

CONCESSION DE SERVICE PUBLIC

CONCESSION DE SERVICE PUBLIC POUR L'AMÉNAGEMENT ET L'EXPLOITATION DES ESPACES DE LIBRAIRIE-BOUTIQUE DU MUSÉE D'ORSAY

Concession n°2026-307

Annexe 05 : Prérequis techniques et obligations légales relatives à la boutique en ligne

1. Définitions et abréviations

Pour l'application du présent contrat, et sauf stipulation contraire, les termes et expressions suivants ont le sens qui est rappelé ou leur est donné ci-après :

« **ANSSI** » désigne Agence Nationale de la Sécurité des Systèmes d'Information.

« **API** » désigne Application Programming Interface.

« **CMP** » désigne Consent Management Platform.

« **CNIL** » désigne la Commission Nationale de l'Informatique et des Libertés.

« **CTA** » désigne Call To Action.

« **MCO** » désigne le Maintien en Conditions Opérationnelles.

« **MCS** » désigne le Maintien en Conditions de Sécurité.

« **MOM** » désigne Mise en Ordre de Marche.

« **PAS** » désigne le Plan d'Assurance Sécurité.

« **PSSIE** » désigne la Politique de Sécurité des Systèmes d'Informations de l'État.

« **RGAA** » désigne le Référentiel Général d'Amélioration de l'Accessibilité.

« **RGESN** » désigne le Référentiel Général d'Ecoconception de Services Numériques.

« **RGI** » désigne le Référentiel Général d'Interopérabilité.

« **RGPD** » désigne le Règlement Général de Protection des Données.

« **Solution** » désigne la boutique en ligne en marque blanche développée et gérée par le CONCESSIONNAIRE pour le compte du musée d'Orsay.

2. Interopérabilité avec les sites de l'EPMO-VGE

Le CONCESSIONNAIRE choisit librement la solution technique à implémenter, en accord avec la stratégie RSO de l'Etablissement, et conformément aux dispositions présentées à l'article 8.3 du Contrat.

2.1. Interopérabilité avec le site internet du musée d'Orsay

Aujourd'hui, les données produits de <https://www.boutiquesdemusees.fr/fr/content/5075-musee-orsay.html?par=3> sont récupérées via API (Application Programming Interface) par l'EPMO-VGE afin de créer des contenus de type produit associés à des expositions ou événements. Le format de l'export s'appuie sur la norme Google Shop. Le CONCESSIONNAIRE s'engage à permettre un export des données produits respectant la même norme.

A termes, l'EPMO-VGE étudie la possibilité de mettre en place des ventes croisées entre la billetterie et la boutique en ligne. Il n'est pas attendu une interopérabilité entre la billetterie et la boutique en ligne lors du lancement du site, mais l'EPMO-VGE se réserve la possibilité de demander la mise en place de cette évolution au cours de la Concession.

2.2. Interopérabilité avec le site internet du musée d'Orsay et sa boutique en ligne

A termes, l'EPMO-VGE étudie la possibilité de mettre en place des synergies commerciales et de communication entre la solution technique implémentée par le CONCESSIONNAIRE, et le site du musée d'Orsay, ainsi que sa boutique en ligne. Il n'est pas attendu une interopérabilité lors du lancement du site, mais l'EPMO-VGE se réserve la possibilité de demander la mise en place de cette évolution, en accord avec les gestionnaires du musée d'Orsay et de sa boutique en ligne.

3. Hébergement

L'EPMO-VGE attend du CONCESSIONNAIRE une solution d'hébergement du site internet qui soit pertinente, de préférence française et Européenne.

Pour rappel, selon les recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), les données (sauvegardes et archives comprises) doivent être hébergées sur le territoire de l'Union Européenne et, si possible, sur le territoire national français.

Disponibilité

Les sites doivent être disponibles 7 jours sur 7 et 24 heures sur 24 avec un taux de disponibilité supérieur ou égal à 99,9 % par mois, avec un maximum de quatre heures consécutives d'interruption.

Le CONCESSIONNAIRE est encouragé à proposer une solution de disponibilité favorisant l'économie d'énergie (disponibilité réduite sur les heures creuses de trafic et de billetterie, utilisation de serveurs optimisant la consommation d'énergie...).

Performances

La plateforme de production est dimensionnée pour supporter la charge de navigation des internautes.

Pérennité

Le système doit être pérenne, défini comme étant un système qui s'appuie sur des technologies qui garantissent son fonctionnement pendant au moins 10 ans.

4. Attentes en termes de suivi et détail des fonctionnalités de tracking

Le CONCESSIONNAIRE doit proposer un plan de marquage adapté aux besoins du service Marketing de l'EPMO-VGE.

A ce titre, afin de mesurer l'efficacité des campagnes marketing, d'optimiser les performances et d'améliorer la compréhension du parcours client, le CONCESSIONNAIRE définit clairement la méthode de tracking des liens URL utilisée, notamment lorsque que l'EPMO-VGE met en avant des produits dont le CTA (Call To Action) bascule l'utilisateur vers le site e-commerce du CONCESSIONNAIRE.

