RULES ON ACCESS TO THE NATIONAL BANK OF BELGIUM FOR EXTERNAL PERSONS

1 January 2019

1. SCOPE

1.1. For the purposes of these rules, "external persons" means all persons who are not employees of the National Bank of Belgium ("the Bank") and who need to enter the premises which are not open to the public.

1.2. External persons may be asked to sign a form expressly stating that they accept the provisions of these rules. The form must be handed over to the Bank within a maximum of two working days following receipt of the identity badge referred to in Article 2. The Bank reserves the right to refuse access to anyone who has not signed that form.

2. REPORTING TO RECEPTION AND USE OF A BADGE

2.1. External persons must report to one of the employees' reception desks of the Bank and present valid proof of identity (identity card or, failing that, passport, driving licence or other valid document). The Bank will check the identity of the external persons and verify whether it has received prior notice of their presence.

2.2. Once the checks have been carried out, the Bank issues a badge to the external persons. The badge gives external persons access to the Bank's premises within the limits and the period of validity of the access rights associated with the badge. Those limits and the period of validity shall not extend beyond what is necessary for carrying out the agreed activities at the Bank.

2.3. External persons must wear the badge visibly at all times while they are on the Bank's premises. They must ensure that the badge is not damaged or rendered unusable in any way.

2.4. The badge is strictly personal. External persons must not use their badge to afford entry to other persons or allow others to use it.

2.5. External persons must surrender the badge at one of the reception desks at the latest on expiry of the period of validity of their access rights.

3. SCREENING

The Bank may make access to premises or areas which are not open to the public dependent on prior checks of the reliability of the person concerned ("screening"). The Bank will only conduct or order screening with due regard for the applicable legal rules. If the outcome of the screening is negative, the person concerned will in principle not be granted access to the Bank.

4. REGISTRATION ON ENTRY AND EXIT AND TIME RECORDING

4.1. As a result of use of the badge, data on external persons are entered in the Bank's entry and exit registration system. If so agreed, external persons must also use the badge to record their attendance at the workplace in the Bank's time recording system.

4.2. The data in the Bank's time recording system and its entry and exit registration system may be used to check that the external persons were present to carry out the activities at the Bank

and to produce interim statements and invoices relating to their services. If the external persons perform work as employees of a contractor or as subcontractors, the Bank may, in the event of any dispute over an invoice on account of any deficiency in the services provided, allow the employer or contractor to access the data recorded in these systems.

5. USE OF THE BANK'S RESOURCES AND MONITORING

5.1. External persons must use their own equipment and resources to carry out the agreed activities. If necessary, the competent Bank service may, at its own discretion, make the following resources available to external persons, depending on the task assigned to them:

- the Bank's premises, equipment or facilities, and/or
- hardware, software and other IT facilities (including the internet and a Bank e-mail address), and/or
- access to specific data sources at the Bank.

5.2. External persons are not permitted to make use of or gain access to other resources of the Bank without the prior express consent of the person in charge of the competent service(s) of the Bank.

5.3. External persons may use the Bank's resources only for carrying out the agreed activities. These resources must not be used for personal purposes or for professional purposes other than those carried out for the Bank. External persons are not permitted to remove the Bank's resources from its premises without the prior express consent of the person in charge of the competent service(s) of the Bank. External persons must in all cases ensure that they do not damage the Bank's resources or render them unusable in any way.

5.4. In regard to the IT facilities and access to the Bank's data sources, external persons must use the applicable security measures (passwords, personal identification numbers (PINs), security tokens, etc.) and respect the rules applicable to data security at the Bank. External persons may only use the Bank's wireless networks in accordance with the applicable internal instructions.

5.5. It is prohibited to make use of the IT facilities made available by the Bank (i) to visit websites or take part in discussion groups of a racist, sexist, or pornographic nature or those which incite hatred or violence, (ii) to download files or programs in the knowledge that this may be in breach of a third party's intellectual property or other rights; (iii) to download or circulate files or programs without applying the procedures specified by the Bank; (iv) to download or circulate files or programs which the Bank has indicated may contain viruses, worms or other programs harmful to the proper operation of the Bank's computer infrastructure.

5.6. The Bank may conduct both continuous monitoring and sample checks on the use that external persons make of the Bank's resources, including checks on the use of e-mail and the internet, and on access to the Bank's data sources. For that purpose it may collect and use all relevant data (loggings, list and content of folders and files opened, websites visited, content of messages sent, duration of activities, etc.). The Bank will use the data exclusively for the purpose of checking compliance with these rules and with the arrangements for the conduct of the agreed activities; for those purposes, the Bank may also pass on these data to the employer or contractor of the person concerned.

