La Maison des Artistes
SÉCURITÉ SOCIALE
60 rue du Faubourg Poissonnière - 75484 PARIS CEDEX 10
www.mda-securitesociale.org

# DOSSIER DE CONSULTATION DES ENTREPRISES

## MAPA n° 2 - 2016 : Infogérance des sauvegardes AGESSA/MDA

### 1-OBJET DE LA CONSULTATION :

L'objet du présent marché est la mise en place et l'infogérance d'une solution de sauvegarde en local et de la réplication de ces sauvegardes sur un site distant pour l'Agessa et la Maison des Artistes.
Les systèmes informatiques de l'Agessa et de la Maison des Artistes sont distincts et séparés physiquement. La prestation objet du marché devra être mise en œuvre dans les deux organismes.

### 2-PRESTATION POUR CHAQUE ORGANISME :

- Sauvegarde locale avec réplication sur site distant en France
- Infogérance de la sauvegarde :
    - Supervision du logiciel et matériel 24h/24 et 7j/7
    - Maintenance corrective de la solution de sauvegarde locale et distante : J+1
    - Assistance téléphonique en français ou via le portail : 8h-19h 5j/7
    - Création, modification et suppression d'agents et de jobs

- Mise à disposition d'un extranet ouvert au client :
    - Accès par compte nominatif (pas de compte banalisé) avec attribution de rôles différents selon les profils
    - Possibilité de lancer une restauration

- Mise à disposition d'un outil de suivi des incidents et demandes :
    - Incidents
    - Demandes :
        - Job : création, modification et suppression
        - Agent : création, modification et suppression
        - Restauration des sauvegardes sur un support externe pour le test du Plan de Secours Informatique dans un délai de 24h 1 fois / an (à inclure dans la redevance annuelle)
        - Demande exceptionnelle de restauration des données sur un support externe

        - Demande exceptionnelle de restauration

- Serveur de sauvegarde local est maitre d'opérations (sauvegarde primaire en local et sauvegarde secondaire sur le site distant)

- Granularité des restaurations :
    - Système : VM, disque virtuel, répertoire et fichier
    - Sql Serveur : instance, base de données, table
    - AS 400 : paramétrage système, data, IFS

- Test de restauration 1 fois / an

- Reporting :
    - Rapport et tableaux de bord quotidien et hebdomadaire
    - Informations souhaitées :
        - état des sauvegardes / job
        - volume des sauvegardes /job + / VM
        - journal des restore (qui, quand et quoi)

- Devoir de conseil : le candidat retenu s'engage à :
    - informer l'Agessa et la Maison des Artistes sur l'état de l'art dans le domaine objet du présent marché,
    - préconiser des évolutions qu'il conviendrait de mettre en œuvre.

**3-EXISTANT :**

Les systèmes informatiques de l'Agessa et de la Maison des Artistes sont distincts et physiquement séparés.

**Engagement de volume global Agessa – la Maison des Artistes = 7 To**

- Agessa :
    - Volume réel d'une sauvegarde complète non compressée : 3.2 To
    - 43 VM dont 4 serveurs de base de données
    - Taux de modification : 2 %
    - Fibre optique 20 Mo
    - Fenêtre de sauvegarde : 00h00 et 07h00 à ajuster en fonction des jobs
    - Fenêtre de réplication : de 00h00 à 8h30

- La Maison des Artistes :
    - Volume réel d'une sauvegarde complète non compressée : 3.7 To
    - 30 VM dont 1 serveur de base de données
    - AS400
    - Taux de modification : 2 %
    - Fibre optique 20 Mo

- Fenêtre de sauvegarde : 00h00 et 07h00 à ajuster en fonction des jobs
- Fenêtre de réplication : de 00h00 à 8h30

## 4-ENGAGEMENTS :

- Intégrité des sauvegardes et donc leur restauration
- SLA : en fonction de la sévérité de l'incident :
  - temps de prise en charge
  - temps de résolution

