Protocole au sens de l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel conclu entre l'Institut belge des services postaux et des télécommunications (IBPT) et la Police de la navigation (SPN/CIM) pour le partage de données au moyen de l'application logicielle Brabo

(Traduction officieuse de la version néerlandaise originale)

Institut belge des services postaux et des télécommunications
Bâtiment Ellipse C | Boulevard du Roi Albert II 35 | 1030 Bruxelles
T +32 2 226 88 88 | **F** +32 2 226 88 77 | **www.ibpt.be**

TABLE DES MATIÈRES

Article 1er Parties au protocole

1. Le présent protocole au sens de l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel[1] est conclu entre les Parties suivantes :

D'une part :

L'Institut belge des services postaux et des télécommunications (IBPT), Bâtiment Ellipse C, Boulevard du Roi Albert II 35, 1030 Bruxelles, représenté par le Conseil de l'Institut ou son président.

L'IBPT est le responsable du traitement de toutes les données à caractère personnel dans Brabo (voir ci-dessous).

Le DPD de l'IBPT peut être contacté par téléphone au numéro général 02/226 88 88 et par e-mail à l'adresse dataprotection@ibpt.be.

D'autre part :

La Police fédérale / Police administrative / Police de la navigation (SPN)/CIM, (SPF Intérieur), Avenue de la Couronne 145/A, 1050 Ixelles, en tant qu'autorité qui reçoit les données à caractère personnel, représentée par son directeur, le directeur de la Police de la navigation.

Le responsable du traitement des données de l'autorité destinataire est la Police fédérale. Le délégué du responsable du traitement est le directeur de la SPN/DPD.

Le DPD du SPN/CIM est le DPD de la Police de la navigation (SPN). Le DPD est une division du service Stratégie et Politique de la SPN. Le DPD est joignable via l'adresse dga.spn@police.belgium.eu.
Le service DPD de la SPN peut être joint par téléphone au 02/642 62 96 ;

[1] Cet article prévoit ce qui suit : Art. 20. § 1er. *Sauf autre disposition dans des lois particulières, en exécution de l'article 6.2 du Règlement, l'autorité publique fédérale qui transfert des données à caractère personnel sur la base de l'article 6.1.c) et e), du Règlement à toute autre autorité publique ou organisation privée, formalise cette transmission pour chaque type de traitement par un protocole entre le responsable du traitement initial et le responsable du traitement destinataire des données.*
(…)
§ 2. Le protocole est adopté après les avis respectifs du délégué à la protection des données de l'autorité publique fédérale détenteur des données à caractère personnel et du destinataire. Ces avis sont annexés au protocole. Lorsqu'au moins un de ces avis n'est pas suivi par les responsables du traitement, le protocole mentionne, en ses dispositions introductives, la ou les raisons pour laquelle ou lesquelles cet ou ces avis n'ont pas été suivis.
§ 3. Le protocole est publié sur le site internet des responsables du traitement concernés.

Article 2 Objet du protocole

2. Pour son fonctionnement quotidien, il est nécessaire que le SPN/CIM, dans le chef du Carrefour d'Information Maritime de la Police de la navigation - SPN/CIM - dispose d'un maximum de données sur les navires et le trafic maritime dans les eaux belges, tant en mer que sur les voies de navigation intérieures, et donc aussi de toutes les données concernant notamment les radiocommunications maritimes sur ces navires.

3. L'IBPT dispose de toutes les données à caractère personnel qui sont liées aux radiocommunications maritimes, à savoir une liste des licences radio avec le nom du propriétaire, les coordonnées du propriétaire telles que le numéro de téléphone, le numéro de GSM, l'adresse e-mail ainsi que les données à caractère personnel des personnes pouvant être contactées en cas d'urgence. L'IBPT met ces données à la disposition de la Police de la navigation dans les conditions et aux fins déterminées dans le présent protocole.

