Etablissement
Public Territorial

Séance ordinaire du conseil territorial du 13 décembre 2022
EXTRAIT DU REGISTRE DES DÉLIBÉRATIONS

DÉLIBÉRATION n°2022-12-13_2983

Convention de mutualisation des fonctions de délégué à la protection des données entre le syndicat mixte ouvert SIIM94 et l'EPT

L'an deux mille vingt-deux, le 13 décembre à 19h les membres du Conseil de l'EPT Grand-Orly Seine Bièvre se sont réunis en Mairie de Vitry-sur-Seine, en séance plénière ouverte par son président, Monsieur Leprêtre, sur convocation individuelle en date du 7 décembre 2022. La séance est retransmise en direct sur le site internet de l'EPT.

Ville	Nom	Présent	A donné pouvoir à	Votes
Villejuif	Mme ABDOURAHAMANE Rakia	Représentée	V. MORIN	P
Vitry-sur-Seine	M. AFFLATET Alain	Représenté	B. VERMILLET	P
Gentilly	M. AGGOUNE Fatah	Présent		P
Villeneuve-Saint-Georges	Mme AMKIMEL Saloua	Absente		
Le Kremlin-Bicêtre	Mme AZZOUG Anissa	Présente		P
Vitry-sur-Seine	M. BELL-LLOCH Pierre	Présent		P
Vitry-sur-Seine	M. BENBETKA Abdallah	Représenté	K BEN-MOHAMED	P
Juvisy-sur-Orge	M. BENETEAU Sébastien	Présent		P
Vitry-sur-Seine	M. BEN-MOHAMED Khaled	Présent		P
Juvisy-sur-Orge	Mme BENSARSA REDA Lamia	Présente		P
Viry Chatillon	M. BERENGER Jérôme	Présent		P
Thiais	M. BEUCHER Daniel	Présent		P
Chevilly-Larue	Mme BOIVIN Régine	Présente		P
Villejuif	M. BOUNEGTA Mahrouf	Présent		P
Vitry-sur-Seine	M. BOURDON Frédéric	Présent		P
Ivry-sur-Seine	M. BOUYSSOU Philippe	Absent		
Villeneuve-Saint-Georges	Mme CABILLIC Kati	Absente		
Viry-Châtillon	Mme CAPELO Vanessa	Représentée	L. SAUERBACH	P
Fresnes	Mme CHAVANON Marie	Présente		P
Savigny-sur-Orge	Mme CHEVALIER Catherine	Représentée	A. TEILLET	P
Athis-Mons	M. CONAN Gautier	Présent		P
Savigny-sur-Orge	M. DARMON Charles	Absent		
Chevilly-Larue	Mme DAUMIN Stéphanie	Présente		P
Cachan	Mme DE COMARMOND Hélène	Représentée	C. VIELHESCAZE	P
L'Haÿ-les-Roses	M. DECROUY Clément	Représenté	F. SOURD	P
Savigny-sur-Orge	M. DEFREMONT Jean-Marc	Présent		P
Le Kremlin-Bicêtre	M. DELAGE Jean-François	Représenté	J-L. LAURENT	P
Arcueil	Mme DELAHAIE Carine	Représentée	I. SOUID-BEN CHEIKH	P
Thiais	M. DELL'AGNOLA Richard	Présent		P
Villeneuve-Saint-Georges	M.DELORT Daniel	Représenté	J-P VIC	P
Vitry-sur-Seine	Mme DEXAVARY Laurence	Absente		
Ivry-sur-Seine	Mme DORRA Maryse	Présente		P
Morangis	M. DUFOUR Jean-Marc	Absent		
Vitry-sur-Seine	Mme EBODE ONDOBO Bernadette	Présente		P
Savigny-sur-Orge	Mme EUGENE Joëlle	Absente		
Villejuif	M. GARZON Pierre	Représenté	A-G LEYDIER	P
Villeneuve-Saint-Georges	M. GAUDIN Philippe	Présent		P
Choisy-le-Roi	Mme GAULIER Danièle	Présente		P
Villeneuve-le-Roi	M. GONZALES Didier	Présent		P
Villeneuve-le-Roi	Mme GONZALES Elise	Représentée	D. GONZALES	P
Ablon-sur-Seine	M. GRILLON Éric	Présent		P
Athis-Mons	M.GROUSSEAU Jean-Jacques	Présent (2)		
Choisy-le-Roi	M. HUTIN Sébastien	Absent		
Choisy-le-Roi	M. ID ELOUALI Ali	Représenté	A. LIPIETZ	P
Orly	Mme JANODET Christine	Présente		P
Vitry-sur-Seine	Mme KABBOURI Rachida	Représentée	M. DORRA	P
Villejuif	Mme KACIMI Malika	Absente		