- Pénalités si non-respect :
  - du SLA
  - des engagements de restauration

## 5-PERIMETRE DE LA SAUVEGARDE :

- VMware 5.5
- Microsoft 2008 R2 et 2012 R2
- Microsoft SQL Serveur 2008, 2012 et 2014
- AS-400 V7 R1

## 6-PLAN DE LA SAUVEGARDE :

| Type sauvegarde | Fréquence | Rétention |
|---|---|---|
| Quotidienne | du lundi soir au vendredi soir | 7 jours |
| Hebdomadaire | le vendredi soir | 1 mois |
| Mensuelle | 1er samedi du mois | 12 mois |
| Annuelle | 1er dimanche de l'année | 2 ans |

## 7-REGLEMENTATION APPLICABLE :

Marché public à procédure adaptée, conformément à l'article 28 du Code des marchés publics.

## 8 - CRITERES D'ATTRIBUTION :

- Prix : 35 %
- Prestation : 30 %
- Engagements de service : 35 %

L'AGESSA et la MDA se réserve le droit de négocier avec, au maximum, les cinq candidats ayant présenté les meilleures offres au regard des critères d'attribution. Une visite sur site est à prévoir.

Documents à fournir lors de la signature de l'acte d'engagement :

- PCA du candidat pour la prestation demandée

## 9 – PLANNING ET RETROPLANNING :

L'Agessa et la Maison des Artistes implémentent déjà une solution de sauvegarde qui arrive à échéance le 31 octobre 2016. La solution retenue doit donc impérativement être mise en place avant le 31 octobre 2016.

- Fin du marché : 7 avril 2016
- Fin de mise en œuvre : **Impérativement** avant le 15 octobre 2016

## 10 - INFORMATIONS COMPLEMENTAIRES :

Les questions techniques ou administratives peuvent être posées à l'adresse suivante : marches-agessa@secu-artistes-auteurs.fr **avant le 24/03/2016.**
L'ensemble des questions et réponses sera disponible en ligne au plus tard le **01/04/2016**.

## 11- PRESENTATION DE VOTRE PROPOSITION ET DES PLIS :

11.1 Présentation de la société

11.2 Références de la société dans le domaine objet du marché

11.3 Présentation détaillé de la solution :

- outils et technologies utilisés
- extranet :
  - fonctionnalités mises à disposition du client
  - droits d'accès et rôles
  - copies d'écran
  - fonctions qui ne seraient pas disponibles depuis l'extranet ou pour certaines technologies (ex : AS400)
- outil de suivi des demandes et incidents :
  - fonctionnalités mises à disposition du client
  - droits d'accès et rôles
  - copies d'écran
- modalités du test de restauration

- Présentation des mesures prises pour la sécurité des données :
  - lors du transport vers le site distant (cryptage, VPN…)
  - sur le site distant (sécurité physique des locaux, sécurité de l'infrastructure, confidentialité, adhérence avec d'autres clients)

- SLA :
    - SLA à préciser en fonction de la sévérité de l'incident :
        - temps de prise en charge
        - temps de résolution
    - Pénalités à préciser si non-respect :
        - du SLA
        - des engagements de restauration
- Modalités de reprise des données à préciser
- Pré-requis Agessa et la Maison des Artistes : matériel, débit internet...
- Méthodologie projet + Planning
- Proposition financière :
    - coût de mise en œuvre
    - redevance annuelle
    - clauses d'évolution
    - coût des travaux par type
- Documents à remplir par le candidat :
    - clause de confidentialité (annexe 1)
    - déclaration CNIL (annexe 2)

### 11.4 Documents administratifs à joindre à votre proposition

Les offres seront entièrement rédigées en langue française et chiffrées en euro.

Le dossier à remettre par chaque candidat comprendra les pièces suivantes :

- La déclaration du candidat (Modèle DC5) incluant notamment :
- Les attestations et certificats délivrés par les administrations et organismes compétents prouvant que le candidat a satisfait à ses obligations fiscales et sociales ou documents équivalents en cas de candidat étranger.
- Une attestation sur l'honneur que le travail sera réalisé avec des salariés employés régulièrement et que le candidat se conforme aux dispositions du Code du Travail relatives au respect de l'obligation d'emploi.
- Une déclaration sur l'honneur selon laquelle le candidat n'a pas fait l'objet d'une interdiction de concourir.
- Les moyens et chiffres d'affaires du candidat au cours des trois dernières années (sauf pour les entreprises nouvellement créées).