4. Les fins auxquelles le SPN/CIM utilise les données partagées peuvent être définies comme suit : l'une des missions légales de la Police de la navigation (SPN) est d'assurer un service de police spécialisé sur l'eau. Le Carrefour d'Information Maritime (SPN/CIM) est le point de contact central où sont rassemblées les informations internes et externes permettant de mener à bien les missions de la Police de la navigation. Dans le cadre de cette mission, le SPN/CIM souhaite pouvoir disposer à tout moment des données visées au point 3 afin de pouvoir accomplir ses missions et tâches de police.

Article 3 Description des catégories de données à caractère personnel transférées et leur format

5. Brabo est un outil contenant une base de données gérée par l'IBPT qui compare les données envoyées par les transpondeurs AIS installés à bord des bateaux avec les données de la licence du navire. Il est également possible de consulter la position du navire en ligne.

6. Les catégories de données suivantes sont consultées :

   - **les données d'identification personnelles** du titulaire de la licence radio pour le mariphone et de deux personnes de contact Ces données à caractère personnel concernent le nom, le prénom, le domicile, l'adresse e-mail et le numéro de téléphone du titulaire de la licence et des deux personnes de contact pouvant être contactées en situations d'urgence ;

   - **les données d'identification électroniques** concernent le MMSI (numéro d'identification unique par navire : « maritime mobile service identity »), un indicatif d'appel et le code ATIS (code d'identification unique lié au navire) ;

   - toutes les **technologies** installées à bord : description des équipements et appareils liés aux communications et à la téléphonie tels que VHF, MF-HF, radar, balises de détresse, SART, Inmarsat, Iridium... ;

7. Les données ne sont pas transférées à des tiers. Bien entendu, les données peuvent néanmoins être transférées par le SPN/CIM aux services d'enquête de la police à des fins policières, judiciaires et d'enquête.

8. L'IBPT met ces données à la disposition du SPN/CIM par le biais d'un accès électronique direct - au nom des membres du personnel concernés auprès du CIM - au traitement des données et à la base de données via l'application/interface Brabo.

Article 4 Base légale du traitement

1. En ce qui concerne l'IBPT

9. L'IBPT traite les données à caractère personnel dans Brabo compte tenu de ses compétences légales visées à l'article 14, § 1er, 3°, a, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges, à l'article 13/1, § 1er de la loi du 13 juin 2005 relative aux communications électroniques et aux articles 5 à 17/1 de l'arrêté royal du 18 décembre 2009 relatif aux communications radioélectriques privées et aux droits d'utilisation des réseaux fixes et des réseaux à ressources partagées.

2. En ce qui concerne le SPN/CIM

10. La justification du partage avec la SPN des données susmentionnées de l'IBPT provenant de l'application et de la base de données Brabo se fonde sur les tâches essentielles, les légitimations et les textes réglementaires suivants :

    - Loi du 3 mai 1999 organisant la répartition des compétences suite à l'intégration de la police de la navigation et les brigades de gendarmerie : chapitre 3 concernant les agents chargés du contrôle de la navigation, dans le cadre de la sécurité sur les voies de navigation maritimes ; remplacée, à partir du 1er septembre 2020, par la loi du 8 mai 2019 introduisant le Code belge de la Navigation (M.B. 01.08.2019).

    - Accord de coopération entre l'État fédéral et la Région flamande concernant la création d'une structure de garde côtière et la coopération au sein de celle-ci du 8 juillet 2005 ;