Ville	Nom	Présent	A donné pouvoir à	Votes
Vitry-sur-Seine	M. KENNEDY Jean-Claude	Présent		P
Ivry-sur-Seine	Mme KIROUANE Ouarda	Présente		P
Arcueil	Mme LABROUSSE Sophie	Présente		P
Vitry-sur-Seine	M. LADIRE Luc	Représenté	P. BELL-LLOCH	P
Villejuif	M. LAFON Gilles	Présent		P
Paray-Vieille-Poste	Mme LALLIER Nathalie	Présente		P
Le Kremlin-Bicêtre	M. LAURENT Jean-Luc	Présent		P
Fresnes	Mme LEFEBVRE Claire	Présente		P
Vitry-sur-Seine	Mme LEFEBVRE Fabienne	Présente		P
Vitry-sur-Seine	M. LEPRETRE Michel	Présent		P
Orly	M. LERUDE Renaud	Présent		P
L'Haÿ-les-Roses	M. LESSELINGUE Pascal	Présent		P
Thiais	Mme LEURIN-MARCHEIX Virginie	Présente		P
Villejuif	Mme LEYDIER Anne-Gaëlle	Présente		P
Athis-Mons	Mme LINEK Odile	Présente		P
Villejuif	M. LIPIETZ Alain	Présent		P
Vitry-sur-Seine	Mme LORAND Isabelle	Représentée	C. VEYRUNES-LEGRAIN	P
Villeneuve-le-Roi	M. MAITRE Jean-Louis	Absent		
Ivry-sur-Seine	M. MARCHAND Romain	Présent		P
Rungis	M. MARCILLAUD Bruno	Présent		P
Ivry-sur-Seine	M. MOKRANI Mehdi	Absent		
Villejuif	Mme MORIN Valérie	Présente		P
Vitry-sur-Seine	Mme MORONVALLE Margot	Représentée	B. EBODE ONDOBO	P
L'Haÿ-les-Roses	M. MOUALHI Sophian	Présent		P
Ivry-sur-Seine	M. MRAIDI Mehrez	Représenté	M. LEPRETRE	P
L'Haÿ-les-Roses	Mme NOWAK Mélanie	Représentée	P. LESSELINGUE	P
Choisy-le-Roi	Mme OSTERMEYER Sushma	Absente		
Choisy-le-Roi	Mme OZCAN Canan	Représentée	E. GRILLON	P
Choisy-le-Roi	M. PANETTA Tonino	Représenté	D. GAULIER	P
Arcueil	Mme PECCOLO Hélène	Présente		P
Ivry-sur-Seine	M. PECQUEUX Clément	Présent		P
Cachan	M. PETIOT David	Représenté	H. PECCOLO	P
Ivry-sur-Seine	Mme PIERON Marie	Représentée	J-C KENNEDY	P
Fresnes	M. PIROLLI Yann	Présent		P
Cachan	M. RABUEL Stéphane	Présent		P
Athis-Mons	M. SAC Patrice	Représenté	G. CONAN	P
Viry Chatillon	M. SAUERBACH Laurent	Présent		P
Ivry-sur-Seine	Mme SEBAIHI Sabrina	Représentée	L. TAUPIN	P
Thiais	M. SEGURA Pierre	Présent		P
Orly	Mme SOUID-BEN CHEIKH Imène	Présente		P
L'Haÿ-les-Roses	Mme SOURD Françoise	Présente		P
Athis-Mons	Mme SOW Fatoumata	Présente		P
Valenton	Mme SPANO Cécile	Représentée	M. YAVUZ	P
Chevilly-Larue	M. TAUPIN Laurent	Présent		P
Savigny-sur-Orge	M. TEILLET Alexis	Présent		P
Choisy-le-Roi	M. THIAM Moustapha	Absent		
Gentilly	Mme TORDJMAN Patricia	Représentée	F. AGGOUNE	P
Le Kremlin-Bicêtre	M. TRAORE Ibrahima	Présent (1)		P
Fresnes	Mme VALA Cécilia	Présente		P
Morangis	Mme VERMILLET Brigitte	Présente		P
Vitry-sur-Seine	Mme VEYRUNES-LEGRAIN Cécile	Présente		P
Villeneuve-Saint-Georges	M.VIC Jean-Pierre	Présent		P
Cachan	M. VIELHESCAZE Camille	Présent		P
Viry Chatillon	M. VILAIN Jean-Marie	Représenté	J. BERENGER	P
Valenton	M. YAVUZ Métin	Présent		P

