



MARCHE DE « PRESTATIONS INTELLECTUELLES »

**« PRESTATIONS POUR LA MISE EN PLACE DU
REGLEMENT GENERAL POUR LA PROTECTION DES DONNEES ET LES
PRESTATIONS POUR LA MISSION DE DELEGUE EXTERNALISE A LA
PROTECTION DES DONNEES »**

**CAHIER DES CLAUSES TECHNIQUES
PARTICULIERES**

Références : M 2025/38

SOMMAIRE

PREAMBULE	3
Article 1- contexte.....	3
Article 2- Objet, nature et forme du marché	4
Article 3 – Conditions d’exécution du marché	5
Article 4 – obligations des parties.....	9
Article 5 – qualifications et capacités attendues du titulaire.....	9
Article 6 – livrables attendus	10

PREAMBULE

L'Etablissement Public Foncier d'Occitanie, établissement public à caractère industriel et commercial de l'État, a été créé par décret du 2 juillet 2008, modifié par décrets du 29 décembre 2014, du 05 mai 2017, 30 mars 2020 et 17 mars 2025. Il est habilité à intervenir sur les 13 départements de la région Occitanie (à l'exception des périmètres des trois EPF locaux du Tarn, Montauban et Toulouse).

Conformément aux dispositions de l'article L. 321-1 du code de l'urbanisme, l'EPF a compétence pour procéder à toutes les acquisitions foncières et immobilières de nature à faciliter l'utilisation et l'aménagement ultérieur des biens acquis. Il peut aussi effectuer les études et travaux nécessaires à leur accomplissement et, le cas échéant, participer à leur financement.

Ces missions peuvent être réalisées par l'EPF soit pour son compte ou celui de l'État et de ses établissements publics, soit pour celui des collectivités territoriales, de leurs groupements, ou de leurs établissements publics en application de conventions foncières passées avec eux. En application de l'article L. 321-1 précité, l'EPF doit mettre en place des stratégies foncières afin de mobiliser du foncier et de favoriser le développement durable et la lutte contre l'étalement urbain.

Ses Principaux champs d'intervention en tant qu'opérateur public sont :

- Les transitions immobilières
- La maîtrise d'ouvrage de travaux et d'études
- La gestion locative et immobilière

A ce jour, les effectifs de l'EPF sont de plus de 80 personnes réparties sur un site principal (à Montpellier) et un site secondaire (à Toulouse).

- Bâtiment 19 à Montpellier :
Parc Club du Millénaire – 1025 rue Henri Becquerel – 34060 MONTPELLIER Cedex 2,
- Bâtiment 21 à Montpellier :
Parc Club du Millénaire – 1025 rue Henri Becquerel – 34060 MONTPELLIER Cedex 2,
- Bâtiment 3 à Toulouse :
78 chemin des Sept deniers – RDC Bâtiment 3 – 31085 TOULOUSE Cedex 2

Site internet pour connaître l'EPF d'Occitanie : <https://www.epf-occitanie.fr/>

ARTICLE 1 - CONTEXTE

En 2021, l'EPF a passé un marché public afin de répondre aux obligations relatives au RGPD

Le prestataire retenu a notamment procédé à la création et la mise à jour d'un registre de traitement pour les fonctions/activités des différentes directions et différents organes de l'établissement, à savoir :

- Direction générale (DG) :
Pôles : direction, instances, communication.
- Direction du pilotage de la performance et de la prospective (D3P) :
Fonctions : suivi des études, des partenariats et de l'activité de l'EPF, productions d'indicateurs de suivi de l'activité ;
- Direction traitement des copropriétés et restructuration urbaine (DTC-RU) :
Fonctions : Suivi du traitement des copropriétés et restructuration urbaine, transactions, gestion locative ;
- Direction administrative, financière, et des systèmes d'information (DAFSI) :
Pôles : financier et budgétaire, juridique, marchés publics, systèmes d'information, bâtimentaire/logistique ;
- Direction Travaux et Expertise Bâtimentaire (DTEB) :

- Suivis des études, travaux et diagnostics techniques ;
- Direction des ressources humaines (DRH) :
Fonctions : gestion des ressources humaines et paie ;
- Direction foncière est (DFE) et Direction foncière ouest (DFO) :
Fonctions : acquisitions, cessions, conventionnement et gestion du patrimoine.
- CSE

Ce travail a permis d'identifier les données personnelles collectées, par l'EPF dans le cadre de son activité pour le compte de collectivités et de l'Etat.

Le présent marché s'inscrit dans la continuité du précédent.

