging requirements for the remote access, the IT infrastructure providing the remote access and ensure their enforcement;
c) ensure the sending of the security logs of the IT infrastructure providing remote access and teleworking to the central log management system, the regular analysis of the log files, the setting of the alert threshold values, the sending of the alerts and the tracking of the resulting actions. Ensure the search for correlations between the remote access security logs from different sources to allow the identification of anomalies and related incidents in a risk-proportionate manner,;
d) pay special attention to the logging of activities performed with privileged rights while teleworking, the setting of alerts, the protection of these log files and the regular monitoring these activities;
e) develop an action plan to manage and control deviations from expected operational parameters (increased remote access, increased traffic, etc.); and
f) regularly verify that the IT infrastructure and endpoint devices used in remote access, comply with applicable information security and IT policies and requirements, ensure that regular vulnerability assessments are performed. While performing technical compliance checks, also use automated tools in a risk-proportionate manner.

IX. Final provisions

29. Recommendation is a regulatory tool with no legal binding force for the institutions, issued in accordance with article 13 paragraph (2) point i) of Act CXXXIV of 2013 on the Magyar Nemzeti Bank. The content of the recommendation issued by MNB represents the requirements imposed by law, as well as the principles, methods, market standards and rules proposed for application based on the law enforcement practice of MNB.

30. MNB monitors and evaluates compliance with the recommendation among the supervised financial institutions falling within the scope of authority of MNB, in line with general European supervisory practices.

31. MNB brings to the attention of the financial institutions that it can incorporate the recommendation into its policies. In this case the financial institution has the right to indicate that the respective policy is in compliance with the pertinent recommendation issued by MNB. If the financial institution wishes to incorporate only certain parts of this recommendation into its policies, then it shall avoid referring to the recommendation, or it shall apply this referral only to the parts actually incorporated.

32. MNB expects the adaptation of this recommendation by the concerned financial institution beginning on 01/01/2021, with the fact that MNB considers it a good practice

that the financial institutions consider the expectations contained in the present recommendation before that date in its development newly created or ongoing at the time of the publication of the recommendation.

Dr. György Matolcsy

President of the Magyar Nemzeti Bank