(1) Jusqu'à la délibération n° 2998
(2) A partir de la délibération n° 3006

Secrétaire de Séance : Monsieur Sophian Moualhi

Nombre de Conseillers en exercice composant le Conseil de territoire			102
N° de délibérations	**Présents**	**Représentés**	**Votants**
2982 à 2998	60	28	88
2999 à 3005	59	28	87
3006 à 3044	60	28	88

Exposé des motifs

Le règlement général européen sur la protection des données (RGPD) entré en vigueur le 25 mai 2018 impose aux organismes publics de désigner un délégué à la protection des données (data protection officer ou DPO). Ce délégué est en charge du pilotage de la mise en conformité permanente de la politique des données de son organisation au RGPD et les obligations qu'il prévoit. Plus précisément, les principales missions d'un DPO sont les suivantes :

- Contrôle du registre des traitements des données personnelles
- Réalisation d'études d'impact
- Mise à jour des règles internes en matière de protection des données personnelles
- Conseil
- Sensibilisation

Par ailleurs, le DPO est le point de contact de l'organisation sur les questions de RGPD :

- Avec la CNIL en tant qu'autorité de contrôle
- Avec les personnes dont les données sont traitées par l'organisme comme les agents ou les usagers

Pour rappel, les infractions liées au non-respect des dispositions prévues par le RGPD peuvent être sanctionnées d'un montant allant jusqu'à 20 millions d'euros. Donc outre son obligation légale, le poste de DPO est hautement sensible.

Dès l'entrée en vigueur du RGPD en 2018, l'EPT a désigné une déléguée à la protection des données rattachée directement au secrétaire général.
Le travail de cette DPO a permis à l'EPT :

- de disposer d'un registre des traitements exploitable et d'un cartographie des logiciels et des sous-traitants qui traitent des données pour le compte de l'EPT
- d'avoir mis en conformité une grande partie des contrats, particulièrement les contrats de logiciels, impliquant des traitements de données à caractère personnel
- de diffuser une culture de la donnée et des bonnes pratiques en matière de données personnelles auprès des services en s'appuyant notamment sur un groupe de référents RGPD au sein de chaque DGA
- de disposer d'une charte des données personnelles

Or, cette déléguée a fait valoir ses droits à la retraite et a quitté l'EPT le premier semestre 2021. Il a été décidé de ne pas renouveler ce poste dont le volume de charge avait été estimé en décroissance régulière par son ancienne titulaire : 0,8 ETP en 2020, 0,7 ETP en 2021 et 0,5 ETP à partir de 2022 selon l'une des conclusions de son dernier rapport d'activité portant sur l'année 2020.

Depuis ce départ et dans un contexte de réorganisations de plusieurs pôles et directions générales adjointes, le pôle du développement numérique a été chargé d'organiser l'externalisation de cette fonction en s'appuyant sur les titulaires du marché correspondant dans le groupement de commandes du Sipperec, auquel l'EPT est adhérent : les cabinets WiseOrga et Bensoussan.

Or cette tentative d'externalisation n'a pas apporté satisfaction : analyse des besoins insuffisante, offre mal proportionnée et inadaptée au fonctionnement de l'EPT, tarifs onéreux en rapport à la réalité des prestations réalisées, défaut de pilotage interne du fait d'un manque de compétence et de compréhension des enjeux juridiques prédominants dans ces missions.

L'EPT a ainsi interrogé la direction du SIIM 94, syndicat informatique mixte ouvert dont l'EPT est adhérent, sur sa capacité institutionnelle et opérationnelle à assurer cette mutualisation de fonction.