6. EMERGENCY INSTRUCTIONS

6.1. If the sirens sound continuously, the buildings must be evacuated in accordance with the instructions issued over the loudspeakers or by the Bank's stewards. Everyone must go to the assembly point indicated by the Bank.

6.2. If possible, external persons should join a group which is evacuating the building and report to the group's steward (identified by a yellow jacket). Otherwise, external persons must leave the building by following the pictograms 'emergency exit', with due regard for the specific instructions given over the loudspeakers or by the Bank's stewards.

6.3. Before the buildings are evacuated, all appliances must be turned off unless it would endanger personal safety to do so. In the event of a fire, doors and windows must be closed to prevent the flow of air. In the event of a bomb alert, doors and windows must be opened to facilitate air displacement.

6.4. Use of the lifts is prohibited during an evacuation.

7. SPECIAL SECURITY AND SAFETY INSTRUCTIONS

External persons must always comply with the special security and safety instructions applicable to them, including the rules relating to the roof and fire permits issued by the Bank. The Bank and its consultants and site safety officers may produce additional written instructions for external persons, with due regard for the nature of the activities which they carry out.

8. PROCESSING OF PERSONAL DATA

8.1. General

8.1.1. The Bank collects and processes personal data on external persons in the context and with the aim of (1) the performance of and supervision of the activities carried out by the external persons at the Bank, (2) ensuring the security of the Bank, its premises and the persons present there, (3) the performance of the Bank's tasks and contractual and legal obligations in relation thereto, and (4) facilitating, controlling and optimizing its internal functioning. This processing of personal data is based on Article 6 (1), (b), (c), (e) and (f), and Article 9 (2), (a) of the General Data Protection Regulation[1]. The personal data processed relate among others to identification and contact data, biometric data, and camera images (see paragraphs 8.2 and 8.3 below), and data on the use of the NBB infrastructure (telecommunication data, use of provided software and hardware, use of the car park, ...). The Bank, with its head office at boulevard de Berlaimont 14, 1000 Brussels, is the controller of the processing of such personal data.

8.1.2. The Bank's employees and the employers or contractors deploying external persons will only have access to the personal data on a need-to-know basis. Third parties have no access to the personal data except (1) in the cases specified by law, (2) where third parties have to carry out assignments concerning the computerised applications for the management of those personal data, and (3) if and to the extent necessary for the performance of the Bank's tasks and the application of its contractual and legal obligations.

8.1.3. The Bank processes personal data of external persons for the duration which is strictly necessary in order to attain the aforementioned purposes of the processing.

8.1.4. In as far as the conditions laid out in the applicable legislation are met, external persons have the right to:
(1) Access their personal data and, as the case may be, rectify them;

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J.E.U., L 119, 4 May 2016, p. 1 to 88.

(2) Object to processing on grounds relating to their particular situation;
(3) Obtain the erasure of such data or the restriction of processing;
(4) Receive the personal data concerning them in a structured, commonly used and machine-readable format, and to transmit those data to another controller;
(5) Lodge a complaint with the Commissie voor de Bescherming van de Privé Levensfeer/Commission de Protection de la Vie Privée if they consider that processing their personal data infringes the applicable legislation.

To exercise the rights mentioned under points (1) to (4), external persons can send an e-mail to the data protection officer of the Bank, at the following address: dataprotection@nbb.be.

8.2. Biometric data

Certain areas of the Bank are only accessible after a biometric data check. External persons needing access to those areas will be asked to record their biometric data (e.g. digital data based on the image of their irises). As a rule, such data will be recorded at the employees' reception desk at boulevard de Berlaimont 14.

8.3. Camera images

8.3.1. Certain areas of the Bank are constantly filmed in accordance with the Law of 21 March 2007 regulating the installation and use of monitoring cameras and in accordance with the Protocol of 21 September 2007 on video monitoring at the National Bank of Belgium. In accordance with the Royal Decree of 28 May 2018 amending the Royal Decree of 10 February 2008 determining the method of indicating the presence of video monitoring, pictograms draw attention to the presence of video monitoring at the entrance to the filmed areas.

