



La charte d'accès au Système d'information pour les prestataires

Version 1.2.5



Identification du document	
Nom du fichier	CHA_Charte Prestataire_v1.2.odt
Date de création	01/08/2024
Date de mise à jour	01/08/2024
État	☐ Brouillon ☐ À valider ☒ Définitif
Rédaction / Contributeur	Jean-Luc Flotté
Version en cours	1.2.5
Classification	☒ Public ☐ sensible ☐ restreint ☐ confidentiel
Nombre de pages	15

Références	
Nom	Liens
PSSI-E	https://www.ssi.gouv.fr/PSSIE
PGSSI-MEF	https://hfds-bercy.alize.finances.rie.gouv.fr/PGSSI
RGS	https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
cahier des clauses simplifiées de cybersécurité	https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037436658/
RGPD	https://www.cnil.fr/fr/reglement-europeen-protection-donnees

Suivi des versions			
Version	Date	Auteur	Commentaire
0.1	10/01/2024	Jean-Luc Flotté	Création
0.1.2	02/2024	DSMR	Validation DSMR et RSSI
1.0	22/02/2024	DSMR	Mise en forme et publication
1.1	23/07/2024	Jean-Luc Flotté	Intégration des remarques
1.2	01/08/2024	DSMR/RSSI	Reformulations

Sommaire

1	Préambule.....	5
1.1	Objectifs.....	5
1.2	Définitions.....	5
1.3	Portée et effet.....	6
1.3.1	Application globale.....	6
1.3.2	Application par le prestataire.....	6
2	Protection et confidentialité des informations.....	6
2.1	Généralités.....	6
2.2	Cas particulier d'accès aux données sensibles.....	8
2.3	Copies des bases de données.....	8
3	Accès physiques.....	8
3.1	Accès physiques aux locaux.....	8
3.2	Connexion du matériel sur le réseau de l'Insee.....	9
3.2.1	Utilisation du matériel de l'Insee.....	9
3.2.2	Utilisation du matériel du prestataire.....	9
4	Accès logiques.....	10
4.1	Généralités.....	10
4.2	Sécurité des accès logiques.....	10
4.3	Protection contre les logiciels malveillants.....	11
5	Télémaintenance.....	12
5.1	Généralités.....	12
5.2	Connexion depuis l'extérieur.....	12
6	Spécificité dans les interventions.....	13
6.1	Généralités.....	13
6.2	Engagements du prestataire.....	13
6.3	Incidents.....	13
7	Audits, traçabilités et contrôles.....	13
7.1	Généralités.....	13
7.2	Traçabilité des accès.....	14
8	Aspects juridiques.....	14
8.1	Responsabilité.....	14
8.2	Respect des lois en vigueur.....	14
8.3	Intitulé des clauses.....	15
8.4	Invalidité d'une clause.....	15
8.5	Exceptions.....	15
9	Signature du prestataire.....	15

	DSI – Division et Maîtrise des Risques	
	Charte d'accès au Système d'information pour les prestataires	Version /Révision 1.2.5



1 Préambule

1.1 Objectifs

La présente charte s'inscrit dans une démarche d'information, de sensibilisation et de responsabilisation des Prestataires afin de poser les règles d'accès et d'utilisation des Systèmes d'Information (SI) de l'Insee

Elle a pour objet de définir les conditions et modalités que le prestataire s'engage à respecter afin d'assurer la sécurité des SI de l'Insee ainsi que de ses données. L'objectif consiste ainsi à éviter que les relations avec les prestataires ne constituent une faille dans les règles de sécurité informatique définies par le Responsable de la Sécurité des Systèmes d'Information (RSSI).

Cette charte, et les règles qu'elle contient, ont été établies sous l'autorité du Responsable de la Sécurité des Systèmes d'Information, en tenant compte de la Politique de Sécurité du ministère (PGSSI) et des recommandations de l'ANSSI. Elle fait partie du référentiel de sécurité de l'Insee . Elle complète tout marché liant le prestataire à l'Insee. Son respect constitue une obligation essentielle à la charge du prestataire.