Le CONCESSIONNAIRE doit assurer la mise en conformité CNIL (Commission Nationale de l'Informatique et des Libertés) du site en intégrant une Plateforme de Gestion du Consentement (CMP). Il est précisé que la solution Piano est utilisée afin de tracker tous les sites internet de l'écosystème EPMO-VGE. Cette solution est susceptible de changer en cours de Concession en fonction d'évolutions réglementaires ou techniques qui seront précisées au CONCESSIONNAIRE, le cas échéant. Par ailleurs, des scripts sont intégrés aux sites afin d'assurer la publicité personnalisée sur les réseaux sociaux suivants : Meta, Instagram, Google Ads, Pinterest, TikTok, Facebook, Facebook ADS et LinkedIn. Cette liste peut être amenée à évoluer. La gestion du consentement est assurée via le CMP et Google Tag manager.

Le CONCESSIONNAIRE doit prévoir la réversibilité des informations clients et l'hébergement des données conformément au RGPD (Règlement Général de Protection des Données), tel que précisé à l'article 5 de la présente annexe. Cette fonctionnalité peut être assurée par la CMP.

5. Conformité avec le RGPD

Le CONCESSIONNAIRE s'engage à respecter intégralement, et tout au long du Contrat, les dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ainsi que les obligations en vigueur qui découlent et relèvent du Règlement Général sur la Protection des Données (RGPD) tout au long de la durée de la Concession.

La Solution est un élément central de la connaissance et la fidélisation client de l'EPMO-VGE, reposant largement sur l'Internet et la communication électronique, le traitement de données personnelles, l'utilisation de trackers et l'agrégation, le croisement et la synchronisation de données distinctes de la Solution. A ce titre, la conformité de la Solution à la réglementation applicable sur la protection des données personnelles et de la vie privée revêt d'un fort enjeu.

La Solution comporte des mécanismes, recourant au maximum à l'automatisation et à l'auto-administration par les personnes concernées, de mise en œuvre des opérations requises par la réglementation susmentionnée :

- Conservation des preuves de consentement ;
- Gestion des demandes d'exercice des droits des personnes concernées ;
- Anonymisation ;
- Pseudonymisation ;
- Purge ou archivage automatique des données personnelles.

Le CONCESSIONNAIRE apporte son concours et son expertise dans ces domaines spécifiques, en conseillant et si besoin en alertant l'EPMO-VGE sur la conformité des opérations dépendant de ce dernier ou d'autres parties en lien avec la Solution.

Des audits et revues conjointes sont régulièrement menées sur ces dispositions afin de garantir le maintien de la conformité dans le temps. Dès lors qu'elles revêtent une fréquence et un caractère raisonnable et proportionné aux enjeux, ces actions de contrôle interne de la conformité ne font pas l'objet d'une facturation spécifique du CONCESSIONNAIRE.

6. Impératifs réglementaires

Le CONCESSIONNAIRE répond aux impératifs réglementaires suivants en vigueur :

- RGI (Référentiel Général d'Interopérabilité) : <https://www.numerique.gouv.fr/publications/interoperabilite/>
- RGAA (Référentiel Général d'Amélioration de l'Accessibilité) – version 5 : <https://accessibilite.numerique.gouv.fr/>
- RGSN (Référentiel Général d'Ecoconception de Services Numériques) :
<https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/>

Exigences de sécurité de l'hébergement

Il est attendu que le CONCESSIONNAIRE garantisse :

- La sécurité physique des sites d'hébergement (site principal, site de secours) ;
- L'autonomie des sites d'hébergement.

L'EPMO-VGE est soumis à la circulaire n°5725/SG du 17 Juillet 2014, relative à la PSSIE (Politique de Sécurité des Systèmes d'Informations de l'État) : tout contrat d'hébergement doit détailler les mesures prévues pour assurer le maintien en condition de sécurité des systèmes et permettre une gestion de crise efficace (conditions d'accès aux journaux, mise en place d'astreintes etc.). Toute évolution relative aux exigences de sécurité de l'hébergement sera partagée au CONCESSIONNAIRE le cas échéant et devra être respectée par ce dernier.

Sécurité du système

L'ensemble du système est sécurisé (données comprises). Les exigences en termes de sécurité des sites internet se rapportent à :

- L'authentification des utilisateurs ;
- La gestion des habilitations ;
- L'anonymisation des données ;
- La sauvegarde des données ;
- L'archivage des données ;
- La gestion de la confidentialité ;
- La gestion des incidents ;
- Le paramétrage ;
- Les audits et la gestion des traces ;
- La détection des tentatives d'intrusion et d'aspiration des données ;
- La protection contre les codes malveillants (antivirus).

Le CONCESSIONNAIRE est tenu de respecter la loi n° 2018-133 du 26 février 2018 portant des dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, plus particulièrement les articles 10 à 15 décrivant les dispositions relatives à la sécurité des réseaux et systèmes d'information des fournisseurs de service numérique.

