Annexe 1.1 convention relative aux utilisateurs de données structure de base bibliothèque numérique

PARTIE 1 : GENERALITES

1. Contexte

Les objectifs de la structure de base bibliothèque numérique ("Basisinfrastructuur Digitale Bibliotheek") sont :
● Faciliter les processus de backoffice des bibliothèques publiques, les uniformiser et les rendre plus efficaces grâce à une approche supra locale dans un système de bibliothèque unique;
● Offrir une base de données unique des emprunteurs : chaque emprunteur est répertorié une seule fois et les données sont toujours actualisées;
● Offrir un meilleur service pour les utilisateurs finaux grâce à l'approche supra locale des sites web des bibliothèques uniques, qui sont et seront optimalisés pour le site web, le catalogue et "Mijn Bibliotheek services" de la bibliothèque.
Quant à l'objet de la convention "Overeenkomst Basisinfrastructuur Digitale Bibliotheek" (ci-après : la Convention), la "VGC" accepte que "Cultuurconnect" agit en tant que responsable du traitement au sens de la législation de la vie privée, et qu'elle agit elle-même en tant qu'utilisateur.

La qualification de la "VGC" s'étend jusqu'aux bibliothèques publiques néerlandophones dans la Région de Bruxelles-Capitale qui utiliseront la "Basisinfrastructuur Digitale Bibliotheek". Quant aux Communes concernées, la "VGC" prévoira les dispositions nécessaires y relatives, de sorte que toutes les dispositions, droits/possibilités, responsabilités et obligations, intégrés dans cette annexe, soient également d'application pour les Communes concernées.

En tant que responsable du traitement, "Cultuurconnect" a désigné des marchés et a conclu des conventions avec des prestataires de services IT de la "Basisinfrastructuur Digitale Bibliotheek" (voir art. 1 §3 de la Convention), en fonction de son développement et de sa gestion. Ces prestataires de services IT sont des sous-traitants de données à caractère personnel dans le cadre des conventions concernées et "Cultuurconnect" établit des conventions concernant ces traitements avec ces prestataires de services IT. Ces 3 conventions en question ont été établies sur la base des "mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel" de la Commission de la protection de la vie privée (maintenant : l'Autorité de protection des données).

Quant au traitement des données personnelles, la "VGC" accepte de ne pouvoir agir que conformément à la Convention et à cette annexe.
Le groupe de pilotage "Basisinfrastructuur Digitale Bibliotheek", dans lequel est représenté le secteur des bibliothèques publiques (voir art. 3 de la Convention), sera également impliqué dans le traitement des données à caractère personnel mais, vu que "Cultuurconnect" est le responsable du traitement, ce groupe ne joue pas de rôle directif dans ce domaine.
Une modification de cette annexe par "Cultuurconnect" sera communiquée à la "VGC" par courrier et/ou courriel. La date de l'envoi est la date de la notification. Si la "VGC" n'accepte pas la modification proposée, elle a le droit de résilier la Convention par lettre recommandée, sauf si la modification est nécessaire pour se conformer aux lois et règlementations contraignantes qui ont été changées.

Une telle résiliation doit avoir lieu dans les 3 mois après la notification de la modification; la date de l'envoi de la lettre recommandée étant la date de la résiliation.

2. Définitions

Cette Annexe utilise les mêmes définitions qui sont utilisées dans les lois et les règlementations qui sont d'application concernant le traitement de données à caractère personnel, dont en tout cas le Règlement Général sur la Protection des Données (RGDP).

3. Organisation de la sécurisation des informations

3.1 Politique de sécurisation des informations et délégué à la protection des données

Lors de la réalisation de la "Basisinfrastructuur Digitale Bibliotheek", "Cultuurconnect" utilise des normes strictes quant aux droits des utilisateurs et la vie privée des utilisateurs finaux; la responsabilité sociale et le respect pour la collaboration étant basés sur l'ouverture et la transparence.
"Cultuurconnect" suit une politique de sécurisation des informations écrite qui stipule les stratégies et les mesures nécessaires pour protéger les données et met à jour cette politique régulièrement sur la base d'évaluations. "Cultuurconnect" adopte les mesures techniques et organisationnelles appropriées, exigées par l'article 32 RGDP.
"Cultuurconnect" a un délégué à la protection des données qui répond aux exigences du RGDP.
"Cultuurconnect" demandera une déclaration sur l'honneur de tous les collaborateurs qui auront accès aux données à caractère personnel dans le cadre de leur fonction, déclaration dans laquelle ils confirment qu'ils n'accèdent à ces données que dans le cadre strict de leur fonction.

3.2 Plan de gestion en cas de violations de données

"Cultuurconnect" dispose d'un plan de gestion en cas d'incidents de sécurité qui puissent nuire à la disponibilité, l'intégrité et/ou la confidentialité des données à caractère personnel (violation de données à caractère personnel, voir art. 4 RGDP). Cette procédure fixe les démarches nécessaires en cas de la découverte d'une violation de données et détermine qui doit régler l'incident pour rétablir la situation normale.
"Cultuurconnect" gardera un inventaire des violations de données.