Le SIIM 94 a apporté une réponse positive à cette interrogation et, suite à des échanges avec les services de l'EPT impliqués sur les questions de données personnelles, a présenté une convention de mutualisation de cette fonction.

Il est proposé au conseil territorial d'autoriser le président de l'EPT à signer cette convention.

DELIBERATION

Vu le Code Général des Collectivités Territoriales et notamment ses articles L5211-9 et L5211-10 et L5219-2 et suivants ;

Vu le décret n°2015-1665 du 11 décembre 2015 relatif à la métropole du Grand Paris et fixant le périmètre de l'établissement public territorial Grand-Orly Seine Bièvre dont le siège est à Vitry-sur-Seine ;

Vu l'avis de la commission permanente " Maîtrise budgétaire et fonctions support"

Entendu le rapport de Monsieur le président, et sur sa proposition,

Le conseil territorial délibère et, à l'unanimité,

1. Approuve le projet de convention relatif à la mutualisation de la fonction de délégué à la protection des données entre l'EPT et le SIIM 94 annexé à la présente.

2. Autorise le président ou son représentant à signer ladite convention et tout document afférent.

3. Invite le Président ou toute personne habilitée par lui, à accomplir toutes les formalités nécessaires à l'exécution des présentes.

Vote : Pour 88

A Vitry-sur-Seine, le 16 décembre 2022
Le Président

Michel LEPRETRE

La présente délibération est certifiée exécutoire,
étant transmise en préfecture le 19 décembre 2022
ayant été publiée le 19 décembre 2022

Le présent acte peut faire l'objet d'un recours devant le Tribunal Administratif compétent dans un délai de deux mois à compter de sa notification et/ou sa publication.

MUTUALISATION DE LA FONCTION DPO ENTRE LE SIIM94 ET GRAND ORLY SEINE BIEVRE

CONVENTION DE MISE EN ŒUVRE

17 OCTOBRE 2022

Ce document propose un cadre de travail pour une prestation de mutualisation de la fonction de délégué à la protection des données entre le SIIM94 et le GOSB.

A. TOOR

SIIM94

Etablissement public d'ingénierie pour l'informatique et les technologies de l'information et de la communication

24, bd Paul Vaillant Couturier – 94200 IVRY SUR SEINE
Tél. 01.43.90.25.30 - Email : direction@SIIM94.net

1 Contexte

Le SIIM94 et l'établissement public territorial « Grand Orly Seine Bièvre » (désigné par la suite « EPT GOSB ») ont été précurseurs dans la mise en conformité au Règlement Général européen sur la Protection des Données Personnelles (RGPD). Les deux établissements ont longtemps travaillé ensemble sur cette obligation réglementaire jusqu'au départ à la retraite début 2021 de la déléguée à la protection des données de l'EPT GOSB. Pour le maintien de sa conformité, l'EPT GOSB propose de mutualiser la fonction de Délégué à la Protection des Données (désigné par la suite « DPO ») avec le SIIM94 et ainsi de bénéficier de son expérience et s'appuyer sur des relations de travail préexistantes. L'objet de la présente convention est de cadrer cette mission.

2 Cadre général de la proposition

La convention est applicable à partir du 1/11/2022 et est valable pour une période d'un an, soit jusqu'au 31/10/2023. Elle est renouvelable par tacite reconduction, chaque partie pouvant librement mettre fin à la convention par l'envoi d'un courrier recommandé à l'autre partie au minimum deux mois avant son échéance.

Sur cette période, le DPO du SIIM94 deviendra également le DPO de l'EPT GOSB. L'article 38 du RGPD stipule que le DPO doit pouvoir rendre compte de son action au plus haut niveau de la direction. Il doit pouvoir exercer ses missions en toute indépendance, et ne subir aucune forme de pression. Dans cet objectif, et en accord avec l'EPT GOSB, le DPO mutualisé sera rattaché :

- Côté EPT GOSB, au secrétariat général ;
- Côté SIIM94, à la direction générale (statut actuel).

Le DPO mutualisé doit également pouvoir s'appuyer sur deux acteurs essentiels : la mission juridique et le pôle développement numérique.