1.2 Définitions

- Système d'information (SI)

On entend par Système d'Information (ci-après le « SI ») l'ensemble des ressources, matérielles et logicielles, des moyens techniques, et des procédures et moyens humains et organisationnels, mis en jeu dans la création, le stockage, le traitement, l'archivage, la transmission, la diffusion et la communication des données et informations utilisées dans le fonctionnement de l'institut. Cela inclut entre autres : les logiciels (applications informatiques, systèmes de messagerie électronique, outils bureautiques, systèmes d'exploitation, outils d'administration, utilitaires, bases de données...), les matériels informatiques ou bureautiques (serveurs, ordinateurs et téléphones – fixes ou portables –, imprimantes et photocopieurs, etc.), les équipements des réseaux de données (routeurs, commutateurs, autocommutateurs, fax...), les médias de stockage (disques durs, CD-ROM, clés USB...) et les équipements de production.

- Marché

Contrat de prestations de services, de fournitures de matériels ou de logiciels / progiciels, de travaux, etc., liant contractuellement au sens du Code des Marchés Publics une société de prestataire à l'Insee. La présente charte peut être annexée au marché en plus, le cas échéant, du Cahier des Clauses Simplifiées de Cybersécurité¹. Dans tous les cas, elle est fournie au prestataire avec la commande de la prestation

¹ <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037436658/>

	DSI – Division et Maîtrise des Risques	
	Charte d'accès au Système d'information pour les prestataires	Version /Révision 1.2.5



- Prestataire

Titulaire du marché, ainsi que ses éventuels sous traitants dont il fait son affaire et pour lesquels il s'engage.

- DSI

Direction des Systèmes d'Informations.

- RSSI

Responsable Sécurité des Systèmes d'Information.

1.3 Portée et effet

1.3.1 Application globale

Cette charte s'applique à toute prestation pour lequel le prestataire intervenant doit avoir accès à tout ou partie du Système d'Information de l'Insee. Le prestataire doit la signer (Signature électronique conseillée) avant le début de la prestation et se conformer à ses dispositions.

Elle s'applique à compter de la date de signature de ce document.

1.3.2 Application par le prestataire

Ses dispositions sont applicables dès la notification du marché ou de la commande à laquelle elle est annexée. Elle reste en vigueur pour toute la durée de l'exécution du marché et/ou de la commande.

Comme tout utilisateur du Système d'Information de l'Insee, tout prestataire est soumis à la charte de l'utilisateur du Système d'Information². La présente charte décrit les dispositions spécifiques aux prestataires dans le cadre de la prestation vis-à-vis du Système d'Information de l'Insee.

2 Protection et confidentialité des informations

2.1 Généralités

L'ensemble des informations et des documents fournis par l'Insee, quel que soit leur support, reste la propriété exclusive, pleine et entière de l'Insee. Le prestataire devra en assurer la protection et respecter la non-divulgateion de leur contenu. Il ne pourra en aucun cas procéder à des démonstrations ou toute autre exploitation utilisant ces informations à d'autres fins que celles pour lesquelles elles lui ont été transmises

Quel que soit le support, le prestataire doit considérer par défaut comme confidentiel l'ensemble des informations, documents et toute donnée qu'il reçoit de l'Insee, traite pour le compte de l'Insee, ou crée pour le compte de l'Insee. Plus particulièrement, et sans être exclusif, le prestataire s'engage à ne pas divulguer les

² « charte-utilisation-outils-num 220318 version définitive.pdf » : Cette charte présente sur l'intranet de l'Insee peut être fournie sur demande auprès du RSSI de l'Insee

	DSI – Division et Maîtrise des Risques	
	Charte d'accès au Système d'information pour les prestataires	Version /Révision 1.2.5



informations recueillies sur les faiblesses et les vulnérabilités du Système d'Information de l'Insee, ainsi que toutes les données, qu'elles soient à caractère personnel, confidentielles ou techniques, dont il aura pu avoir connaissance au cours de sa mission.

Le prestataire doit veiller à la sécurité des ressources informatiques qu'il détient en assurant, en interne et vis-à-vis des tiers, la confidentialité, la disponibilité, la traçabilité et l'intégrité des informations. Ces informations sont strictement couvertes par le secret professionnel conformément à l'article 226-13 du Code pénal.

À ce titre, le prestataire prendra vis-à-vis de son personnel toutes les mesures nécessaires pour qu'il respecte le secret et la confidentialité de toutes les informations, documents et données, appartenant à l'Insee. Pour ce faire, le prestataire s'engage à faire signer à chaque membre de son personnel intervenant dans les prestations pour l'Insee, une copie de la présente charte.