- Si le candidat est en redressement judiciaire, la copie du ou des jugement(s) prononcé(s) à cet effet.

## 12 - FACTURATION

Le mode de règlement utilisé est le virement.

Chaque entité devra faire l'objet d'une facturation séparée à hauteur de 50 % du montant total à facturer.

## 13-MISE EN ŒUVRE, DUREE ET RESILIATION DU MARCHE :

Le marché sera conclu pour une durée initiale de trois ans. Il pourra ensuite être reconduit par tacite reconduction d'une durée d'un an avec une durée maximale de quatre ans.

Au-delà de la période initiale d'engagement ferme ce marché pourra être résilié moyennant le respect d'un préavis de 3 mois par lettre recommandée avec accusé de réception.

A la fin du contrat, le candidat retenu s'engage à supprimer toutes les données de l'Agessa et de la Maison des Artistes.

Réversibilité : Il est convenu que le candidat facilitera l'obtention sur un support externe de l'ensemble des données sauvegardées et l'outil nécessaire à l'exploitation de ces sauvegardes.

## 14 - CONDITIONS DE REMISE DES OFFRES & CONTACT

Les plis cachetés contenant les offres seront transmis **au plus tard le 07/04/2016 – 12h00** sous enveloppe cachetée à l'adresse suivante :

**AGESSA**
**21 bis rue de Bruxelles**
**75439 PARIS Cedex 09**

Avec les indications suivantes :

**MAPA n° 2-2016**
**Ne pas ouvrir par le Service Courrier**

Par lettre recommandée avec accusé de réception ou déposée sur place de 9h30 à 12h30 et de 14h30 à 16h30.

**Contact** : FOURNIER-GUILLOT M.P.
Service Affaires Générales
21 bis rue de Bruxelles
75439 PARIS Cedex 09
marches-agessa@secu-artistes-auteurs.fr

## 15 - DATE LIMITE DE RECEPTION DES OFFRES : 07/04/2016 – 12h00

## ANNEXE : 1 - Clause de confidentialité *(à compléter)*

Cette clause s'appliquera, à compter de sa signature, à toutes les relations contractuelles entre les parties.

La société ..... ci-après dénommée « le prestataire» est tenue, ainsi que l'ensemble de son personnel, au secret professionnel, à l'obligation de discrétion et à l'obligation de confidentialité pendant les prestations commandées par l'AGESSA et La Maison des Artistes et après leur exécution.

Les données qui sont échangées, qu'elles présentent ou non un caractère personnel, sont des données confidentielles et couvertes par le secret professionnel tel que défini aux articles 226-13 et suivants du code pénal. Conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, le prestataire s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

Le prestataire s'engage donc :

- à respecter le secret professionnel auquel il est soumis,
- à faire respecter par ses propres utilisateurs ou salariés les règles de secret professionnel de discrétion et de confidentialité sus-énoncées,
- à ce que les informations, telles que définies ci-dessous, qui sont communiquées ne soient en aucun cas, divulguées ou retransmises à des personnes physiques ou morales non autorisées,
- à n'utiliser les informations confidentielles, telles que définies ci-dessous, qu'aux seules fin de l'exécution des prestations commandées par l'AGESSA et la Maison des artistes.

En outre, le prestataire organise ci-après la protection des informations confidentielles qu'il est amené à traiter.

Le terme «Information confidentielle» est défini comme toute information de quelque nature que ce soit et quelle que soit sa forme, écrite ou orale, y compris sans que cela ne soit limitatif, tout écrit, note, copie, rapport, document, étude, analyse, dessin, lettre, listing, logiciel spécifications, chiffre, graphique, enregistrement sonore et/ou reproduction picturale, quel que soit son support
Il paraît difficile d'identifier les informations communiquées et considérées comme confidentielles par l'apposition d'une mention spéciale.