3.3 Gestion des violations de données

En cas d'une violation de données, "Cultuurconnect" respectera les obligations légales en vigueur.
"Cultuurconnect" communiquera dans les plus brefs délais toute violation de données à la VGC. La notification d'une violation de données qui fait l'objet d'une obligation légale de notification, sera communiquée à l'intention de la personne de contact de la "VGC", mentionnée au 4.7.2. Une telle notification a lieu au plus tard dans les 48 heures après la découverte d'un incident, et comprend les données suivantes, si elles sont connues: (a) la nature de l'incident; (b) la date et l'heure de l'incident et de la découverte de l'incident; (c) le nombre de personnes concernées et affectées par l'incident; (d) les catégories de données à caractère personnel concernées; (e) les mesures - p.ex. le cryptage ou d'autres mesures techniques et organisationnelles - qui ont été prises pour régler l'incident, y compris les mesures prises pour limiter les conséquences négatives éventuelles; (f) le nom et les

données de contact du délégué à la protection des données ou d'une autre personne de contact; et (g) une description des conséquences probables de l'incident.

3.4 Demandes de l'Autorité de contrôle

"Cultuurconnect" répondra aux demandes de l'Autorité de contrôle, et aux communications, avis éventuels ou injonctions de l'Autorité de contrôle dans le délai fixé par l'Autorité de contrôle.

3.5 Demandes des personnes concernées

Les personnes concernées peuvent faire valoir leurs droits de plusieurs façons. Tous les droits peuvent être exercés via le délégué à la protection des données de "Cultuurconnect", certains droits peuvent être exercés via "Mijn Bibliotheekprofiel" par la personne même, ou au comptoir de la bibliothèque où la personne concernée est inscrite. "Cultuurconnect" s'engage à être le point de centralisation pour n'importe quelle demande de personnes concernées dans le cadre de l'exercice de leurs droits.

3.6 Documentation
"Cultuurconnect" gardera toute documentation pertinente concernant la sécurisation des informations et fait régulièrement des mises à jour. "Cultuurconnect" ne refusera pas - sur la base de motifs injustifiés - une demande de consultation de la part de la "VGC" concernant le traitement de données à caractère personnel repris dans la Convention.

4. Données générales concernant le traitement des données à caractère personnel

4.1 Catégories de personnes concernées

Utilisateurs finaux des bibliothèques publiques néerlandophones dans la Région de Bruxelles-Capitale
Collaborateurs des bibliothèques publiques néerlandophones dans la Région de Bruxelles-Capitale
Collaborateurs de la "VGC"
Collaborateurs de "Cultuurconnect"

4.2 Catégories de données à caractère personnel

Concernant les utilisateurs finaux :
● Identification: nom (le cas échéant provenant de la CI-e);
● Données de contact : résidence principale (le cas échéant provenant de la CI-e), une adresse supplémentaire éventuelle (p.ex. lieu de travail, kot étudiant), numéro de téléphone, adresse e-mail;
● Données de connexion : nom d'utilisateur, mot de passe;
● Caractéristiques personnelles : sexe, date de naissance (le cas échéant provenant de la CI-e);
● Numéro du Registre National et/ou le NISS;
● Données de la bibliothèque : numéro de la carte de bibliothèque, données concernant l'abonnement, l'historique des emprunts (quoi, quand, retour, réservations), l'historique des paiements (montants dus, montants payés et date du paiement), l'historique des messages (lettres reçues);
● Données des activités de l'utilisateur, p.ex. l'adresse IP;

● Préférences de communication : la délivrance de message p.ex. par courriel ou par courrier, préférence de la langue;
● Données anonymes et agrégées dans le cadre de l'utilisation du site web, p.ex. type du navigateur, le programme d'exploitation utilisé, les pages consultées;
● Listes des titres favoris;
Concernant les collaborateurs de la bibliothèque, "VGC" ou "Cultuurconnect":
● Identification : nom;
● Données de contact : l'adresse e-mail;
● Données de connexion : nom d'utilisateur, mot de passe;
● Données de la bibliothèque : la bibliothèque;
● Données des activités de gestion par les collaborateurs.

4.3 Lieu de conservation des données à caractère personnel

Toutes les données collectées dans le cadre de l'utilisation de la "Basisinfrastructuur Digitale Bibliotheek", seront conservées sur une localisation externe au sein de l'UE en fonction de la gestion effective des systèmes IT par les fournisseurs IT:
● Les données introduites dans le système de la bibliothèque, ainsi que les données de connexion et des activités des collaborateurs de la bibliothèque, de la "VGC" et de "Cultuurconnect", sont conservées aux Pays-Bas (avec disaster recovery en Allemagne).
● Les données anonymes et agrégées et l'adresse IP, collectées dans le cadre de l'utilisation du site web de la bibliothèque via des cookies, ainsi que les données de connexion et des activités des collaborateurs de la bibliothèque, de la "VGC" et de "Cultuurconnect", sont conservées en Belgique.
● Les données mentionnées en fonction de l'enregistrement et de la connexion sur "Mijn Bibliotheek", ainsi que les données de connexion et des activités des collaborateurs de la bibliothèque, de la "VGC" et de "Cultuurconnect", sont conservées en Irlande.
"Cultuurconnect" prend les mesures nécessaires pour prévoir un back-up des données.
"Cultuurconnect" ne transmettra jamais des données à caractère personnel à des tiers, sauf si cela est nécessaire pour le traitement envisagé (y compris les possibilités de back-up).
Transmettre des données à des tiers est explicitement interdit, sauf moyennant l'accord explicite de "Cultuurconnect" et à condition que la sécurité selon les normes du RGDP soit garantie.