Le prestataire reste seul juge des différents moyens à mettre en œuvre pour assurer et garantir la sécurité des informations et des ressources appartenant à l'Insee. Toutefois, il devra informer l'Insee sur la teneur de ces moyens. De même, le prestataire s'engage à respecter les obligations suivantes et à les faire respecter par son personnel :

- n'effectuer aucune copie des documents et des ressources informatiques confiés par l'Insee, à l'exception de celles nécessaires à l'exécution de sa mission, sous réserve d'avoir obtenu préalablement et par écrit l'accord exprès de l'Insee (chef de division ou équivalent propriétaire des données) ;
- prendre toutes les mesures de sécurité, notamment matérielles, pour assurer la conservation, l'intégrité, la traçabilité et la confidentialité des documents et des informations traités pendant l'exécution des prestations quel que soit le support utilisé ;
- en fin d'exécution du marché ou de la commande, et ce pour quelque cause que ce soit, procéder à la restitution immédiate de tous les documents, les données et les ressources informatiques appartenant à l'Insee. À défaut, le prestataire devra procéder à la destruction sécurisée de chacun des supports et de chacune des informations non restitués ; à ce titre, l'Insee pourra demander que la destruction des données s'effectue en sa présence ou demander des preuves matérielles de cette destruction de données. Ces destructions feront dans tous les cas d'un procès verbal de destruction signé.

Le prestataire s'engage à n'exécuter aucun autre traitement que ceux prévus contractuellement sur les informations et les données fournies ou leurs résultats. Le traitement doit être proportionné et conforme à la finalité prévue, à la présente charte et les règles générales relatives à la sécurité du Système d'Information de l'Insee.

	DSI – Division et Maîtrise des Risques		
	Charte d'accès au Système d'information pour les prestataires	Version /Révision 1.2.5	

2.2 Cas particulier d'accès aux données sensibles³

Au cas où le prestataire serait en position d'accéder à des données sensibles de quelque nature que ce soit dont particulièrement celles relevant du secret statistique⁴ ou du RGPD⁵, il est rappelé que les dispositions juridiques en vigueur s'imposent pour l'accès à ces données et l'Insee demande au prestataire de mettre en place tous les moyens à sa disposition afin de respecter les dispositions réglementaires en vigueur.

En particulier, le prestataire devra porter un soin particulier à l'accès à ces données sensibles lors de l'exécution des actions techniques. Le prestataire devra prendre toutes les dispositions nécessaires pour qu'en aucun cas ces données ne sortent de l'Insee ou soient altérées.

2.3 Copies des bases de données

Qu'il s'agisse de maintenance technique ou autre, toute copie de données est soumise à la stricte autorisation du propriétaire de la donnée (chef de département ou d'unité) et du RSSI (RSSI ou tout membre de la DSMR⁶). Cette copie devra exclusivement se faire au sein de l'Union européenne. Un engagement écrit devra être fourni par le prestataire et validé par l'Insee.

Un prestataire qui copierait ces données sans autorisation formelle s'exposerait à des poursuites immédiates.

3 Accès physiques

L'accès à un bâtiment de l'Insee, que ce soit à la Direction Générale ou en Direction Régionale est régi par un règlement intérieur qui doit être suivi lors de la prestation.

3.1 Accès physiques aux locaux

L'accès aux locaux se fait à l'aide de badges d'identification et sous la stricte responsabilité d'un agent de l'Insee⁷.

Les salles où le prestataire est hébergé, ainsi que les moyens d'accès physiques, lui sont communiqués par l'Insee. Le prestataire s'engage à suivre les règles suivantes :

- n'accéder qu'aux locaux pour lesquels il est habilité ou avec d'autres moyens que ceux mis à sa disposition ;
- ne pas permettre l'accès aux personnes non autorisées dans les locaux de l'Insee ;

³ Les systèmes d'information sensibles sont ceux qui traitent d'informations dont la divulgation à des personnes non autorisées, l'altération ou l'indisponibilité sont de nature à porter atteinte à la réalisation des objectifs des entités qui les mettent en œuvre. (Instruction Interministérielle Relative à la Protection des Systèmes d'Informations Sensibles n° 901/SGDSN/ANSSI NOR : PRMD1503279J)

⁴ Le secret statistique, crée une obligation spéciale dans le cas de données confidentielles collectées, détenues ou produites pour des usages statistiques. Il interdit strictement la communication de données individuelles ou susceptibles d'identifier les personnes, issues de traitements à finalités statistiques, que ces traitements proviennent d'enquêtes ou de bases de données. (<https://www.insee.fr/fr/information/1300624>)

⁵ Règlement Général sur la Protection des Données

⁶ Division Sécurité et Maîtrise des Risques

⁷ Le prestataire devra être en mesure de prouver son identité.

