RÈGLEMENT RELATIF À L'ACCÈS D'EXTERNES À LA BANQUE NATIONALE DE BELGIQUE

1er janvier 2019

1. CHAMP D'APPLICATION

1.1. Pour l'application du présent règlement, il y a lieu d'entendre par « externes » toutes les personnes qui ne sont pas employées par la Banque nationale de Belgique (ci-après « la Banque ») et qui entrent dans les bâtiments non accessibles au public.

1.2. Les externes peuvent être invités à signer un formulaire dans lequel ils déclarent expressément qu'ils acceptent les dispositions du présent règlement. Ce formulaire doit être remis à la Banque au plus tard dans les deux jours ouvrables suivant la réception du badge visé à l'article 2. La Banque se réserve le droit de refuser l'accès à toute personne qui n'aurait pas signé ce formulaire.

2. INSCRIPTION À L'ACCUEIL ET UTILISATION D'UN BADGE

2.1. Les externes se présentent à une des loges « Entrée du personnel » de la Banque, munis d'une pièce d'identité valable (carte d'identité ou, à défaut, passeport, permis de conduire ou autre document faisant foi). La Banque contrôle l'identité des externes et vérifie si leur présence a été annoncée préalablement.

2.2. Une fois les contrôles effectués, la Banque remet un badge aux externes. Ce badge leur donne accès aux bâtiments de la Banque, dans les limites et pendant la durée de validité des droits d'accès associés au badge. Les limites et la durée de validité ne seront pas plus étendues que ce qui est nécessaire pour réaliser les activités convenues à la Banque.

2.3. Les externes portent toujours le badge de manière visible durant leur présence dans les bâtiments de la Banque. Ils veillent à ce que le badge ne soit pas endommagé ou rendu inutilisable de quelque manière que ce soit.

2.4. Le badge est strictement personnel. Les externes ne peuvent pas se servir de leur badge pour faire entrer d'autres personnes, ni permettre à des tiers de l'utiliser.

2.5. Les externes rendent le badge à l'un des points d'accueil, au plus tard à l'expiration de leurs droits d'accès.

3. SCREENING

La Banque peut subordonner l'accès de ses locaux ou zones non accessibles au public à un examen préalable de la fiabilité de la personne concernée (ci-après le « screening »). La Banque ne procèdera ou ne fera procéder à un screening qu'en conformité avec les dispositions légales en vigueur. Si le screening débouche sur une appréciation négative, la personne concernée se verra en principe refuser l'accès à la Banque.

4. ENREGISTREMENT DES ENTRÉES ET DES SORTIES ET ENREGISTREMENT DU TEMPS DE TRAVAIL

4.1. L'utilisation du badge entraîne l'enregistrement de données relatives aux externes dans le système d'enregistrement des entrées et sorties de la Banque. S'il en a été convenu ainsi, les

externes doivent également utiliser leur badge pour enregistrer leur présence sur le lieu de travail dans le système d'enregistrement du temps de travail de la Banque.

4.2. Les données du système d'enregistrement du temps de travail et du système d'enregistrement des entrées et sorties de la Banque peuvent être utilisées pour le contrôle de la présence des externes pour réaliser les activités convenues à la Banque, ainsi que pour l'établissement des états intermédiaires et des factures relatifs à leurs prestations. Si les externes effectuent des prestations au titre d'employés ou de sous-traitants d'un prestataire de services, la Banque peut, en cas de contestation d'une facture pour insuffisance de prestations fournies, permettre à l'employeur ou au prestataire de services de consulter les données figurant dans ces systèmes d'enregistrement.

5. UTILISATION DES RESSOURCES DE LA BANQUE ET CONTRÔLE

5.1. Les externes utilisent leurs propres matériels et ressources pour l'exécution des activités convenues. Si besoin en est, le service compétent de la Banque peut, à sa propre discrétion, mettre les ressources suivantes à la disposition des externes, en fonction de la mission qui leur a été assignée:

- o des locaux, du matériel ou des équipements de la Banque; et/ou
- o du matériel informatique, des logiciels et d'autres ressources informatiques (notamment un accès à l'Internet et une adresse électronique de la Banque); et/ou
- o l'accès à des sources d'information déterminées de la Banque.

5.2. Les externes ne sont pas autorisés à utiliser ou à se procurer l'accès à d'autres ressources de la Banque sans en avoir obtenu au préalable l'accord exprès des responsables du ou des services compétents de la Banque.

5.3. Les externes utilisent les ressources de la Banque exclusivement pour l'exécution des activités convenues. Ces ressources ne peuvent être utilisées ni à des fins personnelles ni à des fins professionnelles autres que celles exercées pour la Banque. Les externes ne sont pas autorisés à sortir les ressources de la Banque hors des bâtiments de celle-ci sans en avoir obtenu au préalable l'accord exprès du responsable du ou des services compétents de la Banque. Les externes veillent en tout état de cause à ne pas endommager les ressources de la Banque et à ne pas les rendre inutilisables de quelque manière que ce soit.