4.4 Mesures de sécurité

Via les conventions de traitement avec les prestataires de services IT (voir également ci-dessus, 1), "Cultuurconnect" a fixé beaucoup de mesures de sécurité. Les grandes lignes :

A. Mesures de sécurité physiques
Contrôle physique et contrôle de l'environnement
• Sécurité 24h sur 24
• Contrôles pour éviter des accès non autorisés
• Toutes les portes, y compris les cages, sont équipées avec des ‘proximity cards’ et des ‘biometric hand geometry readers’
• Closed- Circuit Television (CCTV) : surveillance numérique par caméra de l'ensemble du centre de données, y compris les cages et le système d'archivage
• CCTV intégré avec contrôle d'accès et système d'alarme
• Détecteurs de mouvement liés aux sources lumineuses et couverture CCTV
• Contrôle et screening des produits entrants
• Identification des visiteurs entrants et accompagnement vers la destination dans le centre de données
• La réception et l'envoi de produits sont séparés des lieux de collocation

• Système HVAC pour créer des conditions optimales (température, courants d'air et humidité). Le Downtime lié aux problèmes avec le matériel est donc minimale.
Afin de garantir la continuité des services, les mesures mentionnées ci-dessous sont au minimum prises concernant la prévention, la détection et l'approche de menaces physiques telles que des incendies ou des inondations.
• Systèmes d'extinction d'incendies
• Réglage de l'humidité et de la température
• Sol élevé qui permet une circulation continue de l'air
• Connecté à l'Internet via des connexions routées redondantes de plusieurs fournisseurs de services Internet, gérées à partir de plusieurs Points of Presence du fournisseur de la télécommunication.
• Alimentation souterraine pour les équipements d'utilité publique
• Systèmes d'électricité qui ne peuvent pas être perturbés (UPS)
• Unités de distribution d'alimentation redondantes (PDU's)

• Générateurs diesel avec stockage sur site du carburant diesel à chaque emplacement du centre de données
• Sauvegarde nocturne des données
• Tests réguliers de la restauration des sauvegardes
• Reprise après sinistre

B. Sécurité des réseaux

Mesures de sécurité dans le centre de données :
• Connecté à l'internet à travers de redondant, des liens provenant de différents fournisseurs de services internet de plusieurs fournisseurs de télécommunications Points of Presence qui parcourent de diverses routes.
• Les pare-feu et les *edge routers* bloquent les protocoles non autorisés.
• Les pare-feu internes séparent le trafic entre les niveaux application et base de données.
• Les répartiteurs de charge fournissent des proxys pour le trafic interne
• Le processeur utilise diverses méthodes pour prévenir, détecter et supprimer les logiciels malveillants
• Des audits de sécurité sont périodiquement effectués par des tiers.
• Le personnel de sécurité de l'information des processeurs surveille les notifications provenant de diverses sources et les alertes provenant des systèmes internes pour identifier et gérer les menaces.
• Cryptage de la base de données (basé sur la planification du développement prioritaire).

• Sécurité du trafic entre client et serveur (réseau sécurisé ou HTTPS).

Sécurisation du lien Ma bibliothèque (HTTPS).

Sécurisation des liens entre le Registre national et le système unifié des bibliothèques (voir aussi 4.5).

C. Sécurité logique

Accès restreint et contrôlé (uniquement) pour les employés autorisés des fournisseurs de services informatiques (principe du *need-to-know*), avec gestion individuelle des identifiants et des mots de passe, et expiration périodique du mot de passe.

Définition claire des rôles de l'administrateur avec accès (uniquement nécessaire) aux données personnelles

- Une bibliothèque ne voit que les données de ses propres clients (abonnement à sa propre bibliothèque ou groupe de collaboration) ;
- Les rôles d'utilisateur des administrateurs peuvent être diversifiés afin que le principe du *need-to-know* soit toujours respecté autant que possible. Le rôle utilisateur d'un administrateur détermine les données que l'administrateur verra.
- Utilisation de logins de gestion personnelle avec un certain rôle d'autorisation/utilisateur, renforçant l'utilisation de mots de passe forts. La structure obligatoire du mot de passe est paramétrable dans le système. L'intention est de rendre l'expiration du mot de passe paramétrable pour le système (voir aussi PARTIE 2, 2.2 ci-dessous).

Enregistrement sûr et informé des utilisateurs finaux à l'aide d'un mot de passe personnel avec contrôle de sécurité et déconnexion automatique.

D. Enregistrement

Une journalisation étendue est disponible dans le système. Cette journalisation garantit que, dans certains cas, les informations relatives à l'accès aux données à caractère personnel (quelles données à caractère personnel, par qui, quand, par quelle action) peuvent être récupérées afin de détecter tout accès non autorisé et autres opérations.

Les recherches de données personnelles (journal d'audit) sont conservées pendant une période suffisante (au moins 6 mois en ligne et 10 ans hors ligne) afin de permettre un contrôle plus efficace. L'accès à ces journaux d'audit n'est possible que pour les employés autorisés de Cultuurconnect.