Par conséquent, le prestataire convient que toutes les informations communiquées par les parties sont considérées comme confidentielles.

En outre, le prestataire souscrit, en plus des engagements contenus dans le présent article, les engagements suivants :

- il ne doit pas utiliser les documents et supports d'information confiés par l'une des parties à des fins autres que celles spécifiées dans le cadre des prestations commandées par l' AGESSA et La Maison des artistes,

- il ne doit conserver aucune copie des documents et supports d'information confiés par l'une des parties après exécution des prestations,
- il ne doit pas communiquer ces documents et informations à d'autres personnes que celles qui ont qualité pour les connaître,
- il doit prendre toutes mesures permettant d'éviter toutes utilisation détournée ou frauduleuse des fichiers.

Le prestataire s'interdit tout recours à la sous-traitance sauf accord exprès et écrit de l'AGESSA et de la Maison des artistes.

Dans le cas où le prestataire sous-traiterait l'exécution des prestations à un tiers après accord de l'AGESSA et de la Maison des artistes, ce dernier devra être soumis aux mêmes obligations, et la responsabilité en incombera au prestataire, auquel il pourra être demandé à tout moment de justifier de la signature de la clause de confidentialité par ses sous-traitants.

l'AGESSA et de la Maison des artistes se réservent le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par le prestataire.

Il est rappelé que, en cas de non-respect des dispositions précitées, la responsabilité du titulaire peut également être engagée sur la base des dispositions des articles 226-17 et 226-5 du code pénal.

L'AGESSA et la Maison des artistes pourront prononcer la résiliation immédiate du contrat, sans indemnité en faveur du prestataire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

Fait en 2 exemplaires à Paris, le

Bon pour acceptation

Cachet et signature précédée de la mention « lu et approuvé »

## ANNEXE 2 - A REMPLIR ET A JOINDRE A VOTRE PROPOSITION

| | |
|---|---|
| **Société** | |
| **Prestation** | |
| **Nom, Prénom, Qualité** | |
| **Date** | |

| REF. | THEME | POINT A VERIFIER | REPONSE Oui/Non/Sans objet | COMMENTAIRE |
|---|---|---|---|---|
| Fiche 1 | Risques | Recenser les fichiers et données à caractère personnel et les traitements | | |
| | | Déterminer les menaces et leurs impacts sur la vie privée des personnes | | |
| | | Mettre en œuvre des mesures de sécurité adaptées aux menaces | | |
| Fiche 2 | Authentification des utilisateurs | Définir un identifiant (login) unique à chaque utilisateur | | |
| | | Adopter une politique de mot de passe utilisateur rigoureuse (mots de passe de 8 caractères minimum avec des caractères de types différents) | | |
| | | Changer de mot de passe régulièrement | | |
| | | Obligez l'utilisateur à changer son mot de passe après réinitialisation | | |
| | | Stockage des mots de passe dans un fichier crypté | | |
| | | Choix des mots de passe sans lien avec soi | | |
| | | Ne pas communiquer son mot de passe | | |
| Fiche 3 | Habilitations | Définir des profils d'habilitation | | |
| | | Supprimer les permissions d'accès obsolètes | | |
| | | Documenter les procédures d'exploitation, les tenir à jour et les rendre disponibles aux utilisateurs concernés | | |
| | | Rédiger une charte informatique (annexée au règlement intérieur) | | |
| | | Définir des comptes nominatifs (pas de comptes partagés par plusieurs personnes) | | |
| | | Etablir, documenter et réexaminer une politique de contrôle d'accès en rapport avec la finalité du traitement | | |
| | | Classifier les informations de manière à indiquer si celles-ci sont des données sensibles | | |
| | | Envoyer régulièrement à tous les utilisateurs les mises à jour des politiques et procédures pertinentes pour leur fonction | | |
| | | Sensibiliser et informer à la sécurité de l'information | | |
| | | Prévoir la signature d'un engagement de confidentialité | | |
| Fiche 4 | Sécurité des postes de travail | Limiter le nombre de tentatives d'accès à un compte | | |
| | | Installer un «pare-feu» (firewall) logiciel | | |
| | | Utiliser des antivirus régulièrement mis à jour | | |
| | | Prévoir une procédure de verrouillage automatique de session | | |
| | | Ne pas utiliser des comptes d'exploitation obsolètes | | |
| | | Installer les mises à jour critiques des systèmes d'exploitation sans délai | | |
| | | Limiter les applications nécessitant des droits de niveau administrateur pour leur exécution | | |
| | | Limiter les services du système d'exploitation s'exécutant sur le poste de travail à ceux strictement nécessaires | | |
| | | Mettre à jour les applications lorsque des failles critiques ont été identifiées et corrigées | | |

