EDICIA

Editeur spécialiste de la sécurité urbaine

SOLUTIONS LOGICIELLES EDICIA

DOSSIER RGPD

Table des matières

Glossaire 3
Introduction 7
Mesures existantes ou prévues, pour la protection des données 8
Mesures contribuant à traiter des risques liés à la sécurité des données 8
Mesures générales de sécurité 16
Mesures organisationnelles (gouvernance) 28
Cartographie des risques & Réponses aux questions les plus courantes dans le cadre de l'anticipation des risques en conformité avec la RGPD 33

Glossaire

Accountability	Désigne l'obligation imposée par le GDPR/RGPD aux entreprises, de mettre en œuvre des mécanismes, des documents et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.
Analyse d'impact relative à la protection des données (PIA)	Elle vise à évaluer tous les processus et toutes les bases de données d'un département donné (finalités, durée de conservation des données, droits des personnes…) et à analyser les risques sur la sécurité des données (accès aux données, fraudes…) et leurs impacts potentiels sur la vie privée, afin de déterminer les mesures techniques et d'organisation pour protéger les données.
Anonymisation	Traitement permettant de rendre les données personnelles anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable.
Cartographie des données	Dans un premier temps, l'entreprise doit cartographier les processus de collecte des données à caractère personnel, concernant les employés comme les clients ou les candidats à l'embauche. Elle doit ensuite identifier les traitements qui leur sont associés et, leurs lieux et formats de stockage et consigner le tout dans un registre dédié.
Chiffrement	Opération qui consiste à transformer un message à transmettre, dit « message clair », en un autre message, inintelligible pour un tiers, dit « message chiffré », en vue d'assurer le secret de sa transmission.
CNIL (Commission Nationale de l'Informatique et des Libertés)	Autorité de contrôle chargée de veiller à la bonne application de la règlementation sur les données personnelles.
Confidentialité des données	Selon l'Organisation mondiale de normalisation (ISO), la confidentialité des données consiste à s'assurer que les données ne sont accessibles qu'aux personnes autorisées, et donc à protéger les communications ou des données stockées contre l'interception et la lecture par des personnes non autorisées.
Consentement explicite	Tout individu doit donner son consentement explicite, c'est à dire via une déclaration claire écrite ou orale qui ne permet aucune mauvaise interprétation. Cette déclaration doit préciser la nature des données collectées, le type de traitement et ses impacts potentiels, le caractère obligatoire

	ou facultatif des réponses, ainsi que le détail des données à transférer et les risques liés à ce transfert.
Déclaration CNIL	Procédure administrative effectuée auprès de la CNIL et autorisant les traitements de données personnelles au sein d'un organisme. Cette procédure est supprimée avec l'application du GDPR/RGPD et est remplacée par un processus dit de « registre ».
Données à caractère personnel / Données personnelles	Toute information identifiant directement ou indirectement une personne physique (ex : nom, prénom, n° d'immatriculation, n° de téléphone, date de naissance, commune de résidence, empreinte digitale…). Une donnée qui ne permet pas d'identifier directement une personne peut devenir une donnée personnelle si elle est croisée avec une autre donnée. Ce croisement permettant d'identifier une personne, (ex: une description physique croisée avec un poste dans une entreprise) peut permettre d'identifier une personne précise.
Données sensibles	Information relative à l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.
Délégué à la Protection des Données (DPD) ou DPO (Data Protection Officer)	Le DPO est le garant du respect de la réglementation au sein de l'entreprise. Parmi ses missions, il doit informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés ; contrôler le respect du règlement, d'autres dispositions en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant ; dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci ; coopérer avec l'autorité de contrôle (CNIL) sur les questions relatives au traitement.
Droit d'accès	Droit des personnes d'obtenir du responsable du traitement : La confirmation que les données à caractère personnel sont ou ne sont pas traitées Lorsqu'elles sont traitées, l'accès auxdites données à caractère personnel L'accès aux informations sur les traitements effectués sur ses données personnelles.
Droit à la limitation des traitements	Droit de limiter le traitement qu'une entité peut faire des données personnelles si le traitement n'est plus justifié.