4.5 Lien avec le Registre national

Cultuurconnect a obtenu deux autorisations générales pour le secteur des bibliothèques publiques en Flandre et à Bruxelles. Les communes peuvent démontrer, sur demande individuelle, qu'elles remplissent les conditions énumérées dans l'autorisation générale, afin de pouvoir effectuer le traitement des données qui y est décrit. Il s'agit de :

- ***Délibération RR n° 28/2009 du 18 mai 2009 : demande de Bibnet au profit des bibliothèques publiques néerlandophones en Flandre et à Bruxelles pour obtenir l'accès aux données d'information du Registre national pour l'identification et la gestion de leurs membres (RN/MA/2009/013) ;***
- ***Délibération n° 18/020 du 6 février 2018 relative à l'accès des bibliothèques publiques néerlandophones de Flandre et de Bruxelles aux registres des Banques Carrefour pour l'identification et la gestion de leurs membres (demande de l'association Cultuurconnect).***

Ces autorisations générales donnent aux communes/bibliothèques qui ont soumis une demande approuvée (et tant qu'elles remplissent les conditions imposées), dans le cadre de l'identification et de la gestion de leurs membres, le droit :

- ***D'avoir accès à certaines données d'information du registre national, à savoir celles mentionnées à l'article 3, premier alinéa, 1°, 2° et 5°, WRR : les nom, prénoms, date de naissance et lieu principal de résidence des personnes concernées ;***
- ***d'utiliser le numéro d'identification du registre national ;***
- ***d'avoir accès aux mêmes données personnelles à partir des registres des Banques Carrefour (nom, prénoms, date de naissance et résidence principale) ;***
- ***utiliser le numéro d'identification attribué par la Banque Carrefour de la Sécurité Sociale (cet usage est gratuit au sens de l'art. 8 §2 de la loi du 15 janvier 1990 portant création et organisation d'une Banque Carrefour de la Sécurité sociale).***

Les communes/bibliothèques qui n'auraient pas d'autorisation individuelle au moment de la signature de l'accord s'engagent à lancer la procédure de demande le plus rapidement possible et à faire tout leur possible pour obtenir cette autorisation.. Les communes peuvent demander une autorisation générale en utilisant les formulaires et l'adresse de contact disponibles sur le site web de l'Autorité pour la protection des données.

Cultuurconnect est responsable de la connexion technique entre le système de bibliothèque et le RR/la BCSS en fonction de l'exactitude et de la mise à jour des données de l'utilisateur final. Cultuurconnect prendra les mesures techniques adéquates pour empêcher l'accès à des données personnelles autres que celles couvertes par les mandats. Pour ce lien, un appel est lancé auprès de *Dienstenintegrator Agentschap Informatie Vlaanderen* (MAGDA). Ce lien assure une synchronisation continue entre la base de données des emprunteurs du système de la bibliothèque et les données du Registre national auxquelles l'accès est accordé, garantissant ainsi une mise à jour et une exactitude continue des données de la base de données des emprunteurs.

Cultuurconnect demandera, lorsque cela est possible et pertinent, une extension des autorisations (en ce qui concerne les catégories de données personnelles). Cultuurconnect en discute avec le comité directeur de l'infrastructure de base de la bibliothèque numérique.

4.6 Développements et liens futurs

Cultuurconnect souhaite que la bibliothèque numérique de l'infrastructure de base reste efficace, pertinente et à jour et développera, si nécessaire ou souhaitable, des développements et/ou des liens avec d'autres systèmes, en vue, entre autres choses :

- de tenir à jour les services prévus par la convention avec les derniers développements,
  l'évolution et les tendances (technologiques),
- à des fins culturelles supra-locales,
- la poursuite de l'innovation de la politique culturelle locale, ● changements dans le cadre législatif et réglementaire.

Cultuurconnect, en tant que responsable du traitement, prendra toujours toutes les mesures appropriées pour protéger les données personnelles.

De tels développements feront toujours l'objet d'une discussion préalable avec le comité directeur de l'infrastructure de base de la bibliothèque numérique visé à l'article 3 de la convention. Cultuurconnect en informera toujours le VGC en temps utile et avec soin par courrier et/ou e-mail. La date d'expédition est égale à la date de la notification. Cela peut donner lieu soit à une nouvelle fonctionnalité qui peut être achetée à la discrétion de la VGC (si nécessaire, un avenant à la convention, avec éventuellement un ajustement tarifaire, sera conclu), soit à une intégration qui fait partie intégrante de l'infrastructure de base de la Bibliothèque numérique. Dans ce dernier cas, la VGC acquiert le droit de résilier le contrat par lettre recommandée, à moins que l'intégration n'ait pour but de mettre l'infrastructure de base en conformité avec la législation et la réglementation modifiées. Cet avis doit être donné dans un délai de trois mois à compter de la date de notification de la modification, la date d'envoi de la lettre recommandée étant égale à la date de la résiliation.

4.7 Contacts

4.7.1 Délégué à la protection des données

dpo@cultuurconnect.be

VGC
Wannes Van Herreweghen
dpo@vgc.be

4.7.2 Coordonnées en cas de fuite de données

Cultuurconnect
servicedesk@cultuurconnect.be
dpo@cultuurconnect.be

VGC
Wannes Van Herreweghen
dpo@vgc.be

5. Données spécifiques concernant la communication unique liée à la connexion de la VGC au système de bibliothèque unifiée

En raison de la connexion de la VGC au système de bibliothèque unifié, des données personnelles ponctuelles provenant de l'environnement de bibliothèque numérique des communes/bibliothèques seront communiquées à Cultuurconnect. Nonobstant le fait que l'ensemble de la présente annexe s'applique à cette communication, un certain nombre de données supplémentaires spécifiques à cette communication sont incluses ci-dessous, conformément au décret sur le trafic électronique de données administratives du 18 juillet 2008 (egovdecreet; voir "protocole" à l'article 8).