5.4. S'agissant des ressources informatiques et des accès aux sources d'information de la Banque, les externes sont tenus d'utiliser les mesures de sécurité préconisées (mots de passe, personal identification numbers (PIN), security tokens, etc.) et de respecter les règles applicables au sein de la Banque en matière de sécurité de l'information. Les externes ne sont autorisés à utiliser les réseaux sans fil de la Banque qu'en se conformant aux instructions internes en vigueur.

5.5. Il est interdit d'utiliser les ressources informatiques mises à disposition par la Banque pour (i) consulter des sites Internet ou participer à des groupes de discussion de nature raciste, sexiste ou pornographique ou incitant à la haine ou à la violence; (ii) télécharger des fichiers ou des programmes lorsque l'utilisateur sait que cela pourrait enfreindre les droits de propriété intellectuelle ou des droits d'autre nature détenus par des tiers; (iii) télécharger ou diffuser des fichiers ou programmes sans appliquer les procédures définies par la Banque; et (iv) télécharger ou diffuser des fichiers ou programmes au sujet desquels la Banque a averti qu'ils pourraient contenir des virus, des vers ou d'autres programmes susceptibles de nuire au bon fonctionnement de l'infrastructure informatique de la Banque.

5.6. La Banque peut effectuer des contrôles, en permanence ou par sondages, quant à l'utilisation par les externes des ressources de la Banque, y compris concernant l'utilisation de la messagerie électronique et de l'Internet ainsi que l'accès aux sources d'information de la

Banque. À cet effet, elle peut collecter et utiliser toutes les données utiles (loggings, relevé et contenu des dossiers et fichiers ouverts, sites consultés, contenu des messages envoyés, durée de l'opération, etc.). La Banque utilise ces données exclusivement dans le cadre de la vérification du respect du présent règlement et des accords passés concernant l'exécution des activités convenues; à ces fins, la Banque peut également transmettre ces informations à l'employeur ou au mandant de la personne concernée.

6. DIRECTIVES EN CAS D'URGENCE

6.1. Lorsque les sirènes fonctionnent en continu, il y a lieu d'évacuer les bâtiments en suivant les instructions données par les haut-parleurs ou par les stewards de la Banque. Il convient de se diriger vers le lieu de rassemblement indiqué par la Banque.

6.2. Les externes doivent, dans la mesure du possible, se joindre à un groupe qui est en train d'évacuer les bâtiments et se présenter au steward du groupe (reconnaissable à un gilet jaune). Dans le cas contraire, les externes doivent quitter les bâtiments en suivant les pictogrammes « issue de secours » et en tenant compte des instructions spécifiques données par les haut-parleurs ou par les stewards de la Banque.

6.3. Avant d'évacuer les bâtiments, il y a lieu de mettre tous les appareils hors service, sauf si une telle opération met en péril la sécurité personnelle. En cas d'incendie, les portes et les fenêtres doivent être fermées pour empêcher un appel d'air. En revanche, en cas d'alerte à la bombe, les portes et fenêtres doivent être ouvertes, ceci afin que l'onde de choc ne soit pas confinée.

6.4. Il est interdit d'utiliser les ascenseurs pendant une évacuation.

7. INSTRUCTIONS PARTICULIERES DE SECURITE ET DE PROTECTION

Les externes sont tenus de respecter à tout moment les instructions particulières de sécurité et de protection les concernant, y compris les dispositions en matière de permis pour toit et de permis de feu délivrés par la Banque. La Banque et ses consultants, ainsi que les responsables de la sécurité sur les chantiers, peuvent, pour certains externes, prévoir des instructions écrites supplémentaires, compte tenu de la nature des activités qu'ils exercent.

8. TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

8.1. Généralités

8.1.1. La Banque collecte et traite des données à caractère personnel relatives aux externes dans le cadre et en vue de (1) l'exécution et du contrôle des activités des externes à la Banque, (2) assurer la sécurité de la Banque, de ses bâtiments et des personnes qui y sont présentes, (3) l'exécution des missions de la Banque et de ses obligations contractuelles et légales en lien avec celles-ci, et (4) faciliter, contrôler et optimiser son fonctionnement interne. Ce traitement de données à caractère personnel repose sur l'article 6.1, (b), (c), (e) et (f), et l'article 9.2, (a) du Règlement général sur la protection des données à caractère personnel[1]. Les données à caractère personnel ainsi traitées concernent entre autres les données d'identification et de contact, les données biométriques et les images de caméra (cf. infra, les articles 8.2 et 8.3), et des données sur l'utilisation de l'infrastructure de la BNB (données de télécommunication, utilisation des logiciels et du matériel informatique mis à disposition, utilisation du parking, ...). La Banque, établie à 1000 Bruxelles, boulevard de Berlaimont 14, est le responsable du traitement de ces données à caractère personnel.