Article 5 Modalités de fonctionnement

11. Le devoir de réserve est assuré par le biais des mesures de protection suivantes. D'autres obligations légales, notamment en ce qui concerne les droits d'accès et les profils d'accès, sont également assurées de cette manière (cf. art. 5 du RGPD) :

    a) identifiant individuel par agent mandaté du SPN/CIM, attribué par l'IBPT ;
    b) seuls les agents mandatés du SPN/CIM disposent d'un accès (exclusif) pour consulter la base de données/Brabo ;

c) les agents mandatés du SPN/CIM n'ont accès à la base de données que dans le cadre des missions de police et dans le cadre des dossiers de police qu'ils gèrent ;
d) L'IBPT organise une séance d'information pour le personnel du SPN/CIM au cours de laquelle les fonctionnalités et les options de Brabo sont expliquées en détail afin que le SPN/CIM puisse travailler avec Brabo de manière rapide et efficace et puisse immédiatement exploiter pleinement ses possibilités ;
e) Tous les membres du personnel du SPN/CIM sont liés par le secret professionnel et le code de déontologie des services de police. S'ils enfreignent ces derniers, ils commettent une infraction pénale et/ou disciplinaire.

Article 6 Conditions d'accès et profilage

12. Le chef de service du SPN/CIM est tenu d'envoyer au chef du service Attributions une liste signée des personnes, en principe toutes celles qui travaillent pour le SPN/CIM, et à qui l'IBPT accordera un accès individuel à Brabo ; cette liste sera tenue à jour au SPN/CIM.

13. Les deux Parties sont tenues de prendre les mesures de protection nécessaires pour garantir qu'aucune donnée à caractère personnel ne puisse fuiter de cette liste lors de l'envoi de la liste des noms.

14. L'IBPT est chargé de la création d'un identifiant et d'un mot de passe[2] et est responsable de l'octroi de chaque nouvel accès ; l'IBPT transmet au SPN/CIM les coordonnées de la personne de contact auprès de l'IBPT qui active l'accès électronique au Brabo. Cette activation a lieu après la transmission de la liste par le SPN/CIM. Toute mise à jour de ces listes ou échange concernant les noms, les agents mandatés, etc. doit être adressée au chef de service du SPN/CIM à l'adresse dga.spn.mik@police.belgium.eu.

15. Le SPN/CIM informe à l'avance l'IBPT de tout changement donnant lieu à une mise à jour de cette liste de noms ; si possible, le SPN/CIM informe l'IBPT 14 jours avant que les droits d'accès ne doivent être supprimés, par exemple, après une mobilité du service ou un départ à la retraite ; il en va de même pour un nouveau membre du personnel (14 jours avant le début du service) ;

16. Lorsque, par mesure d'ordre, le SPN/CIM supprime du SPN/CIM un utilisateur ayant une autorisation et un profil d'accès octroyé à la suite d'un abus - soit dans Brabo, soit pour d'autres raisons qui le justifient - le SPN/CIM demandera, dès que cet abus sera établi, de bloquer son accès à Brabo ;

17. Dans les cas précités où l'accès d'un membre doit être bloqué d'urgence, le SPN/CIM prend immédiatement contact avec le responsable Brabo de l'IBPT. Le nom de la personne responsable et son adresse e-mail seront communiqués au SPN/CIM.

[2] Le mot de passe attribué par l'IBPT doit être modifié immédiatement par le membre du personnel du SPN/CIM concerné.

18. En cas de problème de traitement de données (base de données ou serveur de l'IBPT inaccessible aux services de police), le SPN/CIM peut contacter la ligne d'assistance ou la personne de contact suivante pour demander des données radiophoniques ad hoc au service Maritime de l'IBPT à l'adresse e-mail maritime@ibpt.be. Cette procédure via l'adresse e-mail s'applique à tous les agents mandatés qui ont (déjà) un accès électronique à Brabo.

19. Brabo contient une liste de liens permettant de consulter à tout moment les coordonnées des bateaux en cas d'urgence (uniquement pour la base de données MARS de l'UIT et uniquement pour les coordonnées des personnes à contacter en cas d'urgence). Afin de garantir que les coordonnées des personnes à contacter en cas d'urgence restent suffisamment accessibles, l'IBPT recommande de sauvegarder ces liens également en dehors de Brabo, afin que cette partie du service soit toujours garantie.

20. Le SPN/CIM informe le responsable Brabo de l'IBPT d'une mise à jour de cette liste dès que la liste des agents mandatés change.