5.1 Objet de la communication

Lors de la connexion de la VGC au système de bibliothèques unifié, les données personnelles suivantes provenant de bibliothèques déjà existantes dans les bibliothèques publiques néerlandophones de la Région de Bruxelles-Capitale seront communiquées:

- Données d'identification : nom (tiré de la carte d'identité électronique, le cas échéant) ;
- Coordonnées : lieu de résidence principal (le cas échéant, via l'eid), adresse supplémentaire éventuelle (par exemple, adresse professionnelle, adresse du kot), numéro de téléphone, adresse électronique ;
- Caractéristiques personnelles : sexe, date de naissance (si nécessaire, tirée de l'eid) ;
- Numéro de registre national et/ou NISS (si la bibliothèque dispose d'une autorisation) ;
- Renseignements sur la bibliothèque : numéro de carte de bibliothèque, renseignements sur l'abonnement, les prêts en cours, les paiements et les réservations, l'historique des prêts (le cas échéant).

La notification s'effectue via le protocole SFTP (Secure File Transfer Protocol). Dans le cadre de la communication, les transactions et les coûts d'emprunts en cours sont rechargés pour une période de 5 ans. L'historique des prêts est chargé jusqu'il y a 2 ans, sauf si l'utilisateur final a indiqué qu'il ne souhaite pas conserver l'historique des prêts.

La communication de ces données de l'environnement de la bibliothèque numérique au système de bibliothèque unifié est nécessaire pour faire fonctionner le système et permettre ainsi un fonctionnement efficace de la bibliothèque et une bonne gestion des prêts (y compris les contacts et la communication avec les membres de la bibliothèque et la gestion des abonnements et des prêts) (voir aussi les objectifs mentionnés au point 5.2 ci-dessous). Les finalités du traitement ne peuvent être raisonnablement atteintes par d'autres moyens (voir également le point 5.2).

Les données fournies sont conservées pendant une période maximale de deux ans après la fin de l'abonnement à la bibliothèque. Dès la résiliation de l'abonnement et à condition qu'il n'y ait pas de transactions et de coûts ouverts, la période de conservation commence à courir, et à l'expiration, les données sont automatiquement supprimées du système. Si une bibliothèque n'est plus connectée au système de bibliothèque unifié, les données personnelles de ses membres seront supprimées conformément aux accords conclus dans la convention.

5.2 Objectifs et base juridique

Les finalités pour lesquelles les données ont été initialement collectées par les bibliothèques/communes, et pour lesquelles les données seront communiquées à Cultuurconnect lors de la connexion au système de bibliothèque unifié, sont les suivantes :

- Identification et autorisation
    - Traitement en termes d'identification et d'autorisation des utilisateurs finaux ;
- Finalités de gestion

- processus d'exploitation et de gestion : les bibliothécaires autorisés ont accès au système de la bibliothèque pour l'exploiter et le gérer, par exemple en enregistrant un client, en cherchant un client à qui prêter une copie, en dupliquant un client qui apparaît deux fois dans le système, etc ;
- processus de gestion et helpdesk ;
- développement de processus, hébergement, support et helpdesk par des employés autorisés du fournisseur IT.

- Fins fonctionnelles, entres autres :
  - Traitement en fonction du type d'abonnement ;
  - Traitement et suivi des montants impayés ;
  - Traitement de l'envoi de messages de rappel, d'avis de réservation.
- Objectifs de l'échange de données, entre autres :
  - Traite le lien entre *Ma bibliothèque* et le système de bibliothèque en fonction des services en ligne de la bibliothèque pour l'utilisateur final ;
  - traite le lien entre le système de la bibliothèque et le registre national afin de maintenir les données de l'utilisateur final correctes et à jour.
- Objectifs de journalisation
  - Traitement dû à l'enregistrement des activités des utilisateurs à des fins de dépannage et d'audit ;
  - Traitement et enregistrement des opérations des administrateurs par rapport aux données personnelles.
- Buts de la communication et du marketing direct
  - Traitement de la communication sur les activités et les services propres à la bibliothèque.
- Pour des raisons statistiques
  - Génération de rapports et statistiques basés sur l'utilisation propre à la bibliothèque.

La collecte et le traitement des données personnelles à ces fins ont lieu sur la base de l'accord entre la Bibliothèque et l'utilisateur final après la conclusion de l'adhésion à la Bibliothèque. Le traitement par Cultuurconnect des données communiquées a lieu aux mêmes fins.

Cultuurconnect traite également les données personnelles fournies aux fins suivantes :

- Objectifs de l'échange de données
  - le traitement dans le contexte des développements futurs et des liens en fonction des objectifs culturels supra-locaux et de l'innovation future de la politique culturelle locale (voir 4.6 ci-dessus);

- Buts de la communication et du marketing direct
  - Traitement de la communication et du marketing direct dans une perspective supra-locale par rapport aux services utilisés et aux applications disponibles ;
- Fins statistiques

- ○ Génération de rapports et statistiques basés sur l'utilisation dans une perspective supra-locale.

Ces fins sont compatibles avec les fins originales :

- Les utilisateurs finaux, les bibliothèques, la VGC et Cultuurconnect ont tous intérêt à ce que l'infrastructure de base de la bibliothèque numérique reste efficace, pertinente et à jour conformément aux modalités définies au point 4.6, afin de pouvoir mettre en place l'infrastructure de base (voir ci-dessus, 1) sur une base permanente. En ce sens, le traitement dans ce contexte est également dans l'intérêt justifié de Cultuurconnect en tant que fondateur de l'infrastructure de base.
- L'envoi de communications et de marketing direct aux utilisateurs finaux en rapport avec les produits et services qui sont disponibles pour les utilisateurs finaux via la bibliothèque numérique de l'infrastructure de base fait partie des attentes des utilisateurs des produits et services de la bibliothèque.