	DSI – Division et Maîtrise des Risques	
	Charte d'accès au Système d'information pour les prestataires	Version /Révision 1.2.5



- respecter les systèmes de sécurité physique mis en place. En particulier, s'il se trouve être seul dans le local, le fermer systématiquement à clé et ceci même en cas d'absence de courte durée ;
- assurer la protection physique du matériel mis à sa disposition ;
- restituer tous les objets permettant l'accès physique aux infrastructures et prêtés durant la prestation (cartes, clés, etc.) à la fin de l'intervention ;
- ne réaliser aucune copie ou duplicata des moyens d'accès mis à disposition ;
- ne pas entraver le fonctionnement des équipements opérationnels et ceux de sécurité.

Dans le cas des opérations de maintenance (par exemple, réparation matérielle), le prestataire doit transmettre au préalable un descriptif précisant les dates, la nature des opérations à effectuer et les noms des intervenants.

3.2 Connexion du matériel sur le réseau de l'Insee

Cette connexion au réseau se doit de respecter les bonnes pratiques en matière de sécurité. Notamment, cette connexion impose le respect des conditions suivantes :

- respect :
 - ▶ de la charte ministérielle d'utilisation des outils numériques⁸ ;
 - ▶ de la charte de sécurité de l'utilisateur INSEE⁹.
- respect des différents Politiques d'Exploitation de Sécurité (PES Mots de passe V1.1 notamment). Ces PES seront mises à disposition auprès de la DSMR.

3.2.1 Utilisation du matériel de l'Insee

Dans la majorité des cas, l'utilisation de matériels informatiques fournis par l'Insee s'impose. Dans ce cas, quelques règles doivent être respectées :

- le prêt du matériel est demandé par un agent de l'Insee ;
- le prêt est soumis à la signature d'un document¹⁰ engageant le prestataire intervenant ;
- le matériel ne doit pas sortir du territoire national.

3.2.2 Utilisation du matériel du prestataire

Dans le cas où le prestataire aurait besoin, pour l'exécution de sa prestation, de connecter des matériels informatiques lui appartenant sur le réseau de l'Insee, cette connexion est possible aux conditions suivantes :

- intégration du matériel au domaine « Active Directory » sauf dans le cas très particulier des Audits de sécurité de systèmes d'information ;
- socle technique et applicatif à jour ;

⁸ Charte ministérielle d'utilisation des outils numériques : https://intranet.insee.fr/jcms/1422191_DBFileDocument/fr/charte-utilisation-outils-num-220318-version-definitive

⁹ https://intranet.insee.fr/jcms/24856861_DBFileDocument/fr/charte-de-securite-utilisateur-insee

¹⁰ Document_engagements_de_l'utilisateur_et_de_son_entreprise_A_FAIRE_SIGNER_V3-1.pdf

	DSI – Division et Maîtrise des Risques		
	Charte d'accès au Système d'information pour les prestataires	Version /Révision	
		1.2.5	

- présence d'un antivirus à jour et à même de récupérer au moins 1 fois toutes les 24 h les dernières signatures antivirales ;
- le prestataire devra démontrer que son matériel ne présente aucun risque de compromission ou d'infection du réseau informatique de l'Insee ;
- cette connexion ne doit en aucune manière avoir un impact sur les performances, la disponibilité, l'intégrité et la confidentialité du Système d'Information de l'Insee ;
- le matériel doit se connecter au réseau par les prises habituelles. Notamment, les connexions à l'aide Hub sont interdites.

Le prestataire s'engage à ne connecter aucun matériel informatique sans l'accord explicite et écrit de la DSI (chef de division ou PO¹¹ en charge de la prestation).

4 Accès logiques

4.1 Généralités

Sauf dans le cas exclusif et particulier d'un audit exécuté par des agents de l'ANSSI¹² ou par les auditeurs du SHFDS¹³, tout accès logique au Système d'Information de l'Insee nécessite au préalable :

- L'attribution par la DSI d'un compte utilisateur Active Directory nominatif, actif pour le temps exclusif de la prestation et / ou de la connexion au moyen d'une demande effectuée par le personnel de l'Insee chargé du suivi de la prestation ;
- attribution éventuelle de moyens d'authentification forte de type carte à puce, de façon nominative et pour le temps exclusif de la prestation.