Article 7 Mesures de sécurité existantes et supplémentaires dans le cadre du RGPD[3]

1. Introduction

21. La SPN et le SPN/CIM prennent toutes les mesures nécessaires pour protéger les données à caractère personnel conformément à la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

22. Le SPN/CIM déclare fournir les garanties nécessaires pour que le responsable du traitement ou son mandataire puisse à tout moment sauvegarder les droits des personnes concernées, comme le prévoit la loi.

2. Mesures existantes

23. Les mesures qui ont déjà été mises en place auprès de la SPN et qui ont été incluses dans la déclaration de traitement sont les suivantes :

    - Infrastructures et mesures générales de sécurité auprès du SPN/CIM Infrastructure

    - bâtiment protégé et sécurisé sur un site de défense gardé en permanence avec surveillance

[3] Cf. RGPD, considérant 30 : *Les personnes physiques peuvent se voir associer, par les appareils, applications, outils et protocoles qu'elles utilisent, des identifiants en ligne tels que des adresses IP et des témoins de connexion («cookies») ou d'autres identifiants, par exemple des étiquettes d'identification par radiofréquence. Ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes.*

par caméra : sécurité spécifique renforcée avant l'accès à la base navale + badge supplémentaire pour le bâtiment où se trouve le SPN/CIM ;

- accès limité au site et au bâtiment pour le personnel du SPN/CIM uniquement ;

- site gardé par du personnel de défense armé ;

- dossier de la sécurité générale des bâtiments dans le cadre de la lutte contre le terrorisme ;

- Personnel

- prestation de serment ;

- tous les membres du personnel du SPN/CIM ont une habilitation de sécurité (UE-OTAN-BE), niveau minimum « secret ».

- Organisation

- lignes directrices générales sur l'utilisation de l'identifiant et du mot de passe sécurisé ;

- Technologie de traitement et communication

- les données consultées ne sont pas conservées auprès de la SPN mais peuvent uniquement être consultées en ligne ;

- réseau interne Hilde : l'accès des agents mandatés est limité au personnel du SPN/CIM. Uniquement accessible aux collaborateurs, officiers ; le réseau informatique interne Hilde de la Police fédérale est un tampon de sécurité de première ligne ou une passerelle électronique pour pouvoir consulter les données de Brabo en deuxième ligne.

- Brabo n'est accessible que sur des PC réseau du SPN/CIM ; aucune donnée radiophonique obtenue via l'IBPT n'est conservée sur un serveur du SPN/CIM ou sur tout autre support de données au sein du SPN/CIM.

3. Données de connexion supplémentaires

24. Chaque agent mandaté du SPN/CIM reçoit un identifiant et un mot de passe individuels. En outre, le SPN/CIM utilise une procédure de connexion interne pour conserver certaines données de connexion, pour lesquelles les champs nécessaires sont déjà fournis dans Brabo, et qui font partie de la procédure de consultation de Brabo au sein de la SPN : celle-ci consiste à demander à chaque personne qui se connecte de remplir le champ « suivi » avec la raison/justification de son activité de consultation et l'inclusion d'une référence au numéro de dossier ou une autre référence disponible liée à la raison de sa consultation, afin que la justification soit toujours vérifiable et traçable.

4. Collaboration au rapport d'analyse d'impact relative à la protection des données

25. La SPN s'engage à collaborer à tout moment et gratuitement à l'élaboration ou à la mise à jour d'un rapport d'analyse d'impact relative à la protection des données (AIPD).

5. Accès à Brabo

26. Seuls les membres du personnel de l'IBPT qui ont besoin de Brabo dans le cadre de leurs tâches ont accès à l'outil. Ils disposent également d'un identifiant et d'un mot de passe uniques.