Le SIIM94 mettra en place les moyens nécessaires pour assurer une prestation annuelle d'au plus 100 jours/homme (soit environ ½ ETP). Toute sollicitation supplémentaire à 100 jours est possible sous réserve que le SIIM94 puisse libérer des ressources en interne. Cette capacité maximale permet aussi d'apporter de la visibilité à l'EPT GOSB et participe à sécuriser la mission qui sera assurée.

La charge de travail liée à la mission est détaillée dans les paragraphes suivants et se répartit en 3 ensembles :

1) Prise en charge initiale ;
2) Fonction DPO au quotidien ;
3) Sécurisation de la conformité.

2.1 Prise en charge de la prestation

Cet ensemble couvre les missions suivantes :

- La prise de connaissance de l'ensemble de la documentation et des processus existants (~ 5 j.) ;
- La révision complète du registre des traitements de données personnelles (jusqu'à 60 j.).

L'objectif est de mener les actions nécessaires au démarrage de la prestation. Au-delà de la prise de connaissance de la documentation et des processus existants, le meilleur moyen pour le nouveau DPO de maîtriser le contexte et les enjeux du territoire en matière de données personnelles est de procéder à une revue complète du registre des traitements.

Cette révision du registre des traitements, document clé de la conformité, est une charge de travail importante car elle consiste à passer en revue chaque traitement de données personnelles identifié dans le document pour vérifier que les informations associées sont toujours d'actualité. Cela peut impliquer de rencontrer les différents responsables de traitements sur le terrain, permettant au passage au nouveau DPO d'établir des liens avec les directions métiers. Le DPO mutualisé pourra également s'appuyer sur le réseau de référents RGPD déjà en place à l'EPT GOSB.

Remarque : une mise à jour exhaustive du registre ne pourra se faire que si les interlocuteurs concernés se rendent disponibles pour répondre aux questions du DPO mutualisé. Dans le cas contraire, celui-ci ne pourra être tenu responsable.

De par son ampleur, la révision s'étalera sur les 12 premiers mois de la prestation mais ne sera plus nécessaire en année 2 et plus, les processus de mise à jour en continu du registre reprenant seuls le relais. Il en est de même, par définition, de la prise de connaissance de la documentation et des processus existants, qui se fera sur les premières semaines de la prestation. La spécificité de cet ensemble de missions est donc qu'il a vocation à n'être réalisé que la première année.

Remarque : la révision complète du registre n'est pas dans l'absolu une obligation pour initier la prestation mais elle est fortement recommandée car elle a valeur d'audit. Ensuite, le SIIM94 conseille de renouveler ce travail de révision complète du registre sur une base périodique, tous les 3 à 5 ans par exemple.

2.2 Fonction DPO au quotidien

Cet ensemble aura pour objectif :

- La prise en charge des sollicitations des citoyens du territoire pour tout ce qui touche à la protection des données personnelles ;
- La prise en charge des sollicitations des agents du GOSB pour tout ce qui touche à la protection des données personnelles ;
- La gestion des incidents impliquant des données personnelles (fuite, perte...), en coordination avec les services de l'EPT GOSB (DSI, mission juridique, métiers concernés, DG) et, le cas échéant, les fournisseurs et/ou la CNIL. Une organisation sera mise en place au sein du SIIM94 pour assurer une prise en charge des incidents RGPD au plus tard dans les 24h suivant leur déclaration au DPO mutualisé ;
- La fourniture en fin de prestation annuelle d'un rapport d'activité synthétique.

La particularité de cet ensemble de missions, au cœur de la fonction DPO, est qu'il n'est pas possible de déterminer à l'avance la charge de travail associée (proposition de facturation au temps passé). Par définition, ces missions auront la priorité sur les autres activités non visées à la convention.

Pour cela, le SIIM94 mettra en place une organisation permettant une prise en charge en continue de toute sollicitation liée au RGPD d'un citoyen ou d'un agent du GOSB dans les 24h (jours ouvrés). Ce dispositif est en particulier nécessaire pour gérer les violations de données nécessitant une notification à la CNIL dans les 72h.