Il est demandé au titulaire :

- D'actualiser registre de traitement de données collectées par l'EPF au regard de l'évolution forte de son activité depuis 2021 (développement récent en particulier de la gestion locative et des situations d'impayés des locataires)
- de s'assurer en particulier de la conformité des activités métiers
- d'avoir une analyse spécifique du SI de l'EPF qui a fortement évolué en 2025,
- de conduire les AIPD obligatoires notamment identifiés par le titulaire du précédent marché en 2025
- de mettre en place les procédures pour la conformité et la sécurisation des données personnelles.

Une action de mise en place de procédure internes pour la gestion des données personnelles sera à prévoir.

Une action de formation est à prévoir pour sensibiliser le personnel de l'EPF aux règles encadrant les données personnelles et aux risques liés aux libertés et à la vie privée.

Dans le cadre son activité, l'EPF n'a pas vocation à recevoir du public dans ses locaux.

A ce jour, l'EPF n'a reçu aucune demande ou réclamation concernant la protection des données.

ARTICLE 2- OBJET, NATURE ET FORME DU MARCHE

Pour le compte de l'Etablissement Public Foncier d'Occitanie (EPF), la présente consultation a pour objet la mise en place du **Règlement Général de la Protection des données (RGPD) et d'un Délégué externe à la Protection des Données (DPD)**.

En tant que responsable du traitement, l'EPF doit veiller à ce que les données personnelles soient collectées pour un usage déterminé, légitime et pertinent, pour un temps limité, en toute sécurité et confidentialité, et en respectant le droit des personnes (information, accès, opposition, suppression).

Le présent accord-cadre a deux objectifs :

- être en œuvre la conformité à la protection des données à caractère personnel de l'EPF : appréhender et mettre en œuvre les différentes obligations afin que l'EPF puisse assurer la conformité du RGPD et la maintenir, conduire les audits réglementaires, organiser, en lien avec l'EPF les activités de suppression et archivage des données personnelles ;
- de désigner un délégué à la protection des données externe qui aura un rôle actif pour : assister l'EPF, dans la continuité de la mise en conformité engagée pour la RGPD, sensibiliser les salariés aux obligations en termes d'information des personnes sur le traitement des données personnelles collectées, l'objectif du traitement et leurs droits d'accès, de rectification ou d'effacement etc.

Tout au long de la mission, le prestataire sera accompagné par un interlocuteur dédié, en lien avec le pôle juridique et le pôle informatique.

Le marché est décomposé en 2 postes définis comme suit :

- **Poste 1** : Mise en œuvre du RGPD
- **Poste 2** : Externalisation de la mission du DPD/DPO

ARTICLE 3 – CONDITIONS D'EXECUTION DU MARCHE

3.1.1 – Poste 1 : Mise en œuvre du RGPD

En lien avec le responsable du traitement, le prestataire retenu aura pour missions de :

- **Actualiser annuellement la cartographie et le recensement les activités de l'EPF qui nécessitent la collecte et le traitement des données personnelles**
 - Etablir un diagnostic des traitements effectués par l'EPF.
- **Mettre à jour semestriellement au sein de l'EPF, les différents traitements des données :**
 - Registre du responsable du traitement à compléter en fonction de l'évolution des missions dévolues aux directions,
 - Registre des sous-traitants en prenant contact avec chaque sous-traitant pour vérifier leurs obligations en matière de sécurité, de confidentialité et de protection des données personnelles traitées,
 - revue des outils numériques.
- **Mettre en conformité et mise à jour du traitement des données des différentes directions :**

Une fois les registres mis à jour, le titulaire vérifie que chaque traitement de données identifié est conforme au RGPD :

 - en faisant le tri des données en s'assurant que seules subsistent les données strictement nécessaires à la poursuite des objectifs de l'EPF ;
 - en identifiant la base juridique du traitement ;
 - en révisant voire en ajoutant les mentions d'information afin qu'elles soient conformes aux exigences du RGPD ;
 - en s'assurant du respect des droits des personnes concernées (droit d'accès, retrait du consentement...) ;
 - en vérifiant les mesures de sécurité mises en place ;
 - en mettant en œuvre une procédure de gestion du cycle de vie des données personnelles avec les différents services de l'EPF.
- **Réalisation des AIPD (Analyse d'impact des données)**

Mener les AIPD identifiées pour les traitements à risque (article 35 RGPD) selon la méthodologie de la CNIL.