Article 8 Règles relatives aux communications utilisées

27. Le SPN/CIM respecte les règles suivantes :

    a. Les données consultées ne sont pas conservées auprès de la SPN mais peuvent uniquement être consultées en ligne. Brabo n'est accessible que sur les PC réseau du SPN/CIM ; aucune donnée n'est conservée sur un serveur du SPN/CIM ;
    b. En ce qui concerne la communication relative aux autorisations et à l'accès aux données : voir ci-dessus ;
    c. En ce qui concerne la communication avec les personnes concernées et l'exercice des droits : La police peut invoquer l'article 23 du RGPD/article 36 et suivants de la loi du 30/07/18, pour limiter certains droits (par exemple la protection d'une enquête en cours, les infractions, etc.)

28. Étant donné que l'activité de traitement pour le SPN/CIM concerne des traitements opérationnels, il s'agit d'un accès indirect et les personnes concernées peuvent s'adresser directement au COC pour l'exercice de leurs droits. Si nécessaire, le COC (« Controle Orgaan/Organe de Controle ») prendra alors contact avec la SPN.

Article 9 Principe de proportionnalité et exigences de protection des données dès la conception

29. Par le biais du présent protocole, le destinataire déclare qu'il respectera le principe de proportionnalité et qu'il se conformera strictement à l'extraction et à la consultation des données à caractère personnel nécessaires à l'accomplissement de ses tâches de police légales, placées dans un cadre légal plus large sans que les informations demandées soient disproportionnées par rapport à ce à quoi elles devraient et pourraient servir.

30. L'IBPT qui accorde l'accès aux données à caractère personnel prend les mesures spécifiques nécessaires afin que les exigences de protection des données dès la conception et par défaut soient respectées et déclare qu'il prendra les mesures nécessaires afin que le principe de proportionnalité soit respecté à tout moment.

Article 10 Modalités des droits de la personne concernée auprès du destinataire

31. Toute personne concernée peut contacter le COC, soit l'Organe de contrôle de la Police fédérale, à l'adresse e-mail info@organedecontrole.be.

32. La police peut invoquer l'article 23 du RGPD/article 36 et suivants de la loi du 30/07/18, pour limiter certains droits (par exemple la protection d'une enquête en cours, les infractions, etc.)

33. Étant donné que l'activité de traitement pour le SPN/CIM concerne des traitements opérationnels, il s'agit d'un accès indirect et les personnes concernées peuvent s'adresser directement au COC pour l'exercice de leurs droits. Si nécessaire, le COC contactera alors la SPN.

34. En ce qui concerne l'IBPT : toute personne concernée qui estime que ses droits en matière de traitement des données à caractère personnel n'ont pas été respectés peut contacter l'Autorité de protection des données (APD), rue de la Presse 35, 1000 Bruxelles à l'adresse e-mail suivante : contact@apd-gba.be.

Article 11 Obligations

35. Conformément aux articles 32 à 34 du RGPD, les Parties s'engagent à protéger leurs données à caractère personnel contre toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé aux données en question.

36. En signant le présent protocole, l'IBPT confirme qu'il a pris les mesures techniques et organisationnelles appropriées et qu'il a veillé et continuera à veiller à ce que les infrastructures TIC auxquelles sont connectés les équipements intervenant dans le traitement des données à caractère personnel garantissent la confidentialité et l'intégrité de ces données à caractère personnel.

37. L'IBPT s'engage à veiller à ce que toutes les données contenues dans Brabo soient régulièrement mises à jour afin que la base de données réponde à l'exigence de données à caractère personnel actuelles, correctes et transparentes, afin d'éviter l'utilisation ou la conservation excessive de données à caractère personnel erronées ou obsolètes ;

38. Toutes les informations dont le personnel de l'IBPT et les sous-traitants doivent prendre connaissance dans le cadre du présent protocole, tous les documents confiés au partenaire et toutes les réunions auxquelles le partenaire participe, sont strictement confidentielles.