  Dans tous les cas, Cultuurconnect prend des mesures pour informer les utilisateurs finaux à ce sujet et sur leur droit de s'y opposer (notamment au moyen d'une déclaration de confidentialité), et une possibilité effective d'opt-out est prévue dans chaque communication, ce qui conduit au retrait de la liste sur la base de laquelle la communication est envoyée (article XII.13 du Code du droit économique).
- Le traitement ultérieur à des fins statistiques est un traitement compatible avec les finalités initiales (voir art. 89 AVG ; voir également la loi du 30 juillet 2018 relative à la protection des données personnelles). Dans tous les cas, Cultuurconnect prend des mesures pour informer les utilisateurs finaux de ce fait et de leur droit de s'y opposer (y compris via une déclaration de confidentialité), et ce traitement à des fins statistiques a lieu via l'utilisation de pseudonymes.

PARTIE 2 : UTILISATION DES DONNÉES

1. Utilisation et traitement autorisés des données personnelles

Les (employés autorisés de la) VGC sont autorisés, en ce qui concerne l'objet du contrat et sous réserve des dispositions du présent règlement d'utilisation, à avoir accès aux données personnelles des utilisateurs finals et à effectuer des actions sur les données personnelles des utilisateurs finals dans le cadre du présent contrat :

- l'enregistrement d'un client, la recherche d'un client à qui prêter une copie, la reproduction d'un client qui apparaît deux fois dans le système, etc ; ● Gestion des utilisateurs des profils de Ma bibliothèque.

Cultuurconnect veille à ce que des mesures techniques adéquates soient mises en place afin que :

- ***Les employés autorisés de la VGC n'ont accès qu'aux données de leurs propres utilisateurs, c'est-à-dire les utilisateurs finaux qui sont abonnés aux bibliothèques publiques néerlandophones des communes affiliées de la Région de Bruxelles-Capitale.***

- ***Les employés autorisés des bibliothèques publiques néerlandophones des communes affiliées n'ont accès qu'aux données de leurs propres utilisateurs, c'est-à-dire les utilisateurs finaux qui sont abonnés à leur propre bibliothèque ou groupe de coopération.***
- ***Lors de l'enregistrement d'un nouvel utilisateur, un doublon est suggéré si la personne est déjà dans le système. La commune/bibliothèque peut alors ajouter un abonnement à cette personne ;***
- ***Le personnel autorisé de la VGC n'a accès qu'aux profils My Library des utilisateurs des bibliothèques publiques néerlandophones des communes affiliées de la Région de Bruxelles-Capitale.***
- ***Les employés autorisés des bibliothèques publiques néerlandophones des communes affiliées n'ont accès qu'aux profils My Library des utilisateurs de leur propre bibliothèque.***

2. Obligations de la Commission communautaire flamande (VGC)

2.1 Généralités

Lors de l'exécution des tâches relevant de la participation à l'Infrastructure de base Bibliothèque numérique et pendant toute la durée de la participation, la VGC traitera les données à caractère personnel des utilisateurs finaux (utilisation, modification, conservation, etc.) conformément à la législation en vigueur en matière de protection des données.

2.2 Responsabilité des propres collaborateurs

La VGC est responsable de tout acte ou de toute omission conforme au RGPD de ses propres collaborateurs ou préposés, de la manière dont ceux-ci introduisent des données à caractère personnel dans le système de la bibliothèque, et des manipulations qu'ils effectuent sur les données à caractère personnel auxquelles ils ont accès. Cette responsabilité inclut également le respect des dispositions de la Convention et de la présente Annexe, ainsi que de la législation et de la réglementation applicables. Par conséquent, Cultuurconnect n'assume aucune responsabilité en ce qui concerne tout acte ou toute omission de collaborateurs ou préposés de la VGC.

Dans le cadre de l'utilisation autorisée, la VGC prévoit des mesures organisationnelles appropriées afin de protéger les données à caractère personnel et d'en garantir la fiabilité, la disponibilité et l'intégrité. Sans que cela n'ait un effet limitatif, la VGC garantit au moins la mise en place des mesures suivantes :

● Seuls les collaborateurs compétents de la VGC peuvent avoir accès aux données à caractère personnel. Il incombe au moins à la VGC de définir la compétence des collaborateurs, d'en suivre et d'en contrôler le respect et de se conformer au principe du besoin d'en connaître (« Need to know ») dans le chef des collaborateurs.

● Les collaborateurs compétents de la VGC reçoivent des identifiants de connexion personnels et un rôle d'utilisateur précis. Le rôle d'utilisateur d'un collaborateur détermine les données que le collaborateur peut voir. Les rôles d'utilisateur et les droits (d'accès) associés sont décrits en détail dans le manuel.

Il incombe à la VGC de demander le rôle d'utilisateur correct pour le collaborateur et de signaler le départ d'un collaborateur. Le bureau d'assistance Cultuurconnect supprime alors les identifiants de connexion du collaborateur.

● Les collaborateurs peuvent modifier eux-mêmes leur mot de passe et doivent le faire régulièrement, le système imposant un mot de passe fort. L'objectif est, à terme, de permettre de paramétrer l'expiration du mot de passe pour le système.