▪ **Etablir un plan d'action pour les traitements et en particulier pour les traitements identifiés comme prioritaires :**

Pour pouvoir réaliser cette mise en conformité, le titulaire identifie les traitements à risque, qui seront prioritaires et propose un plan de traitement (action, calendrier, pilote, méthode de suivi) :

- En mettant en place les procédures qui garantiront la protection des données à tout moment en prenant en compte l'ensemble des événements pouvant survenir sur un traitement de données personnelles comme les failles de sécurité, des demandes d'accès ou de rectification. La mise en place de la procédure doit permettre de savoir à qui s'adresser pour chaque type d'incident pouvant intervenir ;
- En identifiant des risques liées à la non-conformité ;
- En élaborant un plan de conformité ;
- En produisant les modèles pour le recueil du consentement des personnes concernées ;
- En intégrant les mentions légales et les procédures pour l'exercice de ses droits : dans les marchés publics, les contrats, les conventions et le site internet de l'EPF et dans tout autre document que le titulaire jugera utile ;
- En mettant en place des politiques de procédures internes (type archivage) et proposer des solutions adaptées aux spécificités organisationnelles et techniques de l'EPF.
- En proposant ses Conseils juridiques.

• **Mise en place de la documentation de la conformité :**

Pour chaque traitement de données, le titulaire constitue un dossier permettant de justifier que le traitement est conforme au RGPD.

Cette documentation devra notamment comporter :

- Le registre et les fiches de traitement correspondantes ;
- Les mentions d'information et les modèles de recueil du consentement des personnes concernées ;
- Les procédures mises en place pour l'exercice des droits des personnes concernées ;
- Les contrats de sous-traitance de données personnelles ;
- La procédure interne en cas de violation de données ;
- Les preuves des consentements donnés.

• **Sensibiliser le personnel de l'EPF à la RGPD**

Selon des modalités qui seront arrêtées conjointement lors de l'exécution du marché, le titulaire interviendra dans la communication à destination des directions concernées. Pour cela le titulaire procédera à :

- La rédaction des documents de communication à destination de la direction générale, de la ou les directions concernées et du Directeur de la DAF-SI ;
- La rédaction et présentation de la communication à destination des collaborateurs opérationnels par services ou directions.

• **Rédiger le corpus documentaire de conformité**

Mentions d'information, politiques (politique de confidentialité, politique cookies), procédures (procédure de gestion des violations de données, procédure d'exercice des droits, procédure d'archivage...), processus (privacy by design/default), référentiels des durées de conservation. Cette liste n'est pas exhaustive.

3.1.2 – Objectifs attendus pour le poste n°1

Suite à la mise à jour du registre des traitements, il s'agit dans un premier temps, pour le prestataire sélectionné de :

- Travailler avec elles à une mise à jour de leur registre de traitements et procéder à une déclaration du DPD auprès de la CNIL. La cartographie doit se faire en accompagnement rapproché c'est-à-dire que les directions ne doivent pas renseigner seules un « fichier Excel » mais doivent être accompagnées pour cela ;
- Suivre la mise à jour de la cartographie au fil de l'eau ;
- Proposer un plan d'action de mise en conformité (suppression, archivage, base légale de conformité, mesures de sécurité etc).
- Prioriser le travail de mise en conformité en fonction de l'importance et de la nature (interne ou externe) des traitements ;
- Commencer la mise en conformité des traitements prioritaires, en lien avec l'interlocuteur ;
- S'assurer de la connaissance du RGPD au sein des directions.

Globalement, il s'agit donc d'élaborer un plan d'action de mise en conformité des directions suite au travail amorcé par le précédent titulaire et de sa mise à jour. Un lien régulier avec l'interlocuteur sera nécessaire afin de valider chacun des points.

Si des non-conformités importantes devaient être relevées, celles-ci feraient l'objet d'un échange prioritaire avec l'interlocuteur afin de les corriger rapidement.

La prestation attendue devra accompagner plusieurs directions en parallèle et en rendre compte à l'interlocuteur.

3.1.3 – calendrier et livrables attendus pour le poste n°1

Lors de la réponse à la consultation, il est demandé au candidat de communiquer un planning détaillé pour le suivi et la mise à jour de la conformité du RGPD (poste n°1).

Dans le planning proposé et dans le cadre du prix forfaitaire, les candidats doivent intégrer dans la prestation :

- Une réunion de démarrage sur site ;
- Des réunions intermédiaires en visioconférence à fixer par le prestataire ;
- Une réunion de restitution sur site.
- La production d'un plan d'action (rapport rédigé)

En fonction du temps de travail sur site passé pour les audits des différentes directions de l'EPF, les bons de commandes se feront en demi-journée ou en journée entière (voir BPU).

3.2.1 – Poste 2-a : Externalisation de la mission de DPD

Parallèlement à la mise en place de la conformité du RGPD (poste n°1), le titulaire aura pour mission d'être le DPD externalisé de l'EPF, et gérer tous les documents et dossiers nécessaires à la protection des données.