Droit à l'oubli/ Droit à l'effacement	Droit d'obtenir du responsable du traitement l'effacement de ses données à caractère personnel.
Droit d'opposition	Droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel.
Droit à la portabilité	Droit de recevoir du responsable de traitement dans un format structuré, couramment utilisé et lisible par machine, ses données à caractère personnel et de les transmettre à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées en premier lieu y fasse obstacle.
Droit à la rectification	Droit d'obtenir du responsable du traitement la rectification de ses données à caractère personnel si inexactes.
Habilitation	Capacité légale à accomplir certaines opérations ou à exercer certains pouvoirs. Dans le cadre du RGPD, il s'agit de donner l'accès aux seules données nécessaires à l'accomplissement de leurs missions, après avoir identifié les responsabilités des utilisateurs.
Finalité	Objectif principal d'une application informatique de données personnelles. Ex : gestion des recrutements, gestion des clients, enquête de satisfaction, surveillance des locaux, etc.
Fichier	Traitement de données qui s'organise dans un ensemble stable et structuré de données. Les données d'un fichier sont accessibles selon des critères déterminés.
Loi informatique et libertés	Loi principale française datant du 6 janvier 1978 sur la protection des données personnelles.
Principe de licéité	Les données personnelles ne peuvent être collectées et exploitées que pour un usage donné et légitime, correspondant aux missions du responsable de traitement.
Privacy by design	L'entreprise doit s'assurer de la protection des données dès la conception des produits et services, et tout au long de leur cycle de vie.
Privacy Shield	Auto-certification UE-US sur la protection des données personnelles permettant le transfert de données personnelles issues des personnes localisées sur le territoire de l'UE vers les entreprises certifiées « Privacy Shield ».
Pseudonymisation	Traitement de données personnelles de telle façon que celles-ci ne puissent plus être attribuées à une personne précise sans avoir recours à des informations supplémentaires.
Registre interne des traitements de données à	Le RGPD contraint toute entreprise à consigner dans un registre l'ensemble des traitements de données à caractère

caractère personnel	personnel qu'elle met en œuvre. Les informations suivantes doivent être consignées : le nom et les coordonnées des responsables de traitements, co-responsables de traitements, sous-traitants et destinataires intervenant dans le traitement ; les finalités du traitement ; les catégories de personnes concernées et les catégories de données à caractère personnel ; les transferts de données à caractère personnel hors UE ; une description générale des mesures de sécurité techniques et organisationnelles ; dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données.
Responsable de traitement (Data Controller)	La personne physique ou morale, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens du traitement. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.
RGPD (Règlement Général sur la Protection des données)	Nouveau texte européen sur la protection des données personnelles applicable à compter du 25 mai 2018 et remplaçant et uniformisant l'ensemble des règles applicables dans les états membres de l'Union Européenne sur la protection des données personnelles.
Sous-traitant	La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.
Traitement de données à caractère personnel	Toute opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (Ex : accès, collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, …).
Transfert de données	Toute communication, copie, ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne. Un simple accès à des données stockées en France à partir d'un terminal situé en Chine est donc un transfert. Les transferts sont interdits en dehors du territoire de l'UE sauf exception.
Violation de données	Violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Introduction

Le Règlement Général relatif à la Protection des Données (RGPD) est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union Européenne.

Applicable depuis le 25 mai 2018 à l'ensemble de l'Union européenne, le RGPD renforce les droits des résidents européens sur leurs données et responsabilise l'ensemble des acteurs traitant ces données (responsables de traitement et sous-traitants).

Un éditeur de logiciels est avant tout une entreprise. À ce titre, EDICIA est responsable des traitements sur les données de l'entreprise, et doit respecter un certain nombre de points dans différents domaines (RH, marketing…) afin de respecter le RGPD et de garantir la protection des données relatives à ses clients (contrats, contacts, etc).

Un éditeur de logiciels est également un fournisseur de produits et de services. Dans le cadre des solutions SaaS, EDICIA est également considéré comme sous-traitant de ses clients parle RGPD, et doit donc répondre à ce titre aux obligations associées.

Enfin, en qualité d'éditeur de logiciels, EDICIA n'est pas propriétaire des données et n'est pas non plus considéré comme responsables de traitement. Seuls les utilisateurs le sont par principe. Dans son rôle de conseil et d'assistance, EDICIA s'attache cependant à permettre à ses clients de répondre à leurs obligations conformément aux exigences du RGPD, en leur fournissant les outils logiciels appropriés.

Dans le cadre de la relation de confiance établie avec ses clients, EDICIA met à leur disposition un dossier complet qui détaille les moyens et process par lesquels EDICIA met en application le respect du droit de la protection des données.

Mesures existantes ou prévues, pour la protection des données

Mesures contribuant à traiter des risques liés à la sécurité des données

Chiffrement Moyens mis en œuvre pour assurer la confidentialité des données conservées.	Le chiffrement est une transformation réversible des données, les rendant illisibles par application d'une fonction de chiffrement. Cette fonction peut être inversée uniquement grâce à la clé de chiffrement, détenue par l'entreprise ou par la personne concernée. Cela permet de réduire fortement l'impact d'une fuite de données. Le chiffrement n'est pas obligatoire, mais est considéré comme une technique efficace de sécurisation des données. Le chiffrement est proposé en standard dans les technologies de transfert de données utilisées par nos services.
Anonymisation Mécanismes d'anonymisation mis en œuvre et garanties contre une ré identification éventuelle	Des données à caractère personnel sont des données concernant une personne physique identifiable. Des données sont considérées comme anonymes lorsque la personne concernée n'est plus identifiable, de manière irréversible et par quelque moyen que ce soit, c'est-à-dire qu'aucune donnée ou ensemble de données ne permet de remonter à son identité. Ce ne sont alors plus des données à caractère personnel. Le RGPD précise que toute donnée anonyme, c'est-à-dire dont la personne n'est plus identifiable, n'est pas soumise au règlement. L'anonymisation, irréversible, permet de soustraire des données au périmètre du RGPD, généralement pour des usages de test applicatif ou d'analyse statistique : elle doit pour cela conserver le sens métier et la distribution des données. EDICIA propose une fonction d'anonymisation des données dans son module de gestion des archives. Cette fonction permet de remplacer les valeurs des champs contenant des données dites « personnelles » par une valeur issue d'une fonction de hachage. Elle ne s'applique que sur les données archivées. Le module de gestion des archives est proposé en option.