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE (règlement général sur la protection des données), J.O.U.E. n° L 119 du 04 05 2016, pp. 1 à 88.

8.1.2. Seuls les employés de la Banque et les employeurs ou les mandants des externes ont accès à ces données à caractère personnel, et uniquement dans la mesure où ils en ont besoin pour l'accomplissement de leurs tâches (principe du « need-to-know»). Les tiers n'ont pas accès à ces données à caractère personnel, sauf (1) dans les cas prévus par la loi, (2) lorsqu'ils doivent effectuer des missions ou travaux portant sur les applications automatisées de gestion de ces données et (3) si et pour autant que cela soit nécessaire pour l'exécution des missions de la Banque et le respect de ses obligations contractuelles et légales.

8.1.3. La Banque traite les données à caractère personnel des externes pendant la durée strictement nécessaire afin d'atteindre les finalités du traitement susmentionnées.

8.1.4. Pour autant que les conditions définies dans la législation applicable soient remplies, les externes ont le droit :

(1) d'accéder à leurs données à caractère personnel et, le cas échéant, de rectifier lesdites données ;
(2) de s'opposer à ce traitement pour des raisons tenant à leur situation particulière ;
(3) d'obtenir l'effacement de ces données ou la limitation de leur traitement ;
(4) de recevoir les données à caractère personnel les concernant dans un format structuré, couramment utilisé et lisible par machine, et de transmettre ces données à un autre responsable de traitement ;
(5) d'introduire une réclamation auprès de la Commission de Protection de la Vie Privée s'ils considèrent que ce traitement enfreint la législation et la réglementation applicables.

Pour exercer les droits mentionnés aux points (1) à (4), les externes peuvent envoyer un courrier électronique au délégué à la protection des données de la Banque, à l'adresse suivante : dataprotection@nbb.be.

8.2. Données biométriques

Certains locaux ou zones de la Banque ne sont accessibles que moyennant le contrôle des données biométriques. Les externes qui doivent accéder à ces locaux ou zones sont tenus de faire enregistrer leurs données biométriques (par exemple, des informations numériques basées sur l'image des iris). Cet enregistrement a lieu à la loge « Entrée du personnel » au boulevard de Berlaimont, 14.

8.3. Images de caméra

8.3.1. Certains locaux et zones de la Banque sont filmés en permanence, dans le respect de la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance et en conformité avec le protocole du 21 septembre 2007 en matière de vidéosurveillance à la Banque nationale de Belgique. Conformément à l'arrêté royal du 28 mai 2018 portant modification de l'arrêté royal du 10 février 2008 définissant la manière de signaler l'existence d'une surveillance par caméra, des pictogrammes avertissent de la vidéosurveillance à l'entrée des zones filmées.

8.3.2. La vidéosurveillance a pour objectif d'assurer la surveillance générale et de garantir la sécurité et la protection des biens et des bâtiments de la Banque, ainsi que des personnes qui se trouvent dans ces bâtiments. L'enregistrement d'images est effectué dans le but de réunir la preuve d'éventuels faits constitutifs d'infraction ou générateurs de dommages, de rechercher et d'identifier les auteurs des faits, les perturbateurs de l'ordre public, les témoins ou les victimes. Par ailleurs, la Banque enregistre les images pour pouvoir les visionner lorsqu'un incident se produit, pour pouvoir déceler toute irrégularité lors d'une intervention par le personnel de la Banque ou par des tiers, et/ou pour pouvoir écarter tout soupçon d'intention malveillante dans le chef des différentes personnes qui ont effectué l'intervention sur place.

9. INFORMATIONS CONFIDENTIELLES

9.1. La Banque et les membres de son personnel et de ses organes sont soumis à un strict devoir de secret professionnel. La communication d'informations confidentielles aux externes ne peut être effectuée que lorsqu'elle est indispensable à l'exercice des activités convenues et moyennant un engagement de stricte confidentialité de leur part. Toute communication d'informations confidentielles doit se faire dans le respect de la législation et des règles internes de la Banque.

9.2. Les externes ne peuvent divulguer, sur quelque support que ce soit, les informations confidentielles qui leur sont communiquées par la Banque, ni les informations confidentielles auxquelles ils ont accès ou dont ils ont pris connaissance dans le cadre de l'exercice de leur activité à la Banque, à aucune personne, sauf à leur employeur ou à leur mandant si et quand cela s'avère nécessaire à l'exercice de leurs activités à la Banque.