La prestation attendue doit être en tout point conforme aux articles 38 et 39 du règlement UE n°2016/679.

Comme indiqué sur le site de la CNIL, le rôle du délégué à la protection des données est d'être le « chef d'orchestre » de la conformité en matière de protection des données.

A ce titre :

- il devra constamment garantir l'exercice des droits des personnes conformément aux articles 15 - 16 - 17 - 18 - 19 - 20 - 21 et 22 du règlement UE n°2016/679 (droits d'accès, de rectification et d'effacement, d'opposition et de prise de décision individuelle automatisée,).
- il devra s'assurer de la mise en œuvre ainsi que de la vérification des procédures mises en place concernant l'ACCOUNTABILITY, le PRIVACY BY DEFAULT et le PRIVACY BY DESIGN ou équivalent.

Il est principalement chargé de :

- Informer et de conseiller le responsable de traitement ou le sous-traitant ainsi que leurs salariés ;
- Contrôler le respect du règlement et du droit national en matière de protection des données ;
- Conseiller si besoin l'établissement sur les risques liés à la protection des données et d'en vérifier l'exécution ;
- Contrôler les procédures mises en place ;
- Coopérer avec l'autorité de contrôle (CNIL) et d'être le point de contact de celle-ci pour l'EPF ;
- Répondre aux personnes concernées exerçant leurs droits ;
- Recevoir et répondre à toute question ou réclamation relative à la protection des données ;
- Notifier dans les délais réglementaires les violations de données ;
- S'assurer de la tenue à jour de l'ensemble des registres (registre d'exercice des droits et registre des violations de données).

Le prestataire sera déclaré comme DPD auprès de la CNIL.

La mission aura pour périmètre l'intégralité des traitements des données à caractère personnel mis en œuvre par l'EPF d'Occitanie.

Le DPD interviendra aussi en relais des actions et des demandes des services supports et opérationnels, et assure le cas échéant un certain nombre de tâches opérationnelles : collecte et analyse des informations remontées par les services de l'EPF, relecture critique, mise en forme de documents...etc.

Le DPD rendra compte a minima mensuellement à l'EPF. Le soumissionnaire proposera dans sa réponse, une périodicité propre.

3.2.2 – Poste 2-b : Formation et assistance pour la protection des données

Il est demandé au DPD d'assurer la sensibilisation des salariés à la protection des données :

- Expliciter le contenu et les enjeux du RGPD à l'ensemble du personnel de la structure, pour sensibiliser et veiller à la prise de conscience sur l'importance du respect de ce règlement.
- Présenter aux salariés les obligations en termes d'information des personnes sur le traitement des données personnelles collectées, l'objectif du traitement et leurs droits d'accès, de rectification ou d'effacement...

En fonction des besoins des directions de l'EPF, les formations se feront sur bons de commande.

A des demandes courtes et précises par l'EPF via son interlocuteur, il est demandé au prestataire d'effectuer une assistance en ligne.

Le Titulaire pourra répondre, par courrier électronique ou par téléphone, sur demande, et déterminer les solutions (notamment juridiques) aux questions ponctuelles et être rémunéré sur la base du BPU (1 heure ou 4 heures).

Cette formule d'assistance repose sur le principe d'une réponse simple et rapide par des experts du domaine.

Le délai de réponse sera fonction du type de demande formulée :

- En cas de demande dite « classique », le délai de réponse sera, au plus, de 2 jours ouvrés ;
- De manière exceptionnelle, en cas de demande urgente nécessitant une intervention rapide (par exemple importante violation de données ou sollicitation de l'autorité de contrôle), la réponse devra intervenir dans les plus brefs délais (1 jour ouvré maximum).

Chaque sollicitation donnera lieu à la rédaction d'une note détaillée de la réponse apportée, sur laquelle l'EPF pourra s'appuyer pour mettre en œuvre la solution proposée.

Le temps consacré à cette prestation sera inscrit dans un fichier de suivi qui contiendra, a minima, les éléments suivants :

- Date et heure ;
- Demande ;
- Temps nécessaire pour le traitement de la demande ;
- Synthèse de la réponse apportée.

Ce fichier de suivi sera mis à jour et transmis à l'EPF, immédiatement après chaque sollicitation.

La facturation basée sur le BPU sera effectuée au temps réel passé qui sera mentionné dans le fichier de suivi. Les heures indiquées au BPU sont fractionnables en temps réel.