2.3 Sécurisation de la conformité RGPD

Cet ensemble a pour objectif d'établir les livrables permettant de sécuriser la conformité RGPD du territoire. Le tableau ci-dessous reprend les recommandations de l'audit « Mission de délégué à la protection des données - Evaluation et rationalisation de la documentation » réalisé par le cabinet Wiseorga et intègre la charge de prise en charge de la mission. L'EPT GOSB donne son accord pour viser une mise en œuvre des éléments indiqués en priorité « haute » en année 1, estimé à environ 76 jours (hors fonction DPO au quotidien) :

Recommandation de l'audit	Analyse SIIM94	Priorité estimée	Charge DPO estimée
1. Politique générale de protection des données personnelles. • Mettre à jour ou supprimer la charte relative à la protection des données personnelles et de la vie privée en intégrant les éléments à la politique de gestion des données personnelles • Mettre en place une politique interne de protection des données personnelles	Des éléments sont en place, il s'agit surtout de les réviser et de les centraliser au sein d'un nombre plus réduit de documents. L'estimation de charge nécessite une pré-analyse qui sera faite en année 1.	Normale	1 j. (pré-analyse)
2. Nomination d'un DPO. • Désigner le (..) DPO • Faire le processus de saisie du DPO. Il existe des modèles de formalisation des avis du DPO à réaliser. • Elaborer un projet de communication interne sur la désignation du nouveau DPO	La désignation officielle du DPO, et la communication interne/externe associée, est incontournable et sera faite en début d'année 1. Ces éléments seront assurés par GOSB, avec l'aide du DPO mutualisé.	Haute	1 j.
3. Gouvernance de la donnée personnelle. • Rédiger une lettre de mission des référents RGPD • Réaliser et mettre en place une politique de gouvernance • Mettre en place des comités et l'animation du réseau de référent	Faire un retour d'expérience du travail avec les référents : d'autres organisation sont en effet envisageables. La charge correspond à une étude : audit de l'existant dont	Normale	10 j.

	entretiens avec les référents et proposition formalisée d'organisation de la gouvernance.		
4. Cartographie technique et cartographie légale. • Revoir la complétude des fiches de traitement de données personnels et les mettre à jour • Compléter les 5 dernières fiches de traitement des données personnels	Au-delà de la charge indiquée de complétude des fiches de traitement, il est fortement recommandé de disposer d'une cartographie du SI (travail annoncé comme en cours donc hors périmètre).	Normale	3 j.
5. Données personnelles. • Réaliser un référentiel de données afin d'obtenir un catalogue général de données personnelles • Mettre en place un catalogue des données par application	Plutôt que réaliser un catalogue des données par application, il faut commencer par identifier les données dites « sensibles » au sens du RGPD (charge intégrée dans le point 7), puis mener des EIVP pour les traitements associés (Cf. point 13).	Haute	Intégré au point 7 (hors EIVP, Cf. point 13)
6. Traitements. • Analyser la conformité de chaque traitement sur la base de la cartographie	Gros travail d'évaluation de conformité des traitements recensés, à faire idéalement en même temps que la révision du registre en année 1.	Haute	Intégré au point 7
7. Registres. • Mettre à jour le registre des traitements sur la base de la cartographie des traitements • Maintenir le registre en en condition opérationnelle • Mettre en place une procédure de tenue du registre des traitements	Cycle de mise à jour des entrées des registres (211 + 5 entrées manquantes). Charge d'engagement de moyens du SIIM94. Pas obligatoire dans l'absolue mais fortement recommandé. La procédure de tenue du registre est moins prioritaire.	Haute	60 j. (5 j./mois, engagement de moyens, hors procédure de tenue de registre)