| | | | | |
|---|---|---|---|---|
| Fiche 5 | Sécurisation de l'informatique mobile | Prévoyez des moyens de chiffrement pour les ordinateurs portables et<br>Prévoir des moyens de chiffrement pour les ordinateurs portables et les unités de stockage amovibles (clés USB, CD, DVD…) | | |
| | | Ne pas conserver des données personnelles dans les équipements mobiles lors de déplacement à l'étranger | | |
| | | Verrouillage automatique des appareils mobiles après quelques minutes d'inactivité | | |
| Fiche 6 | Sauvegardes et continuité de d'activité | Effectuer des sauvegardes régulières | | |
| | | Stocker les supports de sauvegarde sur un site extérieur | | |
| | | Sécuriser le lieu de stockage des sauvegardes par au moins une des solutions suivantes : chiffrement des sauvegardes, chiffrement des données, stockage dans un lieu sécurisé | | |
| | | Mettre en place des détecteurs de fumée | | |
| | | Les matériels informatiques ne doivent pas être mis au sol mais surélevés | | |
| | | Utilisation d'onduleur pour les matériels critiques | | |
| | | Prévoir une redondance de matérielle des unités de stockage | | |
| | | Prévoir et tester régulièrement la continuité d'activité | | |
| Fiche 7 | Maintenance | Garantir que les données ne seront pas compromises lors d'une intervention de maintenance par une au moins des solutions suivantes : enregistrement des interventions dans une main courante, encadrement des interventions par des tiers, ne pas autoriser la télémaintenance sans autorisation | | |
| | | Effacer les données de tout matériel avant sa mise au rebut | | |
| | | Recueillir l'accord de l'utilisateur avant toute intervention sur son poste | | |
| | | Ne pas installer des applications pour la maintenance vulnérables (http://www.cert.ssi.gouv.fr/site/CERTA-2009-AVI-035/) | | |
| | | Restreindre, voire interdire l'accès physique et logique, aux ports de diagnostic et de configuration à distance | | |
| Fiche 8 | Tracabilité et gestion des incidents | Prévoir un système de journalisation des activités des utilisateurs, des anomalies et des évènements liés à la sécurité avec au minimum l'identifiant, la date et l'heure de connexion et de déconnexion dans le cadre prévu par la CNIL | | |
| | | Ne pas utiliser les informations issues des dispositifs de journalisation à d'autres fins que celles de garantir le bon usage du système informatique | | |
| | | Synchronisation des horloges à l'aide d'une source de temps fiable et préalablement définie | | |
| | | Le responsable de traitement doit se tenir informé des vulnérabilités techniques des systèmes et entreprendre les actions appropriées | | |
| Fiche 9 | Sécurité des locaux | Restreindre les accès aux locaux au moyen de portes verrouillées | | |
| | | Installer des alarmes anti-intrusion et vérifiez-les périodiquement | | |
| | | Vérifier et entretenir le matériel de climatisation | | |
| | | Mettre en place des dispositifs d'authentification pour accéder aux zones dans lesquelles des informations sensibles sont traitées ou stockées | | |
| | | A l'intérieur des zones d'accès réglementé, exiger le port d'un moyen d'identification visible | | |
| | | Les visiteurs doivent avoir un accès limité (la date et heure de leur arrivée doivent être consignées) | | |
| | | Réexaminer et mettre à jour régulièrement les permissions d'accès aux zones sécurisées et les supprimer si nécessaire | | |
| Fiche 10 | Sécurité du réseau informatique | Limiter les flux réseau au strict nécessaire | | |
| | | Sécuriser les accès distants des appareils informatiques nomades par VPN | | |
| | | Utiliser le protocole SSL avec une clé de 128 bits pour les services web | | |
| | | Ne pas utiliser le protocole telnet pour la connexion à distance aux équipements actifs du réseau (préférer SSH) | | |
| | | Mettre en œuvre le protocole WPA - AES/CCMP pour les réseaux WiFi | | |
| | | Cloisonner le réseau (segmenter le réseau en sous-réseaux logiques) | | |
| | | Mettre en place des systèmes de détection d'intrusion (IDS) | | |