3.2.3 Calendrier et livrables

Le DPD propose en début de prestation un plan de sensibilisation des personnels à mettre en œuvre annuellement ainsi que les supports à diffuser.

Il assure des retours mensuels sur les sollicitations de l'exercice des droits des personnes.

ARTICLE 4 – OBLIGATIONS DES PARTIES

Prestataire :

- prendre en compte l'organisation de l'EPF et mettre en place des dispositifs pour le maintien et mise à jour de la prise en compte du RGPD ;
- Proposer des intervenants dont il garantit les compétences et l'expérience ;
- Non-divulgaration des éléments réunis sur la conformité des directions de l'EPF, éléments réputés confidentiels ;
- Faire valider les supports utilisés par l'EPF ;
- Concéder de façon permanente l'utilisation de tous les supports réalisés lors de la prestation.

L'EPF :

- Accompagner le prestataire pour une bonne compréhension de l'organisation et des procédures à finaliser et à mettre en place ;
- Faciliter le dialogue avec les directions en présentant le titulaire lors de la première réunion de prise de contact.

ARTICLE 5 – QUALIFICATIONS ET CAPACITES ATTENDUES DU TITULAIRE

Conformément aux articles 37 et 39 du règlement UE n°2016/679, le prestataire est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière des données et de sa capacité à accomplir les missions (article 39).

Par conséquent, il :

- Justifie d'une connaissance du droit et des pratiques en matière de protection des données à caractère personnel ;
- Justifie avoir suivi des formations RGPD et, le cas échéant, de formations labellisées par la CNIL et, le cas échéant, d'une certification des compétences du DPD délivrée par un organisme de certification agréé par la CNIL ;
- Dispose d'une connaissance appropriée en matière de systèmes d'information et de sécurité informatique de nature à lui permettre d'identifier les enjeux et appréhender les recommandations et exigences de la CNIL et autres autorités de protection des données à caractère personnel en la matière ;
- Dispose d'une connaissance approfondie de l'environnement légal et réglementaire applicable au secteur public ;
- Dispose de compétences en gestion des risques, audit et contrôle interne ;
- Dispose des qualités relationnelles permettant de favoriser la sensibilisation des équipes et l'accompagnement aux changements de pratiques ;
- Justifie d'une expérience professionnelle dans des missions transverses, d'animation de réseau, etc. ;
- Respecte le principe de confidentialité voire est soumis au secret professionnel ;
- S'engage à veiller à ce que les éventuelles autres fonctions de l'équipe de DPD externalisé n'entraînent pas de conflit d'intérêt avec l'activité de l'EPF ;
- Est disponible ;
- Justifie de références pour des actions similaires.

Savoir-faire :

Le DPD doit maîtriser les techniques propres à son métier, concernant notamment :

- La conception/réalisation d'actions de sensibilisation ;
- La formulation de conseils/préconisations ;
- La conception de procédures ;
- La réalisation ou le pilotage d'études/d'audits ;
- La sécurité informatique.

Savoir-être :

Le DPD fait preuve d'objectivité, d'indépendance, de probité et de discrétion.

Il doit également être un « communicant » pour sensibiliser et accompagner les équipes dans la mise en conformité.

ARTICLE 6 – LIVRABLES ATTENDUS

Le titulaire devra fournir l'ensemble des documents réglementaires conformément au RGPD pour le poste n°1, suivant la liste non exhaustive :

- Compte-rendu d'entretiens ;
- Cartographie des traitements de données personnelles et liste des traitements à risques ;
- Recensement des mesures de sécurité informatique et organisationnelle existantes ;
- AIPD
- Rapport de synthèse du diagnostic de conformité (analyse des écarts de conformité et des risques vis-à-vis des exigences RGPD) ;
- Fiches de traitements ;
- Registre des traitements ;
- Registre des sous-traitants ;
- Plan d'action avec calendrier, priorisation, responsable de l'action, etc... ;
- Compte rendu d'Audit de maturité RGPD ;
- Compte rendu Diagnostic sécurité des SI ;
- Compte-rendu des copils ou de toute réunion de préparation auprès de l'EPF ;
- Etc...

Tous les livrables et documents seront générés par un logiciel et ils deviendront la propriété de l'EPF et devront être exploitables par des logiciels standards.

Pour le suivi du RGPD et chaque mois, le prestataire produit un compte-rendu de la mise à jour de la mise en conformité.

Les délais de remise des documents seront précisés par le titulaire et tous les documents devront être envoyés à l'interlocuteur.

A l'issue de la prestation, une réunion de clôture avec le responsable du traitement sera prévue afin d'assurer une bonne transmission de toutes les informations nécessaires pour le suivi des actions et des derniers livrables.