4.2 Sécurité des accès logiques

Les comptes utilisateurs fournis doivent être nominatifs et individuels.

Aussi, il appartient au prestataire de s'assurer de la bonne utilisation de ces comptes et en particulier :

- garantir que ces codes d'accès ne sont accessibles qu'aux personnels autorisés ;
- s'assurer de la mise à jour régulière des personnels autorisés, notamment suite à des départs éventuels de personnels chez le prestataire – les accès adéquats devront être révoqués en cas de cessation du besoin et / ou de départ du personnel concerné ;
- traiter ces informations de connexion comme des informations hautement confidentielles, engagement pour lequel le prestataire est soumis à une obligation de résultats ;
- assurer de façon générale la protection contre tout accès non autorisé par tous les moyens adéquats (protection périmétrique, protection physique, etc.) - le prestataire est soumis à une obligation de résultat sur ce point.

¹¹ Product Owner

¹² Agence Nationale de la sécurité des systèmes d'information

¹³ Service du Haut fonctionnaire de défense et de sécurité

	DSI – Division et Maîtrise des Risques		
	Charte d'accès au Système d'information pour les prestataires	Version /Révision 1.2.5	

Le prestataire s'engage à :

- faire respecter la protection, la non-divulcation et le non-partage du mot de passe des intervenants qui doivent en assurer une utilisation strictement personnelle. Le mot de passe est inaccessible et doit être suffisamment robuste ;
- communiquer à l'Insee, dès l'ouverture des autorisations d'accès au système et en cas de changement, le nom des intervenants et l'identification utilisateur associés ;
- ne pas user de leur droit pour accéder à des applications, à des données ou à un compte informatique autres que ceux qui leur auront été éventuellement attribués ou pour lesquels ils ont reçu l'autorisation d'accès ;
- ne pas user, par quelque moyen que ce soit, du droit d'accès d'un autre utilisateur ;
- ne pas altérer ou détruire des traces ou preuves relatives à des actions ou des événements sur les Systèmes d'Information, le concernant ou non ;
- ne pas entraver le fonctionnement des équipements opérationnels et ceux de sécurité et dans tous les cas ne pas porter atteinte à la production informatique.

Le prestataire devra avertir le personnel de l'Insee responsable du suivi de la prestation de tous dysfonctionnements constatés et/ou de toutes anomalies générées de son fait ou ne le concernant pas mais relevant de la sécurité, qu'il aura pu observer lors de l'exécution de ses prestations. À cet égard, la procédure d'alerte consiste à prévenir par tout moyen et dans les plus brefs délais la DSMR ou le RSSI, qui s'attachera à faire isoler le dysfonctionnement.

4.3 Protection contre les logiciels malveillants

Ce paragraphe fait référence aux virus, spyware, etc., c'est-à-dire à tout malware ou logiciel malveillant.

Toutes les solutions, qu'elles soient logiques ou physiques, doivent s'intégrer dans la stratégie antivirale de l'Insee. Étant noté que l'utilisation d'un quelconque outil ou matériel sur le réseau de l'Insee est interdite, sauf accord préalable de la DSI et/ou du RSSI, dans les cas rares où des machines du prestataire devraient être introduites sur le réseau, le prestataire devra amener la preuve de l'innocuité en termes de sécurité desdites machines. Ainsi, elles devront avoir une protection antivirale à jour de façon à éviter toute contamination du SI de l'Insee. En tout état de cause, l'Insee se réserve le droit de faire vérifier les machines par sa propre suite antivirale.

De même, tous les supports d'informations devront avoir été balayés, en présence d'un agent de la DSI, par l'antivirus de l'Insee, chaque fois qu'ils doivent être utilisés sur les matériels de l'institut. Le prestataire s'engage à procéder de même pour l'utilisation de tels supports sur son propre matériel.

Lorsque le prestataire intervient sur site, l'Insee se réserve le droit d'installer eux-mêmes un antivirus sur les machines utilisées par le prestataire dans le cadre de sa prestation afin d'effectuer le scan de chaque poste et des supports d'information du prestataire.