8. Durée de conservation et purge. • Réaliser une politique de durée de conservation des données personnels. Cette politique doit notamment contenir une description du processus d'archivage, de purge ou d'anonymisation • Réaliser des référentiels de durées de conservation par direction	C'est au métier de communiquer les durées de rétentions légales quand elles existent : la question sera posée dans le cadre de la mise à jour du registre. Le travail sur la politique de durée de conservation sera réalisé ultérieurement.	Normale	Intégré au point 7 (hors politique de durée de conservation)
9. Contrats et mentions obligatoires. • Réaliser un mode opératoire relatif aux mentions d'information • Réaliser et implémenter le mode opératoire sur la qualification des acteurs contenant des clauses types de protection des données selon la qualification de l'acteur retenue	Sujet incontournable mais l'essentiel du travail semble avoir été fait. La priorité doit être de vérifier différents éléments, dont l'existence de clauses mentionnant le RGPD, dans les contrats fournisseurs concernés (Cf. point 18) : la réalisation d'un mode opératoire sera vu ultérieurement.	Normale	A estimer
10. Protection des données dès la conception **11. Protection des données par défaut** • Réaliser une politique de protection des données dès la conception et par défaut.	Adaptation de la procédure du SIIM94 d'intégration de la SSI et du RGPD dans les projets TIC.	Normale	10 j.
12. Responsabilisation (Accountability) • N/A	En cas de contrôle, le nouveau DPO doit être en capacité de démontrer avec facilité le niveau de conformité de l'EPT.	Haute	Intégré à l'ensemble « Prise en charge de la mission » (5 j.)
13. Analyse d'impact. • Identifier tous les traitements éligibles à l'analyse d'impact (cf. Analyse par traitement) • Réaliser une procédure d'analyse d'impact	Commencer avec une règle simple : tout traitement impliquant des données dites « sensibles » devrait faire l'objet d'une EIVP. La charge dépend de la	Normale	A estimer selon volume et complexité des EIVP

	complexité du traitement : une estimation sera fournie après la révision du registre. Les EIVP pourront faire l'objet d'une priorité pour l'année 2.		
14. Sécurité et gestion des failles. • Réaliser une politique générale de sécurité (PGSSI) en y intégrant la gestion des accès et des mots de passe ainsi qu'un modèle de questionnaire d'évaluation de la sécurité • Mettre en place un SOC et un système de gestion des incidents • Revoir le processus de gestion des violations de données afin de le rendre plus opérationnel et de le simplifier	Le SIIM94 dispose d'une grande expérience en matière de sécurité des SI. L'EPT GOSB pourra aussi s'appuyer sur le parcours de cyber sécurité de l'ANSSI en cours. Remarque : une mutualisation du SOC avec le SIIM94 est envisageable.	Haute	A estimer selon les prestations sollicitées
15. Droits des personnes. • Mettre à jour la procédure relative à l'exercice des droits des personnes afin de la rendre plus opérationnelle et en y intégrant des modèles types de réponses adaptés	RAS	Normale	5 j.
16. Formation et sensibilisation. • Mettre en place un plan de formation annuel • Réaliser des ateliers de sensibilisation • Réaliser et communiquer auprès des agents les fiches pédagogiques sur les sujets abordés lors des ateliers de sensibilisation	Le SIIM94 propose de commencer par un état des lieux sur le sujet de la formation et de la sensibilisation. C'est à l'issue de cet état des lieux qu'un plan de formation et sensibilisation pourra être conçu.	Normale	5 j. (état des lieux)
17. Flux transfrontières. • Réaliser et mettre en place une cartographie des flux • Réaliser et mettre en place une procédure d'encadrement des flux	Concerne a priori peu de flux qui pourront être détecté lors de la mise à jour du registre. La procédure sera faite ultérieurement.	Normale	Intégré au point 7 (hors procédure spécifique)

18. Sous-traitants. • Identifier les cas des prestations réalisées en sous-traitance en se référant à la fiche pédagogique et au mode opératoire sur la qualification des acteurs • Réaliser et mettre en place un mode opératoire sous-traitant contenant une procédure détaillée, les vérifications et contrôles à opérer ; la grille d'évaluation de la conformité du contrat entre le responsable du traitement et le sous-traitant, un modèle de lettre d'accompagnement de l'avenant relatif à la protection des données concernant les contrats en cours d'exécution, un questionnaire de garantie de conformité sous-traitant et un modèle de clause et de contrat types • Vérifier la conformité des contrats de sous-traitance étant conclus	La responsabilité du GOSB est engagée en cas de faute, incident ou non-conformité RGPD chez un de ses sous-traitants. Le SIIM94 propose de donner la priorité à la vérification de la conformité des contrats de sous-traitance conclus. Possibilité d'une démarche en commun avec la DSI de l'EPT pour y associer des éléments spécifiques à la cyber sécurité.	Haute	10 j. (revue des contrats de sous-traitance)
19. Conformité. • Définir des diagnostics des dispositifs en place pour assurer la conformité (contrôle permanent) • Détecter les manquements et proposer un plan de remédiation • Identifier des codes de conduite ou des normes auxquels l'EPT peut adhérer ou pour lesquels elle peut obtenir une certification • Réaliser et mettre en place une politique de contrôle interne permettant de surveiller le maintien de la conformité	En année 1, le DPO sera en grande partie focalisée sur la prise en charge initiale de la mission et les actions et livrables dont la priorité a été positionnée comme « haute » dans ce tableau. Les audits et contrôles seront mis en place ultérieurement, mais le DPO sera au quotidien attentif à tout élément ou situation pouvant affaiblir le niveau de conformité de l'EPT.	Normale	A estimer