● L'accès au compte personnel doit être suffisamment sécurisé, entre autres par une prompte déconnexion de l'application. Il est recommandé à la VGC de prévoir un verrouillage au niveau du système d'exploitation.
● La VGC veille à ce que chaque collaborateur ou préposé compétent dispose d'informations et d'une formation à jour concernant ses obligations et ses responsabilités en matière de protection de l'information et de confidentialité des données à caractère personnel. La VGC oblige ses propres collaborateurs à s'engager à faire uniquement usage de leur accès aux données à caractère personnel dans le cadre strict de l'exercice de leur fonction (par exemple au moyen d'une déclaration sur l'honneur ou en incluant cette obligation dans le règlement ou le contrat de travail) et applique à tous ses collaborateurs une politique qui interdit la divulgation d'informations confidentielles.
● Les champs de texte libre (tels que les champs « remarques ») ne sont pas faits pour traiter des données à caractère personnel. La VGC veille à ce qu'aucune donnée à caractère personnel ne soit saisie dans de tels champs.
● L'Infrastructure de base Bibliothèque numérique n'exige aucunement de conserver des données à caractère personnel hors ligne. Toute conservation hors ligne relève donc de la seule responsabilité de la VGC.

2.3 Communication depuis le système de la bibliothèque

2.3.1 Communication fonctionnelle

Le système de la bibliothèque envoie des e-mails qui font partie des processus administratifs de la bibliothèque, par exemple lorsqu'une réservation est prête, que des articles empruntés ne sont pas rendus à temps, qu'une amende est infligée, etc. Ces messages sont envoyés par défaut par e-mail lorsque l'emprunteur a communiqué une adresse e-mail au guichet ou s'est enregistré dans « Mijn Bibliotheek ». Si aucune adresse e-mail n'a été fournie, ces messages sont envoyés par courrier postal. Les utilisateurs finaux ne peuvent pas choisir de ne pas les recevoir parce qu'ils sont fonctionnels et nécessaires aux processus de la bibliothèque.

Les rappels d'échéance forment une catégorie à part. Il s'agit d'e-mails envoyés par le système de la bibliothèque quelques jours avant l'expiration du délai de prêt. Ces « e-mails de rappel » sont plutôt un service de confort et peuvent être désactivés par l'utilisateur final. Cette option est disponible sous forme d'opt-in dans le profil du client, de sorte qu'un collaborateur compétent peut la cocher ou la désactiver à la demande d'un utilisateur final. ***La commune/bibliothèque est donc chargée de gérer les utilisateurs de la fonction « rappels d'échéance » à la demande de l'utilisateur final.*** L'objectif est, à terme, d'intégrer également cet opt-in dans « Mijn Bibliotheek » afin que l'utilisateur puisse à tout moment y gérer ses autorisations.

2.3.2 Module de marketing

Les bibliothèques peuvent aussi se servir du module de marketing du système de la bibliothèque pour envoyer des lettres d'information, des campagnes, etc., à leurs membres. Ce module de marketing sera peaufiné à terme et comprendra des options disponibles sous forme d'opt-in dans le profil du client, en examinant la possibilité pour l'utilisateur final de gérer lui-même son accord concernant la réception de ces communications par le biais de son profil « Mijn Bibliotheek ». Si la commune/bibliothèque utilise le module de marketing, elle est elle-même responsable du contenu des communications envoyées de cette manière et de la gestion des utilisateurs de cette fonction à la demande de l'utilisateur final.

2.4 Rapports et statistiques

Les collaborateurs compétents de la VGC peuvent générer et consulter des rapports et des statistiques sur l'utilisation de certaines applications par les utilisateurs finaux des bibliothèques publiques néerlandophones des communes affiliées de la Région de Bruxelles-Capitale dans le cadre de traitements statistiques pseudonymisés (par ex.,nombre

de prolongations dans la bibliothèque, sexe et âge, utilisation, utilisation des collections numériques, etc.).

Les collaborateurs compétents des bibliothèques publiques néerlandophones des communes affiliées peuvent générer et consulter des rapports et des statistiques sur l'utilisation de certaines applications par leurs propres utilisateurs finaux dans le cadre de traitements statistiques pseudonymisés (par ex., nombre de prolongations dans la bibliothèque, sexe et âge, utilisation, utilisation des collections numériques, etc.).

2.5 Fourniture d'informations aux utilisateurs finaux

Cultuurconnect a rédigé une déclaration de confidentialité de l'Infrastructure de base Bibliothèque numérique.

La VGC s'engage à instaurer, dans sa relation contractuelle avec les communes bruxelloises, une méthode de travail prévoyant que la déclaration de confidentialité de l'Infrastructure de base Bibliothèque numérique et toutes ses modifications ultérieures éventuelles convenues avec le groupe de pilotage de l'Infrastructure de base Bibliothèque numérique, soient comprises dans la fourniture d'informations aux utilisateurs finaux, et ce une première fois lors de l'affiliation à l'Infrastructure de base Bibliothèque numérique. Cette méthode de travail garantit que l'utilisateur final est informé de l'existence et du contenu de cette déclaration de confidentialité dans un délai raisonnable après le début de la participation à l'Infrastructure de base Bibliothèque numérique et après la communication de toute modification de la déclaration de confidentialité. Cela peut par exemple être prévu dans le règlement de la bibliothèque ou via la remise d'une brochure donnant des informations à jour extraites de la déclaration de confidentialité à l'utilisateur final. ***La commune/bibliothèque veille à ce qu'une copie de la (version la plus récente) de la déclaration de confidentialité de l'Infrastructure de base Bibliothèque numérique soit toujours disponible à l'accueil de toutes les bibliothèques.***

La déclaration de confidentialité de l'Infrastructure de base Bibliothèque numérique est aussi publiée par Cultuurconnect sur le site web de la bibliothèque. La VGC ou, respectivement, la commune/bibliothèque s'engage à ne pas publier sur le site web de la bibliothèque de déclarations complémentaires pouvant contenir des dispositions contraires à la déclaration de confidentialité de l'Infrastructure de base Bibliothèque numérique. Chaque fois que la déclaration de confidentialité de l'Infrastructure de base Bibliothèque numérique est modifiée, l'utilisateur final en est informé lors de sa connexion suivante à « Mijn Bibliotheek ».