Cloisonnement des données Mécanismes de cloisonnement du traitement (par rapport au reste du système d'information)	L'objectif du cloisonnement des données est de réduire la possibilité de corréler des données à caractère personnel qui pourrait aboutir à une violation de la protection des données personnelles. **Au niveau des machines de stockage des données :** Les machines virtuelles qui hébergent l'application, les moteurs applicatifs et la base de données sont dédiées par client (une machine virtuelle par client). Cette organisation garantit le cloisonnement des données pour une machine virtuelle (VM). **Au niveau des applicatifs :** Nos solutions logicielles permettent également un cloisonnement des données au niveau applicatif : - les utilisateurs accèdent aux seules données dont ils ont besoin - l'application gère des droits d'accès différenciés selon les processus métiers (gestion des plannings, gestion des mains courantes, gestion de l'armement, …)
Contrôle des accès logiques Définition et attribution des profils utilisateurs	Le système de gestion des droits de l'application SMART POLICE fonctionne est basé sur une gestion de profils. A chaque profil est associé un ensemble de droit (consultation, modification, …) pour chaque module ou ensemble de donnée et pour chaque action de l'application. Le dispositif permet de gérer très finement les droits en créant les profils nécessaires. L'application propose une interface (IHM) spécifique de gestion des profils d'utilisation du logiciel : le module Habilitations. L'utilisation de ce module est soumise à des droits d'utilisation. La plateforme SMART POLICE permet de créer un nombre infini de profils différents. Elle permet de personnaliser à loisir la notion de profil/habilitation en combinant les différents droits (saisie, édition, modification…) avec l'accessibilité ou non aux différents modules. Lors de la mise en place de l'application, l'administrateur doit définir les différents profils d'utilisation qui lui seront nécessaires. Par défaut, l'application est livrée avec plusieurs profils prédéfinis. La création d'un profil d'utilisation/habilitation est très simple, ce qui permet à l'administrateur de l'application d'être rapidement autonome sur la création et l'administration des habilitations. Une fois le profil/habilitation créée, l'administrateur peut l'attribuer à un ou plusieurs utilisateurs.

Authentification Moyens d'authentification mis en œuvre	**Identification de l'utilisateur** L'utilisation du logiciel est soumise à authentification. Lors de la mise en place de l'application, l'administrateur attribue aux personnels habilités un identifiant et un mot de passe initial personnels. Pour garantir la confidentialité du mot de passe, le champ de saisie du mot de passe affiche un nombre aléatoire de caractères. A la première connexion avec ce mot de passe (initial ou temporaire), l'application demande à l'utilisateur de personnaliser son mot de passe. Ainsi, il est le seul à connaître le mot de passe. L'utilisateur peut à tout moment renouveler son mot de passe : il dispose d'un menu Mon compte qui lui permet de créer un nouveau mot de passe personnel. **Connexion / Déconnexion** Au lancement, le logiciel affiche la fenêtre de connexion. L'utilisateur doit saisir son code utilisateur (identifiant) et son mot de passe afin de pouvoir accéder aux fonctionnalités du logiciel. Quand un utilisateur se connecte à l'application, il est instantanément « reconnu » : les droits d'utilisation liés à son profil de référence sont activés, et l'application historise les actions qu'il réalise dans le logiciel (modification, création, etc.). La confidentialité du mot de passe individuel est essentielle pour assurer la sécurité et la confidentialité des données, mais aussi la traçabilité des actions (qui a fait quoi quand).
Mot de passe Règles applicables aux mots de passe	**Niveau de complexité** Par paramétrage, l'administrateur de l'application peut définir le niveau de complexité attendu pour les mots de passe : • Longueur minimale attendue, • Présence de caractères majuscules et minuscules, • Présence de caractères spéciaux et d'au moins un chiffre, • Interdiction d'utiliser un mot de passe déjà utilisé par le passé (deux dernières occurrences). Toute création de nouveau mot de passe doit respecter les exigences définies par l'administrateur. Si une exigence n'est pas respectée, un message avertit l'utilisateur de la non-conformité du mot de passe. **Durée de validité** Dans les paramétrages, l'administrateur de l'application peut définir • une durée de validité V des mots de passe, définie en jours ;