A noter que les charges indiquées sont estimatives et ont surtout pour objectif d'apporter une visibilité budgétaire. Dans la mesure du possible, le SIIM94 cherchera à affiner les prévisions de charge au début et/ou en cours de chaque prestation, afin qu'elles puissent faire l'objet de concertations.

3 Aspects financiers

Conformément à la délibération n°2022-01-07 actant l'adoption par le comité syndical du SIIM94 d'une Grille Tarifaire pour les Prestations d'Infogérance, l'EPT GOSB peut solliciter la réalisation de la prestation de mutualisation du DPO par émission de bons de commande adressés au SIIM94. La prestation à référencer est le forfait journaliser « Assistance à maîtrise d'ouvrage SI ». Le SIIM94 propose de procéder à une facturation trimestrielle sur la base d'un relevé d'activité associé au nombre de jours effectivement réalisé.

Bon pour accord :

Michel LEPRÊTRE Président de l'Etablissement Public Territorial Grand Orly Seine Bièvre	Malika KACIMI Présidente du SIIM94 *Dûment habilitée par la délibération du 7 juin 2022*

4 Annexe : missions générales du DPO mutualisé

Au-delà des activités ciblées listées au paragraphe précédent, la description générale des missions du DPO mutualisé est facilitée par la préexistence de lettres de mission identiques au GOSB et au SIIM94 (car basées toutes deux sur le modèle de AFCDP, l'Association Française des Correspondants à la protection des Données à caractère Personnel) :

- Informer et conseiller le responsable de traitement– ainsi que l'ensemble des agents - sur les obligations incombant à la collectivité en vertu du Règlement Général à la Protection des Données (RGPD) et d'autres dispositions en matière de protection de données à caractère personnel ;
- Si besoin, informer le responsable de traitement des manquements constatés, le conseiller dans les mesures à prendre pour y remédier, lui soumettre les arbitrages nécessaires ;
- Veiller à la mise en œuvre de mesures appropriées pour permettre de démontrer que les traitements sont effectués conformément au RGPD, et si besoin, réexaminer et actualiser ces mesures ;
- Veiller à la bonne application du principe de protection des données dès la conception et par défaut dans tous les projets comportant un traitement de données personnelles ;
- Auditer et contrôler, de manière indépendante, le respect du RGPD par la collectivité, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation des agents participant aux opérations de traitement et les audits s'y rapportant ;
- Piloter la production et la mise en œuvre de politiques, de lignes directrices, de procédures et de règles de contrôle pour une protection efficace des données personnelles et de la vie privée des personnes concernées ;
- S'assurer de la bonne gestion des demandes d'exercice de droits, de réclamations et de requêtes formulées par des personnes concernées par les traitements de la collectivité, s'assurer de leur transmission aux services intéressés et apporter à ces derniers votre conseil dans la réponse à fournir aux requérants ;
- Etre l'interlocuteur privilégié de l'Autorité de contrôle (CNIL) et coopérer avec elle ;
- Dispenser des conseils en ce qui concerne les études d'impact sur la vie privée et en assurer la pertinence ;
- Mettre la collectivité en position de notifier d'éventuelles violations de données auprès de l'Autorité de contrôle et porter conseil au responsable de traitement, notamment concernant les éventuelles communications aux personnes concernées et les mesures à apporter ;
- Tenir l'inventaire et documenter les traitements de données à caractère personnel de la collectivité en tenant compte du risque associé à chacun d'entre eux compte tenu de sa nature, sa portée, du contexte et de sa finalité ;
- Présenter un bilan annuel de vos activités au responsable de traitement.

FIN DE DOCUMENT