	DSI – Division et Maîtrise des Risques	
	Charte d'accès au Système d'information pour les prestataires	Version /Révision 1.2.5



5 Télémaintenance

5.1 Généralités

La télémaintenance est nécessaire au bon maintien en condition opérationnelle et de sécurité de beaucoup d'équipements utilisés par le SI de l'Insee.

Elle se divise en 2 cas d'utilisation :

- cas 1 : le prestataire se connecte, depuis l'extérieur de l'Insee, à une solution dédiée à cette fonction - il s'agit de télémaintenance à proprement parler ;
- cas 2 : le prestataire a positionné sur le réseau du SI de l'Insee un équipement qui envoie des informations techniques (logs, traces, alertes, etc.) à un équipement du prestataire situé en dehors du réseau — ce cas d'usage s'apparente à de la supervision ;

5.2 Connexion depuis l'extérieur

Dans le cadre de la télémaintenance, l'accès direct au SI de l'Insee n'est pas autorisé. Tout accès au système d'information de l'Insee depuis l'extérieur devra donc se faire par une plateforme de télémaintenance sécurisée. Cette solution proposera, sur invitation d'un agent de l'Insee dûment habilité, un déport de l'affichage, du clavier et/ou de la souris. De plus :

- aucun accès en télémaintenance n'est ouvert en permanence ;
- pendant toute la durée de l'intervention, les actions du prestataire sont sous la surveillance de l'agent de l'Insee ;
- tout accès en télémaintenance sur un équipement production doit passer par une invitation : c'est la solution qui fait cette invitation par un envoi de mail au prestataire : les adresses mail devront être connues et listées dans l'annexe adossé à cette charte dès le début de la relation contractuelle avec le prestataire ;
- l'ouverture d'un accès en télémaintenance doit avoir une durée limitée à la durée de l'intervention ;
- il est nécessaire de tracer nominativement les personnes des sociétés extérieures qui accèdent en télémaintenance ; les comptes nominatifs sont un moyen idéal ;
- Pour des raisons de confidentialité, l'accès en télémaintenance par le prestataire à un serveur de production contenant des données réelles doit être une exception. L'accès en télémaintenance à un serveur de tests ou de pré-production doit être privilégié, afin de réaliser les opérations techniques qui seront ensuite répercutées sur l'environnement de production ;
- L'accès en télémaintenance à un serveur de production ne se justifie que dans un cas d'urgence, avec approbation écrite de la DSI (chef de division ou PO en charge de la prestation) et sous contrôle de celle-ci (agent de la DSI qui travaille en direct avec le prestataire)

Tout manquement à ces règles engage la responsabilité du prestataire. En ce qui concerne l'accès par le prestataire aux postes de travail des agents de l'Insee :

	DSI – Division et Maîtrise des Risques	
	Charte d'accès au Système d'information pour les prestataires	Version /Révision 1.2.5



- en aucun cas cet accès ne constitue un droit de visualiser des données confidentielles (données statistiques par exemple) - à ce titre le prestataire devra limiter son intervention aux strictes opérations nécessaires pour assurer sa mission et sous la surveillance d'un agent de l'Insee ;
- tout manquement aux règles de confidentialité et de déontologie engage la responsabilité du prestataire ;
- tous les accès sont tracés.

6 Spécificité dans les interventions

6.1 Généralités

Toute intervention sur le SI de l'Insee que ce soit à distance ou sur site, présente des risques inhérents de perturbation dans le fonctionnement des applications.

6.2 Engagements du prestataire

La récupération des flux et autres actions visant à tester la robustesse des Systèmes d'Information sont interdites (excepté en cas de demande préalable et explicite de l'Insee : audit, tests d'intrusion, tests de montée de charge, validation de performance, etc.).

Par ailleurs, le prestataire s'engage à ne pas se servir du réseau de l'Insee pour tout autre raison que celle pour laquelle il a un engagement, comme présenter une solution ou procéder à de l'avant-vente. Pour de telles démonstrations, il devra mettre en place sa propre architecture. En particulier, il est strictement interdit au prestataire d'utiliser le réseau de l'Insee afin de procéder à une démonstration (par exemple de la nouvelle version d'un progiciel déjà détenu par l'Insee, ceci n'étant qu'un exemple) directement dans un service utilisateur et sans passer par le point de contact unique qui est la DSI (chef de division ou PO en charge de la prestation), qui devra avoir explicitement et par écrit autorisé une telle utilisation.

