

## **ACTE D'ENGAGEMENT DE MISE A DISPOSITION DES FICHIERS de données relatives à l'implantation des infrastructures et réseaux de communications électroniques**

Les fichiers informatiques de données numériques désignés ci-après sont récupérés par la Région Provence-Alpes-Côte d'Azur auprès des différents opérateurs d'infrastructure de réseaux de télécommunication présents sur le territoire régional et diffusés auprès de ses partenaires ayants droit.

### **Ces fichiers sont mis à disposition de :**

l'organisme : .....

.....

dont le siège se situe :

.....

représenté par :

.....

.....

et ayant le numéro de SIRET suivant :

.....

Ci-après désigné le « demandeur »

### **Par la Région Provence-Alpes-Côte d'Azur**

Adresse : Hôtel de Région - 27 place Jules Guesde - 13481 Marseille cedex 20

SIRET : 23130002100012

### **Confidentialité**

- 1) Le demandeur s'engage à garder strictement confidentielles les informations qui lui seront transmises par le diffuseur.

Le demandeur prendra toutes les mesures nécessaires pour préserver le caractère confidentiel des informations. Ces mesures ne pourront pas être inférieures à celles prises par elle pour la protection de ses propres informations confidentielles.

- 2) Le demandeur s'engage à ne communiquer lesdites informations qu'aux membres de son personnel appelés à en prendre connaissance et à les utiliser, ou un tiers concourant à l'aménagement du territoire avec lequel elle est en relation contractuelle. Ces personnes sont limitativement désignées par le demandeur et tenues au secret professionnel conformément aux conditions définies aux alinéas 3 et 4 et 5 du IV de l'article D.98-6-3 du Code des Postes et Communications Electroniques.

Les personnes désignées sont :

3)

- 3) Le demandeur s'engage à prendre toutes les dispositions pour que ses employés et contractants traitent lesdites informations conformément aux dispositions de confidentialité définies au IV de l'article D 98-6-3 du Code des postes et des communications électroniques.
- 4) En cas de redistribution des données à des collectivités d'échelle inférieure, le demandeur possède les mêmes droits que la collectivité initiale, mais uniquement sur le périmètre qui lui est propre. Il est ainsi en mesure de redistribuer, à son tour, ces données à une échelle inférieure, ou à un tiers, selon les mêmes contraintes de formalisme et d'engagement que celles demandées pour la communication de ces données par la Région. La communication de données « infrastructures d'accueil et réseaux » entre les collectivités territoriales et/ou leurs groupements s'effectue strictement sur leur périmètre d'intervention commun. Un découpage géographique de ces données est donc nécessaire lorsqu'il s'agit de communiquer ces données à une collectivité d'un niveau inférieur géographiquement.

Dans le cas où les données sont partagées entre plusieurs collectivités au sein d'un système d'information unifié, l'octroi de droits d'accès à ce système d'information doit être considéré comme une communication à part entière. Il doit être précédé d'une demande respectant le formalisme des demandes initiales, faire l'objet d'une information des opérateurs concernés et être restreint au périmètre géographique de la collectivité bénéficiant de ce droit d'accès. Par ailleurs, ce système de partage doit intégrer un dispositif permettant de définir le périmètre géographique de chaque accès octroyé. Les exigences de chiffrement (type VPN) des liaisons entre les collectivités utilisatrices s'appliquent tout particulièrement dans ce cas.

Dans tous les cas, la collectivité doit informer préalablement les opérateurs et les gestionnaires d'infrastructures concernés de la communication de ces données et de leur destination.

Pour plus d'informations, se référer au « Guide de la connaissance des réseaux » édité par l'ARCEP (Autorité de Régulation des Communications Electroniques et des Postes) sur le lien suivant : [Microsoft Word - 2012-10-24\\_guide\\_connaissance\\_des\\_reseaux\\_VF.doc \(arcep.fr\)](#)

- 5) Il est rappelé que la communication des données ne doit pas créer de discrimination entre opérateurs et ne doit pas porter atteinte au secret en matière commerciale et industrielle, mentionné à l'article 6 de la loi n°78-753 du 17 juillet 1978.

## **Sécurité**

Le demandeur s'engage à mettre en œuvre une série de mesures visant à garantir la sécurité des informations communiquées et notamment à :

- héberger les informations sur des serveurs dont l'accès physique n'est autorisé qu'aux personnes désignées, telles que décrites à l'article 5 du présent acte d'engagement,
- n'effectuer le chargement, la consultation et le traitement des informations que sur des postes de travail disposant d'identifiants propres aux personnes désignées,
- maintenir à jour en permanence un logiciel antivirus sur ces postes de travail et être à jour de l'ensemble des correctifs de sécurité pour tous ses logiciels installés sur ces postes de travail,
- ne relier ces postes de travail à l'Internet uniquement à travers un réseau interne doté de passerelles sécurisées et de pare-feu bien paramétrés,
- dans les cas où ces postes de travail sont reliés à un serveur distant, à assurer par un réseau interne à la Partie Bénéficiaire la liaison entre les postes et le serveur et à ce qu'en aucun cas les informations ne circulent sur le réseau public, sauf mise en œuvre d'un chiffrement de la liaison (type VPN).

## **Limitation de responsabilité**

Le demandeur reconnaît et accepte que les données sont fournies en l'état, telles que détenues par la Région dans le cadre de ses missions, sans autre garantie, expresse ou tacite. La Région ne peut garantir au demandeur l'absence de défauts et ne peut être tenue responsable de tout préjudice ou dommage de quelque sorte subi par le demandeur ou par des tiers du fait de la réutilisation.

Fait à \_\_\_\_\_, le \_\_\_\_/\_\_\_\_/202\_\_

Nom et qualité du signataire :