	• un délai D pour avertir l'utilisateur de l'expiration prochaine de son mot de passe, défini en jours. D jours avant la date d'expiration du mot de passe, l'application affiche un message pour avertir l'utilisateur que son mot de passe arrive à échéance, et qu'il doit le renouveler dans les D jours.
Traçabilité (journalisation) Journalisation des évènements et durée de conservation des traces	La journalisation a pour but de détecter les incidents concernant des données à caractère personnel de façon précoce, et de disposer d'éléments exploitables pour les étudier ou pour fournir des preuves dans le cadre d'enquêtes. **Journalisation au niveau des serveurs** EDICIA a conçu ses applications logicielles en incluant une architecture de journalisation permettant de conserver une trace des événements de sécurité et du moment où ils ont eu lieu. Les événements journalisés sont sélectionnés en fonction du contexte, des supports, des risques et du cadre légal. Si les événements journalisés comprennent des données à caractère personnel, l'opération est menée dans le respect des exigences de la loi informatique et libertés. Les événements sont horodatés en prenant comme référence le temps UTC (Coordinated Universal Time). Les journaux utilisent une source de temps fiable sur laquelle les équipements se synchronisent (serveur NTP Network Time Protocol). La capacité de stockage des journaux est adaptée et permet de conserver les journaux sur un délai de 30 jours. Les équipements de journalisation et les informations journalisées sont protégés contre le sabotage et les accès non autorisés. **Journalisation au niveau de l'application SMART POLICE** L'application SMART POLICE intègre une fonction d'historisation des actions des utilisateurs permettant une traçabilité des manipulations réalisées par les utilisateurs. Toutes les modifications de données sont historisées avec l'horodatage, l'utilisateur, l'ancienne et la nouvelle valeur. Il est possible de retrouver qui a effectué une action dans le logiciel (création, modification, suppression, etc.…). L'application utilise l'heure locale du serveur. Cette fonctionnalité est soumise à des droits, et son accès peut être

	limité à un petit nombre de personnes (personnels d'encadrement par exemple). L'historique est alors accessible dans l'application par un administrateur fonctionnel qui dispose de fonction de filtre et de recherche. Ces traces sont conservées jusqu'à ce qu'elles soient purgées.
Contrôle d'intégrité Mécanismes de contrôle d'intégrité des données stockées	Le contrôle d'intégrité permet de lever une alerte en cas de modification non désirée ou de disparition de données à caractère personnel. EDICIA a mené un travail spécifique sur les formulaires de saisie/modification des données. **Identification des données dont l'intégrité doit être contrôlée et des risques liés** Validation des données : • Règles CRUD : vérification des champs obligatoires, des contraintes de taille, de format et de valeur par défaut • Versionnage des objets : contrôle de concurrence optimiste (gestion des accès concurrents) • Enregistrement des objets : vérification des types de données et exploitation des champs à partir du modèle XML • Suppression des données en double : contrainte d'unicité sur les références de documents **Mise en œuvre de moyens de contrôle de l'intégrité selon le contexte, les risques identifiés et la robustesse attendue** Contrôle d'accès : • Authentification via identifiant/mot de passe personnels, sécurisation par token, gestion de droits d'accès par profil d'utilisation Validation des entrées : • Source connue : l'utilisateur est identifié par son jeton dans chacune de ses requêtes • Traçage des appels http (traçage de l'IP source, du TIMESTAMP, des ressources accédées) Audit : le module Historique • Traces ajoutées automatiquement (journalisation) • Accès soumis à identification (identifiant/mot de passe personnels) • Chaque événement (CRUD) est tracé et historisé (qui a fait quoi, quand) • Horodatage de chaque action

	Pour le cas où des données sont saisies par des utilisateurs externes au service Client (portail web RAPO par exemple), mise en place de mesures d'analyse permettant de prévenir les attaques par injection SQL ou de scripts Les formulaires de saisie « externes » sont conformes aux préconisations OWASP. L'application contrôle la nature des éléments saisis, et empêche la saisie de données non conformes (caractères spéciaux, commandes SQL, etc.) : choix imposé dans des listes déroulantes, limite du nombre de caractères saisis dans les champs de saisie libre, … Les données sont contrôlées avant leur enregistrement. Un antivirus spécifique contrôle l'intégrité des éventuelles pièces jointes au formulaire (documents scannés, etc) Nos équipes procèdent à des tests dans la chaine d'intégration continue (tests d'intrusion), et vérifient le maintien de la conformité OWASP. L'outil de tests de vulnérabilité utilisé est : OWASP ZAP
Archivage Processus de gestion des archives	Les données personnelles ne peuvent être conservées de façon indéfinie dans les fichiers informatiques. Elles doivent être conservées et accessibles par les services opérationnels uniquement le temps nécessaire à l'accomplissement de l'objectif poursuivi lors de leur collecte. La durée de conservation doit être définie par le Client (le propriétaire et donc le responsable du fichier), sauf si un texte impose une durée précise. La durée de conservation va dépendre de la nature des données et des objectifs poursuivis. Une fois cet objectif atteint, ces données doivent être supprimées ou anonymisées Cependant, il peut être justifié que les données personnelles soient conservées pour des durées plus longues en archivage intermédiaire, distinctement de la base active, avec accès restreint (par exemple en cas de contentieux, justifiant de les conserver le temps des règles de prescription/forclusion applicables). EDICIA propose un module d'Archivage des données. Ce module permet au Client d'être autonome dans la conservation et la gestion de ses archives électroniques, dans le respect des exigences du RGPD.