6.3 Incidents

Le prestataire s'engage à informer immédiatement le personnel de l'Insee en responsabilité de la prestation et/ou le RSSI de tout événement pouvant affecter la disponibilité, l'intégrité, la traçabilité, la confidentialité ou la perte d'informations de l'Insee qu'il détient, auxquelles il accède ou qu'il manipule.

7 Audits, traçabilités et contrôles

7.1 Généralités

Tout accès au SI de l'Insee est tracé, conformément aux lois informatiques et Liberté. Les traces sont conservées jusqu'à 1 an en fonction de leur typologie.

	DSI – Division et Maîtrise des Risques	
	Charte d'accès au Système d'information pour les prestataires	Version /Révision 1.2.5



7.2 Traçabilité des accès

Il appartient au prestataire, dans le cas de l'attribution d'un compte de service (c'est-à-dire affecté au prestataire et non pas nominativement à un ou plusieurs employés) de gérer la traçabilité des accès. Ce cas de figure se doit de rester très exceptionnel.

L'Insee doit, sur simple demande, pouvoir disposer de l'historique nominatif de l'utilisation de ce type accès, s'entend quel employé du prestataire a utilisé cet accès, à quelles dates et heures, pour quelle durée et pour quelle action.

8 Aspects juridiques

8.1 Responsabilité

Le prestataire est responsable de tous les dommages corporels, matériels et immatériels, directs ou indirects, trouvant leur origine aussi bien dans une exécution fautive, même partielle ou une mauvaise exécution ou une inexécution des obligations mises à sa charge dans la présente charte.

Le prestataire est seul responsable du respect des présents engagements et de leur mise en œuvre ainsi que de leur respect par son personnel.

Nonobstant sa responsabilité contractuelle, le prestataire est informé que, selon la faute commise, des sanctions civiles (par exemple pour atteinte au droit à l'image d'un tiers) et/ou pénales (par exemple pour intrusion frauduleuse dans les SI ou pour violation du secret professionnel) pourront être prononcées par les juges.

8.2 Respect des lois en vigueur

Le prestataire s'engage non seulement au respect de la présente charte, mais déclare également connaître et respecter la réglementation en vigueur et notamment à titre non limitatif :

- la loi 78-17 du 6 janvier 1978 modifiée par la loi du 4 août 2004¹⁴ relative à l'informatique, aux fichiers et aux libertés et ses textes d'application ;
- les dispositions du Code pénal relatives à la fraude informatique (articles 323-1 à 323-7 du Code pénal)¹⁵ ; – les dispositions du Code civil relatives aux atteintes aux droits de la personne (notamment atteintes à l'intimité de la vie privée et au droit à l'image) ;
- les dispositions du Code pénal relatives aux atteintes aux droits de la personne (notamment, atteintes à la vie privée, au secret des correspondances privées, atteintes au secret professionnel et atteintes résultant de fichiers ou de traitements informatiques) ;

¹⁴ <https://www.legifrance.gouv.fr/loda/id/LEGISCTA0000023784585>

¹⁵ https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA0000006136043/#LEGISCTA0000006136043

	DSI – Division et Maîtrise des Risques	
	Charte d'accès au Système d'information pour les prestataires	Version /Révision 1.2.5



- les dispositions du Code de la propriété intellectuelle relative au droit d'auteur (les logiciels, toutes les œuvres de l'esprit quelle que soit leur nature, les bases de données)¹⁶, aux brevets, aux marques et aux dessins et modèles.

8.3 Intitulé des clauses

Les intitulés portés en tête de chaque article ne servent qu'à la commodité de la lecture et ne peuvent en aucun cas être le prétexte d'une quelconque interprétation ou dénaturation des clauses sur lesquelles ils portent.

8.4 Invalidité d'une clause

Si une ou plusieurs stipulations de la présente charte sont tenues pour non valides ou déclarées telles en application d'une loi, d'un règlement ou à la suite d'une décision définitive d'une juridiction compétente, les autres stipulations conserveront leur pleine validité sauf si elles présentent un caractère indissociable avec la stipulation non valide.

8.5 Exceptions

Chaque cas d'exception appelant une dérogation à la présente charte devra systématiquement être soumis à la DSI et au RSSI (ou tout membre de la DSMR) pour identification, validation et suivi.

9 Signature du prestataire

La société :

déclare accepter sans réserve les conditions du présent document.

Fait à :

Le :

Signature (de préférence électronique) :

¹⁶ https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006069414/2022-06-07/