2.6 Assistance en cas de fuite de données

Si la VGC constate une fuite de données, elle en informe Cultuurconnect le plus rapidement possible. On parle de fuite de données lorsque des données à caractère personnel sont divulguées, perdues, détruites ou modifiées de manière illicite.

17

Si une fuite de données est soumise à une obligation de notification légale, en fonction de la situation concrète, Cultuurconnect décidera si le signalement doit être effectué par elle, par chaque commune/bibliothèque séparément à ses utilisateurs finaux concernés, ou par la VGC. Dans ce dernier cas, la commune/bibliothèque ou, respectivement, la VGC, s'engage à procéder au signalement suivant les modalités (contenu, calendrier) communiquées par Cultuurconnect.

La communication à ce sujet entre Cultuurconnect et la VGC se déroule en principe entre les personnes de contact mentionnées dans la Partie 1, point 4.7.2.

2.7 Assistance en cas de demandes de l'autorité de contrôle

Si une demande, une communication, un avis ou une injonction de l'autorité de contrôle parvient directement à la VGC, celle-ci en informe Cultuurconnect immédiatement, et au plus tard dans les cinq jours ouvrables.

La VGC prête une assistance raisonnable à Cultuurconnect, à la demande de celle-ci, pour réagir à une demande, une communication, un avis ou une injonction de l'autorité de contrôle.
La communication à ce sujet entre Cultuurconnect et la VGC se déroule en principe entre les délégués à la protection des données mentionnés dans la Partie 1, point 4.7.1.
2.8 Assistance en cas de demandes de personnes concernées
Si une demande d'une personne concernée parvient directement à la commune/bibliothèque ou, respectivement, à la VGC, celle-ci s'efforce dans un premier temps de donner suite elle-même aux demandes de personnes concernées qui prouvent leur identité. Dans ce cas, Cultuurconnect prête toujours son assistance si celle-ci est demandée.
S'il n'est pas possible ou souhaitable que la commune/bibliothèque ou, respectivement, la VGC donne elle-même suite aux demandes de personnes concernées, la commune/bibliothèque ou, respectivement, la VGC transmet immédiatement, et au plus tard dans les cinq jours ouvrables, une copie de cette demande à Cultuurconnect.
La commune/bibliothèque ou, respectivement, la VGC, prête assistance si nécessaire à Cultuurconnect pour répondre aux demandes, même si les demandes parviennent directement à Cultuurconnect.
Si Cultuurconnect ne reçoit aucune copie d'une demande de la part de la commune/bibliothèque ou, respectivement, de la VGC, elle part du principe que la commune/bibliothèque ou, respectivement, la VGC traite la demande concernée à temps et correctement. Dans ce cas, la responsabilité à cet égard incombe à la commune/bibliothèque ou, respectivement, à la VGC.

3. Contrôle

Il relève de la responsabilité collective de l'ensemble des parties prenantes de garantir au maximum l'intégrité de l'Infrastructure de base Bibliothèque numérique. ***La VGC ou, respectivement, la commune/bibliothèque s'engage à prendre des mesures raisonnables du point de vue du respect de la vie privée aux fins du respect des accords pris dans la présente convention relative aux utilisateurs de données par ses collaborateurs, d'une part, et d'un comportement adéquat des utilisateurs finaux dans les bibliothèques, d'autre part.***
Cultuurconnect contrôle le respect de la présente Annexe de façon active et réactive. ***S'il existe des indices raisonnables indiquant que la commune/bibliothèque ou, respectivement, la VGC ne respecte pas ses obligations au titre de la présente Annexe, Cultuurconnect obtient un droit d'audit sur les activités et les installations de traitement de la commune/bibliothèque ou, respectivement, de la VGC.*** À cet effet, elle a le droit de se rendre dans les locaux ou les lieux où la commune/bibliothèque ou, respectivement, la VGC réalise le traitement des données par l'intermédiaire d'un auditeur indépendant, moyennant le respect d'un préavis de deux semaines. La commune/bibliothèque ou, respectivement, la VGC prête son concours raisonnable à cet égard et fournit les informations nécessaires afin de permettre à l'auditeur d'évaluer si la commune/bibliothèque ou, respectivement, la VGC a rempli ses obligations au titre de la présente Annexe. Les coûts d'un tel audit sont supportés par Cultuurconnect. Si un non-respect de la présente Annexe par la commune/bibliothèque ou, respectivement, la VGC est constaté, Cultuurconnect et la VGC ou, respectivement, la commune/bibliothèque se concertent à ce sujet en vue de trouver une solution dans un délai raisonnable de façon à ne pas compromettre l'utilisation de la VGC ou, respectivement, de la commune/bibliothèque au titre de la présente Annexe ni la participation à l'Infrastructure de base Bibliothèque numérique. Le manquement continu aux obligations de la présente Annexe peut entraîner le refus de l'accès à l'Infrastructure de base Bibliothèque numérique pour la VGC ou, respectivement, la commune/bibliothèque.