	Fonctionnement du module d'archivage pour les anciens modules L'archivage des données au sens RGPD est géré au niveau applicatif. Le ou les utilisateurs désignés par le Client comme disposant des droits sur l'archivage sélectionnent une date. Toutes les fiches ayant été créées avant cette date sont supprimées physiquement de la base de données de référence (purge). Elles sont stockées dans des fichiers XML. Le ou les utilisateurs désignés par le Client comme disposant des droits sur l'archivage peuvent télécharger un module de consultation des archives (soumis à identification spécifique). **Fonctionnement du module d'archivage pour les modules en version 3** L'archivage des données au sens RGPD est géré au niveau applicatif. Les objets (fiches) ayant dépassé la date d'archivage (date paramétrable selon les modules) ne seront plus visibles par les profils utilisateurs de l'application. Seul un profil avec le droit « Archive » aura le droit de consulter ces données. **Gestion des profils « archiviste »** Le Client doit définir et mettre en œuvre la politique d'archivage (PA) en identifiant les processus de gestion des archives (fréquence, etc), et s'assurer que les rôles et missions en matière d'archivage sont identifiés. Il doit également vérifier qu'il existe une déclaration des pratiques d'archivage (DPA). **Traçabilité de l'archivage** Le module Archivage assure l'identification et l'authentification de l'origine des archives, l'intégrité des archives, l'intelligibilité et la lisibilité des archives, la traçabilité du versement dans les archives, la disponibilité et la sécurisation de l'accessibilité des archives. **Consultation des archives** Le Client doit mettre en œuvre les modalités d'accès spécifiques aux données archivées en définissant les droits d'accès dans l'application EDICIA. Il doit également choisir un mode opératoire de destruction des archives.

Sécurité des documents papier Impression, stockage, échange et destruction des documents papier	En règle générale, les équipes EDICIA n'ont pas recours à l'impression des documents présentant des données clients. Si l'impression de documents s'avérait néanmoins nécessaires, EDICIA a mis en place une politique destinée à limiter les risques d'accès aux documents papiers contenant des données à caractère personnel par des personnes non autorisées. **Marquage des documents contenant des données** Les éventuels documents papier contenant des données personnelles seront marqués au tampon par une mention visible et explicite : Données protégées. **Protection des documents papier** Nos équipes sont sensibilisées aux bonnes pratiques : • Récupération des documents immédiatement après leur impression • Diffusion aux seules personnes destinataires • Stockage des documents dans des armoires d'archivage fermant à clé • Destruction par broyage des documents obsolètes **Traçabilité des échanges** • Conservation des traces des éventuels envois • Protection des documents sensibles (envoi recommandé, sous double enveloppe, ...) En complément, il est à signaler que - l'accès aux locaux EDICIA est protégé par badge individuel - l'accès aux bureaux nécessite une clé (les bureaux sont fermés chaque soir). **...et pour les impressions générées par les clients dans le logiciel :** Dans les versions à venir (à partir de la version 3.6.0), les impressions ou les exports de documents générés à partir du logiciel Smart Police porteront une mention spécifique pour alerter l'utilisateur sur la présence de données personnelles.

Mesures générales de sécurité

Sécurité de l'exploitation Mise à jour des logiciels et application des correctifs de sécurité	EDICIA a mis en place des mesures destinées à limiter la vraisemblance et la gravité des risques visant les supports utilisés en exploitation. **Organisation de l'exploitation** Toutes les tâches d'exploitation et d'administration technique de la plateforme SaaS sont assurées par une équipe dédiée et spécialisée, constituée uniquement de collaborateurs Edicia. Ces intervenants regroupent des profils techniciens, administrateur et ingénieur systèmes, réseaux et bases de données. Leur plage de présence et d'intervention permettent de couvrir l'ensemble des niveaux de service souscrits par les clients. EDICIA s'engage dans ses contrats sur un SLA, avec garantie de temps d'intervention (GTI) et garantie de temps de rétablissement (GTR). L'équipe est pilotée par le responsable infrastructures EDICIA, suppléé en cas d'absence par le directeur technique EDICIA. **Documentation des procédures d'exploitation** La documentation est mise à jour régulièrement et communiquée à l'ensemble des personnels EDICIA concernés. **Inventaire des logiciels et matériels utilisés en exploitation** Les équipes maintiennent une liste exhaustive des logiciels, des serveurs physiques et machines virtuelles, des éléments d'infrastructures, des services gérés par des tiers et des équipements réseaux et de télécommunications utilisés pour l'exploitation des traitements de données personnelles. Cette liste inclut les informations matérielles, les types de système d'exploitation, les informations réseau (adresse IP, adresse MAC), les applications utilisées, les versions présentes et les correctifs appliqués, et les versions des firmwares (pour les équipements pour lesquels ceux-ci peuvent être mis à jour). **Veille sur vulnérabilités découvertes des logiciels utilisés en exploitation** Les systèmes de mise à jour automatique des logiciels sont activés, et les éventuelles mises à jour correctives sont installées dès leur disponibilité. **Documentation des mises à jour (logiciels et équipements)**