L'identification et la classification des risques de sécurité numérique permettent de déterminer et de prioriser les axes d'amélioration pour mieux protéger le patrimoine informationnel et matériel et de garantir la continuité d'activité.

Le CONCESSIONNAIRE doit disposer d'une cartographie des risques couvrant l'ensemble du périmètre des services, en utilisant une méthode documentée et garantissant la reproductibilité et comparabilité de la démarche.

Le CONCESSIONNAIRE fournit, à la demande, dans un document spécifique, les risques résiduels liés à l'existence de lois extra-européennes ayant pour objectif la collecte de données ou métadonnées de l'EPMO-VGE sans un consentement préalable.

Le CONCESSIONNAIRE met à la disposition de l'EPMO-VGE, sur demande, les éléments d'appréciation des risques liés à la soumission des données de l'EPMO-VGE au droit d'un État non-membre de l'Union Européenne.

Le CONCESSIONNAIRE détaille les moyens mis en œuvre pour couvrir les risques de perte et ou de corruption de données afin notamment de respecter les engagements de maintien de services exigés par l'EPMO-VGE : certification Iso et RGPD notamment, outils pour pallier la perte accidentelle de données, chiffrement pour le site distant, sauvegardes, durée de conservation des sauvegardes, systèmes de logs, etc.

La direction du CONCESSIONNAIRE doit accepter formellement les risques résiduels identifiés dans l'appréciation des risques et l'homologation doit être documentée.

Le CONCESSIONNAIRE doit réviser annuellement l'appréciation des risques et à chaque changement majeur pouvant avoir un impact sur le service.

Le CONCESSIONNAIRE peut être force de proposition et proposer une architecture technique permettant d'optimiser la sécurité du système.

Plan d'Assurance Sécurité (PAS)

Le CONCESSIONNAIRE doit être en mesure de présenter un plan d'assurance sécurité (PAS) au plus tard **cinq (5)** jours après la MOM (Mise en Ordre de Marche). Ce dernier devra tenir compte des exigences suivantes de l'EPMO-VGE :

- Détection des tentatives d'intrusion et des incidents de sécurité ;
- Communication dans les plus brefs délais de toute faille de sécurité entraînant des conséquences directes ou indirectes ;
- Communication à l'EPMO-VGE de toute plainte adressée par un individu concerné par le traitement de ses données.

Le PAS devra notamment être conforme aux orientations précisées dans le mémoire remis par le CONCESSIONNAIRE dans son offre et rendu contractuel.

Respect des règles de l'ANSSI

Dans ce cadre, le CONCESSIONNAIRE se conforme à la réglementation en vigueur et aux bonnes pratiques énoncées par l'ANSSI. Les modalités de gestion des fraudes et de lutte contre la cybercriminalité sont documentées.

Maintien en conditions opérationnelles (MCO) et de sécurité (MCS)

Le CONCESSIONNAIRE de la Solution fournit un plan d'assurance qualité et son plan de sécurité contenant les meilleures pratiques et mesures mises en œuvre afin de garantir le maintien en condition opérationnelle et le maintien en conditions de sécurité ainsi que les performances de l'ensemble des systèmes, matériels, logiciels, données, interfaces, personnels et processus sous sa responsabilité contractuelle constituant l'écosystème de la boutique en ligne.

7. Gestion de la fin de contrat

Le CONCESSIONNAIRE est tenu de prévoir la réversibilité de la boutique en ligne : dix-huit (18) mois avant l'échéance du contrat de Concession, l'EPMO-VGE et le CONCESSIONNAIRE doivent prévoir d'échanger sur les modalités de fin de gestion pour en faciliter la passation.

La réversibilité a pour objectif de permettre à l'EPMO-VGE de récupérer l'ensemble des données et informations contenues dans la Solution, et ce, dans les meilleures conditions. La réversibilité intervient lorsque la relation contractuelle cesse, quelle qu'en soit la cause.

Le CONCESSIONNAIRE est tenu de prévoir un plan de réversibilité comprenant :

- Une assistance en biseau auprès de l'EPMO-VGE, en présence ou non du CONCESSIONNAIRE (selon qu'il y a notification d'un nouveau marché ou non), sur une période de trois (3) mois afin de permettre la reprise des données que le CONCESSIONNAIRE s'engage à communiquer sans réserve et dans des formats et supports facilement exploitables (.csv, .xls ou autre format convenu entre les parties) ;
- Le détail des modalités (durée, activités, livrables) de la réversibilité des prestations et des données et du transfert de compétences requis ;
- Un engagement à ne pas conserver de copies des données de l'EPMO-VGE après validation du plan de réversibilité et à ne pas les utiliser à quelque fin que ce soit.

Le CONCESSIONNAIRE remettra une attestation sur l'honneur confirmant que les copies des données de l'EPMO-VGE ont bien été détruites. En cas d'absence de destruction ou de fausse déclaration sa responsabilité pourra être engagée. Cette attestation sera remise au plus tard au terme de la réversibilité.