9.3. Les externes ne peuvent utiliser les informations confidentielles que pour l'exercice de leurs activités à la Banque. Il leur est interdit d'utiliser ces informations à des fins privées ou à d'autres fins professionnelles.

9.4. Les externes sont tenus de respecter les dispositions du règlement relatif à la classification et au traitement des informations. Une copie de ce règlement est disponible sur simple demande ou via l'intranet de la Banque.

10. ABUS DE MARCHÉ ET OPÉRATIONS D'INITIÉS

L'attention des externes est attirée sur la réglementation en matière d'abus de marché (le règlement européen (EU) n° 596/2014 du 16 avril 2014 sur les abus de marché et les dispositions de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers qui interdisent les abus de marché et les opérations d'initiés). Les externes sont tenus au strict respect de ces règles. Les infractions à ces dispositions sont passibles de sanctions pénales et d'amendes administratives conformément aux dispositions de la réglementation précitée.

Il est notamment interdit à quiconque dispose d'une information dont il sait ou devrait savoir qu'elle a un caractère privilégié :

a) d'acquérir ou de céder, ou de tenter d'acquérir ou de céder, pour son compte propre ou pour le compte d'autrui, directement ou indirectement, les instruments financiers sur lesquels porte l'information, sauf pour assurer l'exécution d'une obligation d'acquisition ou de cession d'instruments financiers lorsque cette obligation est devenue exigible et résulte d'une convention conclue avant que l'intéressé dispose de l'information privilégiée en question;
b) de communiquer une telle information à une autre personne, si ce n'est dans le cadre normal de l'exercice de son travail, de sa profession ou de ses fonctions;
c) de recommander à un tiers d'acquérir ou de céder, ou de faire acquérir ou céder par une autre personne, sur la base de l'information privilégiée, les instruments financiers sur lesquels porte l'information.

11. REPRESENTATION ET PUBLICITE

11.1. Les externes ne peuvent à aucun moment se faire passer pour un travailleur ou pour un représentant de la Banque, sauf, pour ce qui concerne ce dernier aspect, moyennant un mandat écrit exprès de la Banque.

11.2. Les externes s'engagent à ne pas utiliser la mission qu'ils ont effectuée pour la Banque comme référence ou comme publicité sans l'autorisation écrite préalable de celle-ci.

12. DISPOSITIONS DIVERSES

12.1. Il est interdit de fumer dans les locaux de la Banque, excepté dans les espaces prévus à cet effet.

12.2. Il est interdit d'effectuer des photos, des vidéos ou des enregistrements sonores à la Banque, excepté au cas où ceci est nécessaire pour l'exécution des activités convenues et moyennant l'autorisation écrite préalable du service compétent de la Banque. Des règles spécifiques sont d'application dans certains locaux ou zones de la Banque en ce qui concerne l'introduction d'appareils photo ou vidéo, en ce compris les outils informatiques, le hardware et les téléphones portables équipés d'une possibilité d'enregistrement. Ces appareils doivent, durant la présence de l'externe dans ces locaux ou zones, être entreposés dans une armoire fermant à clé. Des exceptions peuvent être accordées uniquement par le responsable de ces locaux ou zones.

12.3. Les externes peuvent utiliser le parking de la Banque à la condition qu'ils en aient reçu l'autorisation préalable et qu'ils aient rempli les formalités nécessaires. Ils sont tenus de respecter le règlement d'utilisation du parking, dont une copie est affichée aux entrées et sorties habituelles du parking et peut être obtenue sur simple demande.

12.4. Les externes peuvent utiliser le restaurant d'entreprise de la Banque à condition qu'ils en aient reçu l'autorisation préalable et selon les modalités convenues. Les repas ne peuvent être pris que dans les locaux spécialement aménagés à cet effet.

12.5. Les externes ne peuvent pas entrer dans la Banque avec des paquets, sauf moyennant une autorisation préalable du service Sécurité et Surveillance. Les externes entrant avec un paquet doivent déposer celui-ci sous leur propre responsabilité dans une consigne prévue à cet effet.

12.6. Les externes acceptent que les agents de surveillance de la Banque puissent les fouiller et contrôler leurs biens et leurs bagages conformément aux dispositions de la loi du 10 avril 1990 réglementant la sécurité privée et particulière. En cas de vol ou en cas de nécessité imposée par la sécurité, la Banque peut notamment faire vérifier par les personnes mandatées à cette fin le contenu des sacs à main, des serviettes, d'autres bagages ou effets personnels, ainsi que le contenu des casiers de vestiaires ou d'autres aménagements mis à la disposition des externes.

13. ARRÊT DES ACTIVITÉS

Lorsqu'un externe agit en infraction au présent règlement ou à d'autres règles applicables à Banque, la Banque peut mettre fin unilatéralement et sans délai à ses activités en son sein, sans que cela ouvre un quelconque droit à des indemnités.

* *
*