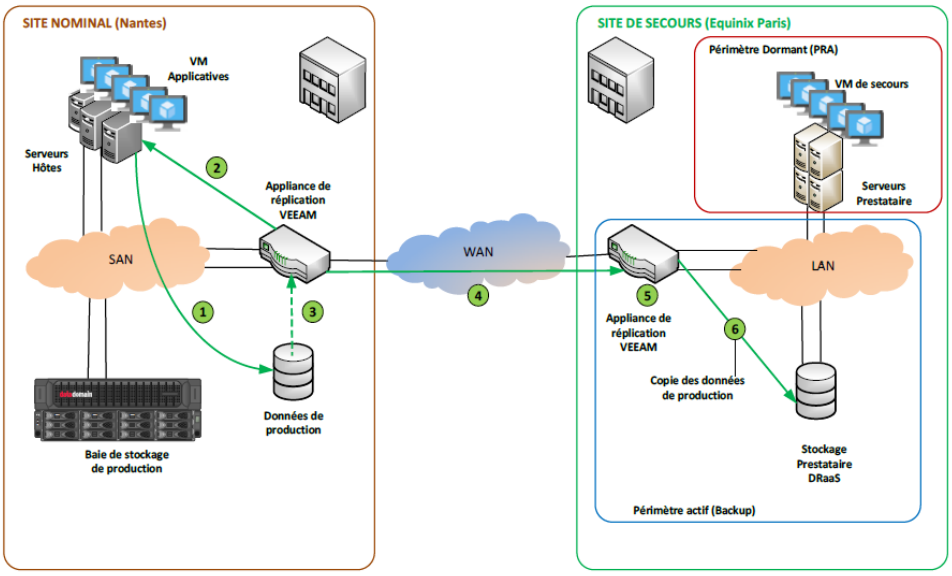
Les serveurs de production (serveurs de base de données, serveur web, serveur de messagerie, etc.) ne sont utilisés que dans le cadre prévu initialement.
EDICIA utilise des unités de stockage de données utilisant des mécanismes de redondance matérielle, et des mécanismes de duplication des données entre plusieurs serveurs et/ou sites.
Nos équipes de supervision s'assurent que le dimensionnement des capacités de stockage et de calcul est suffisant pour assurer le fonctionnement correct des traitements.

EDICIA garantit que les conditions physiques d'hébergement (température, humidité, fourniture d'énergie, etc.) sont appropriées à l'usage prévu des matériels, et incluent des mécanismes de secours.

L'accès physique aux matériels sensibles (serveurs de production) est limité :

- les accès sont sécurisés et soumis à identification biométrique et badge d'accès ;
- l'accès aux baies est protégé par cadenas.

EDICIA a mis en place un PRA (Plan de Reprise d'Activité) pour assurer la disponibilité des traitements mis en œuvre. EDICIA dispose d'une solution de PRA (Plan de reprise d'activité) permettant de basculer la production sur un site de secours (Cf. schéma ci dessous). Le second Data Center est implanté à plus de 10km du site nominal.



Un mécanisme de réplication asynchrone recopie périodiquement les machines virtuelles (VM) du site principal vers le site de secours.

	Ce mécanisme est basé sur l'utilisation d'appliances de réplication VEEAM. Les machines virtuelles synchronisées sur le site du prestataire sont prêt à démarrer en cas de chute du site nominal. Le SLA inclut également • des engagements en termes de reprise de la production (RTO, Recovery Time Objective) en cas de sinistre du site nominal. • des engagements en termes d'intégrité des données (RPO, Recovery Point Objective). La solution de PRA est testée une fois par an en dehors des heures ouvrées. Un process de supervision permet de détecter, enregistrer, qualifier et traiter les incidents de sécurité. **Plan de continuité d'activité (PCA)** En complément du PRA, un PCA (Plan de continuité d'activité) a été défini. Il permet, en cas de défaillance, d'activer une solution de secours pour chaque élément différent de la plateforme. Cette activation est automatique pour 90% des éléments. Les solutions de secours sont testées une fois par an. Pour celles provoquant une interruption de service, le test est planifié durant une plage de maintenance une semaine à l'avance et communiquée aux clients.
Lutte contre les logiciels malveillants	EDICIA assure la sécurité des serveurs qu'elle utilise (serveur de production des services internes, serveurs de production des solutions de ses Clients). Dans ce cadre, EDICIA met en œuvre les bonnes pratiques dans le but de de protéger les accès vers Internet, ainsi que les accès aux postes de travail et aux serveurs contre les codes malveillants qui pourraient affecter la sécurité des données à caractère personnel (antivirus, firewall, proxy, anti-spyware, remontée des événements de sécurité, etc.). Un antivirus est installé et régulièrement mis à jour sur tous les postes (Kaspersky) ; il assure une analyse en temps réel du système. Le service en charge de l'infrastructure de l'entreprise réalise une veille continue sur les alertes de sécurité et assure la mise à jour des correctifs de sécurité. Un logiciel de lutte contre les logiciels espions (anti-spyware) est également installé sur le système informatique.