8.3.2. The purpose of video monitoring is to provide general surveillance and to ensure the security and protection of the Bank's property and buildings, and of persons present in those buildings. Camera images are taken in order to collect evidence of any incidents constituting an offence or causing damage, and to trace and identify the perpetrators, disorderly persons, witnesses or victims. In addition, the camera images are taken so that, in the event of an incident, the images can be viewed in order to detect any irregularity in any intervention on the part of the Bank's personnel or third parties and/or to exclude any suspicion of malicious intent on the part of the various persons intervening.

9. CONFIDENTIAL INFORMATION

9.1. The Bank, its personnel and the members of its organs are subject to a strict professional secrecy obligation. Confidential information may only be disclosed to external persons if it is necessary for the performance of the agreed activities and with a strict undertaking from them to maintain confidentiality. Confidential information may only be disclosed in accordance with the law and the Bank's internal regulations.

9.2. The confidential information, on whatever medium, which the Bank discloses to external persons, or to which external persons have access, or which comes to their knowledge in the course of their activities at the Bank, must not be disclosed by them to any persons except to their employer or contractor if it is necessary for carrying out their activities at the Bank.

9.3. External persons may use the confidential information only for the performance of their activities at the Bank. They are not permitted to use that information for personal or other professional purposes.

9.4. External persons must respect the provisions of the rules on the classification and processing of information. A copy of those rules is available on request or via the Bank's intranet.

10. MARKET ABUSE AND INSIDER TRADING

The attention of external persons is drawn to applicable law on market abuse (Regulation (EU) No 596/2014 of 16 April 2014 on market abuse and the Law of 2 August 2002 on the supervision of the financial sector and on financial services, which prohibit market abuse and insider trading). External persons must comply strictly with those provisions. Infringements of those provisions may be subject to criminal penalties and administrative fines in accordance with the aforementioned laws.

In particular, any persons who have access to information which they know, or ought to know, to be inside information are prohibited from:

a) the actual or attempted, direct or indirect acquisition or disposal, for their own account or on someone else's behalf, of the financial instruments to which that inside information relates, except for transactions effected in order to discharge an obligation to acquire or dispose of financial instruments if that obligation has become due and results from an agreement concluded before the person concerned had access to the relevant inside information;
b) communicating that inside information to anyone else except in the normal course of their work, occupation or duties;
c) on the basis of that inside information, recommending someone else to acquire or dispose of the financial instruments to which that inside information relates, or arranging the acquisition or disposal of such instruments by any other person.

11. REPRESENTATION AND ADVERTISING

11.1. External persons must not at any time present themselves as employees or representatives of the Bank except, in regard to the latter status, with the Bank's express written authorisation.

11.2. External persons undertake not to use their assignment for the Bank as a reference or for advertising purposes without the Bank's prior written consent.

12. MISCELLANEOUS PROVISIONS

12.1. Smoking is prohibited on the premises of the Bank except in the designated areas.

12.2. It is prohibited to take photographs or make video or audio recordings in the Bank except as necessary for the performance of the agreed activities and with the prior written consent of the competent service of the Bank. Certain areas of the Bank are subject to special rules on bringing in photographic or video equipment, including IT equipment, hardware and mobile phones equipped with recording devices. While external persons are in these areas they must store such equipment in a locker. Exceptions can only be permitted by the person in charge of these areas.

12.3. External persons may use the Bank's parking facilities so long as they have obtained prior consent and have completed the required formalities. They must comply with the rules on the use of the parking facilities; a copy of those rules is available on request and is displayed at the usual car park entrances and exits.

12.4. External persons may use the Bank's staff restaurant provided they have obtained prior consent and in accordance with the agreed arrangements. Meals may only be taken in the areas specifically fitted out for this purpose.

12.5. External persons may not bring packages into the Bank except with the prior authorisation of the Security and Surveillance Service (VT). External persons bringing in a package must deposit it on their own responsibility in a storage place provided for this purpose.

12.6. External persons agree that the Bank's security staff may search and check their property and baggage in accordance with the Law of 10 April 1999 laying down rules on private and special

security. In the event of theft or any other incident involving security, the Bank may in particular order duly authorised persons to check the contents of handbags, briefcases, other baggage or personal effects and wardrobes or other furniture made available to external persons.

13. TERMINATION OF THE ACTIVITIES

If any external person contravenes these rules or other rules applicable on the Bank's premises, the Bank may immediately and unilaterally terminate the activities of the person concerned on its premises without any right to compensation for the latter.

* *
*