| | | | | |
|---|---|---|---|---|
| | | Mettre en place l'identification automatique de matériels comme moyen d'authentification des connexions à partir de lieux et matériels spécifiques | | |
| Fiche 11 | Sécurité des serveurs et des applications | Adoptez une politique de mot de passe administrateur rigoureuse (mots de passe de 10 caractères minimum avec des caractères de types différents pour les mots de passe d'administration) | | |
| | | Changer de mot de passe au départ d'un administrateur | | |
| | | Installer les mises à jour critiques des systèmes d'exploitation sans délai | | |
| | | Ne pas utiliser les serveurs à d'autres fins que celles prévues (naviguer sur internet, accéder à la messagerie…) | | |
| | | Utiliser des comptes nominatifs pour l'accès aux bases de données | | |
| | | Mettre en œuvre des mesures et/ou installer des dispositifs pour se prémunir des attaques par injection de code SQL, scripts | | |
| | | Prévoir des mesures particulières pour les bases de données sensibles | | |
| | | Assurer une continuité de disponibilité des données | | |
| | | Mettre à jour les applications lorsque des failles critiques ont été identifiées et corrigées | | |
| | | Ne pas utiliser des services non sécurisés (authentification en clair, flux en clair….) | | |
| | | Ne pas placer des bases de données dans une zone directement accessible depuis internet | | |
| | | Les systèmes sensibles doivent disposer d'un environnement informatique dédié (isolé) | | |
| | | Utilisation d'outils de détection des vulnérabilités (http://nmap.org/, http://www.tenable.com/products/nessus-vulnerability-scanner, https://cirt.net/nikto2) | | |
| | | Assurer l'intégrité des traitements par le recours à des signatures garantissant qu'il n'a subi aucune altération | | |
| Fiche 12 | Sous-traitance | Prévoir dans les contrats une clause de confidentialité | | |
| | | Prendre des dispositions (audits de sécurité, visite des installations…) afin de s'assurer de l'effectivité des garanties offertes par le sous-traitant en matière de protection des données | | |
| | | Prévoir les conditions de restitution des données et leur destruction en cas de rupture ou à la fin du contrat | | |
| | | Ne pas avoir recours à des services offrant des fonctionnalités d'informatique répartie (cloud) sans garantie quant à la localisation géographique effective des données | | |
| Fiche 13 | Archivage | Mettre en œuvre des modalités d'accès spécifiques aux données archivées | | |
| | | Détruire les archives obsolètes de manière sécurisée | | |
| | | Ne pas utiliser des supports présentant une garantie de longévité suffisante (CD, DVD…) | | |
| Fiche 14 | Echange d'informations avec d'autres organismes | Chiffrer les données avant leur envoi | | |
| | | S'assurer qu'il s'agit du bon destinataire | | |
| | | Transmettre le secret lors d'un envoi distinct et via un canal différent | | |
| | | Ne pas transmettre des données personnelles en clair via des messageries web du type Gmail ou Hotmail | | |
| | | Utiliser des calculs d'empreintes pour s'assurer de l'intégrité des données | | |
| | | Utiliser des signatures électroniques pour garantir l'origine de la transmission | | |