	Le service en charge de l'infrastructure de l'entreprise met en œuvre des mesures de filtrage permettant de filtrer les flux entrants/sortants du réseau (firewall, proxy, etc.). Les événements de sécurité de l'antivirus sont remontés sur un serveur centralisé afin de permettre une analyse statistique en vue de détecter les problèmes récurrents. EDICIA n'est pas responsable des incidents en lien avec le SI client (postes de travail, serveurs du Client…). Le Client doit s'assurer que toutes les mesures sont prises pour assurer la sécurité sur son SI.
Gestion des postes de travail Mesures de sécurité mises en œuvre sur les postes de travail (verrouillage automatique, pare-feu…etc.)	**Poste de travail des personnels EDICIA** EDICIA assure la sécurité des postes de travail de ses personnels. Dans ce cadre, EDICIA met en œuvre les bonnes pratiques dans le but de de diminuer la possibilité que les caractéristiques des logiciels (systèmes d'exploitation, applications métiers, logiciels bureautiques, paramétrages, etc.) ne soient exploitées pour porter atteinte aux données à caractère personnel (mises à jour, protection physique et des accès, travail sur un espace réseau sauvegardé, contrôleurs d'intégrité, journalisation, etc.). **Poste de travail chez le Client** Les applications EDICIA ne sont pas installées sur les postes de travail du Client. Elles sont installées sur un serveur distant, et est accessible via un navigateur. EDICIA n'est pas responsable des incidents en lien avec les équipements du Client (postes de travail, serveurs du Client…). Le Client doit s'assurer que toutes les mesures sont prises pour assurer la sécurité sur ses équipements. **Utilisation des applications EDICIA chez le Client** Pour assurer la protection des applications EDICIA, le Client peut paramétrer un délai au delà duquel, si l'utilisateur n'a pas réalisé de manipulation, l'application se verrouille automatiquement.

Sécurité des sites web Sécurisation des sites web	EDICIA met en œuvre les bonnes pratiques pour minimiser la possibilité que les caractéristiques des sites web soient exploitées pour porter atteinte aux données à caractère personnel. Les applications sont conformes aux « recommandations pour la sécurisation des sites web » de l'ANSSI. Le seul site de télé-service est le portail de dépose en ligne des RAPO. Il est conforme au référentiel général de sécurité (RGS), et utilise un certificat signé par une autorité racine de confiance "qualifiée" (certificat TBS internet). Le chiffrement des flux est garanti par TLS.
Sauvegardes Gestion et sécurisation des sauvegardes	La sauvegarde des données a pour objectif d'assurer la disponibilité et/ou l'intégrité des données à caractère personnel, tout en protégeant leur confidentialité (régularité des sauvegardes, chiffrement du canal de transmission des données, test d'intégrité, etc.). Le plan et la procédure de sauvegarde permettent d'assurer l'intégrité et la pérennité des données à caractère personnel, tout en conservant leur confidentialité. Le plan de sauvegarde définit les objectifs généraux attendus des sauvegardes en matière de protection des données et les mesures organisationnelles nécessaires pour atteindre ces objectifs. EDICIA met en œuvre les moyens opérationnels et techniques pour satisfaire au plan de sauvegarde (procédure de sauvegarde). La politique de sauvegarde est exécutée conformément aux engagements contractuels signés par le client. Par défaut, les modalités suivantes sont appliquées : **Politique de sauvegarde :** EDICIA réalise une sauvegarde incrémentale quotidienne des données de ses clients. Une sauvegarde complète est effectuée chaque semaine, le dimanche. **Politique de rétention :** Le plan de rétention est le suivant : 7 sauvegardes journalières, 4 sauvegardes hebdomadaires et 3 sauvegardes mensuelles (soient 4 mois de profondeur). • 6 dernières sauvegardes incrémentales quotidiennes

	• 4 dernières sauvegardes complètes hebdomadaires. **Modalités** Les sauvegardes sont réalisées sur disque et sur bande type LTO. Les sauvegardes sur bande sont dupliquées pour externalisation hebdomadaire sur un site distant et sécurisé autre que le site de PRA. Un rapport d'exécution de l'ensemble des sauvegardes est généré automatiquement et contrôlé quotidiennement par un technicien d'exploitation. Une fois par trimestre, un contrôle manuel approfondi d'un échantillon significatif de sauvegardes est réalisé par le responsable infrastructures. **Les erreurs de sauvegardes sont traitées comme suit :** • une sauvegarde à chaud est reprise dans la journée • pour une sauvegarde à froid, l'exécution suivante de celle-ci est supervisée par l'équipe d'astreinte afin de pouvoir être corrigée et reprise aussitôt en cas de seconde défaillance. Un test de restauration significatif est exécuté au moins une fois par trimestre pour valider les procédures de restauration et maintenir les compétences des collaborateurs. Dans son SLA, EDICIA s'engage en termes de délai de restauration (suite à un crash, à une perte de données ou à la demande).
Maintenance Gestion de la maintenance physique des équipements	EDICIA met en œuvre les mesures nécessaires pour limiter la vraisemblance des menaces liées aux opérations de maintenance sur les matériels et logiciels dont elle a la charge. **En interne :** • La réalisation des opérations de maintenance est réalisée par les personnels d'EDICIA. Si l'intervention d'un prestataire s'avérait nécessaire, elle serait encadrée par un contrat de sous-traitance. • Toutes les opérations de maintenance et de télémaintenance sont tracées dans une dans une main courante. • Les éventuels matériels envoyés en maintenance externe sont débarrassés des données qu'ils contiennent avant envoi, • Avant élimination ou recyclage du poste de travail, toutes les données et les paramètres (y compris la mémoire) sont effacés. **Opérations de maintenance sur les applications utilisées par nos Clients :**