39. L'IBPT s'engage à garder secrètes toutes les informations confidentielles, de quelque nature qu'elles soient, qui seront communiquées ou dont il sera pris connaissance dans le cadre du présent protocole, tant pendant qu'après leur traitement.

40. L'IBPT garantit que son personnel et son (ses) sous-traitant(s) traiteront ces informations de manière confidentielle et s'engage à ne pas les communiquer à des tiers. Seules les données strictement nécessaires à l'exécution des tâches seront communiquées au personnel et au(x) sous-traitant(s) du partenaire.

41. Les Parties s'engagent à respecter les obligations découlant de l'exercice des droits de la personne concernée.

Article 12 Modification du protocole

42. Si les Parties le jugent nécessaire, le présent protocole sera révisé.

43. Le présent protocole ne peut être modifié que par écrit, d'un commun accord entre les deux Parties.

44. Tout amendement entrera en vigueur à la date spécifiée dans le protocole modifié.

Article 13 Litiges et sanctions

45. En cas de difficultés dans la mise en œuvre ou de violation du présent protocole, les Parties s'engagent à se concerter et à coopérer en vue de trouver une solution à l'amiable dans les meilleurs délais.

46. Un partenaire est responsable des dommages que l'autre Partie subirait si le partenaire lui-même, le sous-traitant ou les membres du personnel du partenaire ne respectai(en)t pas les obligations dans le cadre du présent protocole.

47. Dès qu'une violation du protocole est constatée, par laquelle les droits de la personne concernée sont violés, les Parties respectives doivent immédiatement informer l'APD et/ou le COC.

Article 14 Entrée en vigueur

48. Le protocole entre en vigueur le premier jour ouvrable suivant sa signature et est valable pour une durée illimitée.

Article 15 Avis du DPD

49. Le DPD de l'instance publique fédérale qui détient les données à caractère personnel transférées/consultées, en l'occurrence l'IBPT, a émis un avis :

Positif - ~~Négatif~~ (biffer la mention inutile)

~~*(à compléter en cas d'avis négatif du DPD) :*~~
~~Bien que l'avis du DPD ait été négatif, le président de l'IBPT, en tant que responsable du traitement, a tout de même signé le présent protocole pour les motifs suivants :~~
.....

50. Le DPD de l'instance publique fédérale auquel les données à caractère personnel transférées sont destinées, en l'occurrence la DGA/SPN, a émis un avis :

Compte tenu de toutes les mesures de sécurité de nature différente qui s'appliquent à plusieurs niveaux au sein du CIM et de la SPN en général et au SPN/CIM en particulier, on peut conclure que la sécurité des données à caractère personnel dans le cadre du présent protocole est garantie à un degré élevé dans les opérations du SPN/CIM. Les accords contenus dans le présent protocole y contribuent également dans une mesure proportionnelle.
Il n'y a aucune raison de penser que les droits de la ou des personne(s) concernée(s) seraient compromis de quelque manière que ce soit. La personne concernée peut faire valoir ses droits en matière de protection des données à caractère personnel par les voies appropriées, comme décrit également au paragraphe « Modalités des droits de la personne concernée » du présent protocole.
Au sein de la SPN, le service du DPD signale la nécessité de prendre une décision sur l'établissement ou non d'un rapport d'analyse d'impact relative à la protection des données pour le traitement interne des données à caractère personnel par le SPN/CIM, et ce, dès que les mesures de distanciation sociale liées au Covid-19 le permettront.

Positif - ~~Négatif~~ (biffer la mention inutile)

~~(à compléter en cas d'avis négatif du DPD) :~~

~~Bien que l'avis du DPD ait été négatif, le responsable du traitement de la Police fédérale, ou son mandataire, dans le chef du directeur de la Police de la navigation, a tout de même signé le présent protocole pour les motifs suivants :~~ .....

Date de la signature : .....

Pour accord (IBPT) Pour accord (SPN/CIM)

Président du Conseil de l' IBPT Directeur de la SPN

Michel van Bellinghen Dirk Van Nespen