	Pour les opérations de maintenance sur les logiciels en production chez le Client : • Les opérations de maintenance nécessitant une prise en main à distance sur un poste de travail sont toujours assujetties à l'accord de l'utilisateur • Les équipements mobiles (téléphones) peuvent être verrouillés après une période d'inactivité (paramétrage accessible à l'administrateur de l'application chez le Client). **Cas particulier des équipements mobiles (smartphones)** Les smartphones installés par EDICIA et son partenaire TIMCOD sont équipés d'un outil d'administration à distance. Outre son rôle essentiel dans le cadre des opérations de maintenance, cet outil permet également de géo localiser, et/ou de rendre inutilisable un téléphone perdu ou volé.
Sécurité des canaux informatiques (réseaux) Mesures de sécurisation des réseaux	EDICIA met en œuvre les mesures nécessaires pour diminuer la possibilité que les caractéristiques de ses canaux informatiques internes (réseau filaire, wifi, ondes radio, fibre optique, etc.) soient exploitées pour porter atteinte aux données à caractère personnel. Nos équipes d'architectes : • Tiennent à jour la cartographie détaillée du réseau (y compris les accès Internet, en indiquant les mesures de sécurisation appliquées à chacun d'entre eux) • S'assurent que les canaux informatiques sont correctement dimensionnés par rapport aux flux prévus • Assurent la segmentation du réseau en sous-réseaux logiques étanches selon les services qui y sont déployés • Interdisent toute communication directe entre des postes internes et l'extérieur. • Assurent le bon fonctionnement du pare-feu (afin que seuls des flux explicitement autorisés soient accessibles) • Supervisent globalement l'activité réseau. • Sécurisent les flux d'administration et interdisent, l'accès physique et logique aux ports de diagnostic et de configuration à distance • Interdisent le raccordement d'équipements informatiques non maîtrisés. **Spécificités pour les connexions aux équipements actifs du réseau** Nous utilisons le protocole SSH pour la connexion aux équipements

	actifs du réseau (pare-feu, routeurs, commutateurs) **Spécificités pour les outils de prise de main à distance** La prise de main à distance d'une ressource informatique locale est limitée aux agents du service en charge de l'informatique Les utilisateurs de l'outil de prise de main à distance sont identifiés et authentifiés (identifiant personnel et mot de passe robuste). L'utilisateur est systématiquement informé qu'une prise de main à distance est en cours sur son poste de travail. **Spécificités pour les postes nomades ou se connectant à distance** EDICIA met en place toutes les mesures pour réduire les risques liés à l'utilisation distante des postes nomades ou se connectant à distance. **Spécificités pour les interfaces sans fil (Wifi, Bluetooth, infrarouge, 4G, etc.)** Dans le cas de connexions à l'aide d'interfaces sans fil, seules les communications sécurisées sont autorisées. **Spécificités pour le Wifi** L'accès au WIFI est soumis à authentification WPA avec un mode de chiffrement AES/CCMP. Un pare-feu est activé au point d'entrée/sortie du réseau, afin de cloisonner les équipements connectés en fonction des besoins. **Spécificités pour la navigation sur Internet** Le protocole TLS (HTTPS) est systématiquement utilisé pour assurer l'authentification des serveurs et la confidentialité des communications.
Contrôle d'accès physiques Sécurisation des accès physique aux locaux	EDICIA fait preuve d'une vigilance particulière concernant les accès physiques aux données, qu'il s'agisse des données de l'entreprise ou des données appartenant à ses clients. Elle met en œuvre les mesures nécessaires à la protection des locaux dans le but de limiter l'accès aux données aux seules personnes autorisées. **Séparation des zones selon les risques : Données EDICIA** Le stockage des données internes est assuré dans une salle serveur verrouillée. Les accès aux stations d'administration du réseau, aux éléments actifs du réseau, aux ressources sensibles telles que des

	équipements d'alimentation et de distribution d'énergie, ou des équipements réseau et de téléphonie sont placés dans une zone fermée à clé. Seul un nombre restreint de personnels autorisés peuvent accéder aux équipements. Tout visiteur est systématiquement accompagné par une personne salariée d'EDICIA (depuis son entrée, pendant sa visite et jusqu'à sa sortie des locaux). **Séparation des zones selon les risques : Données appartenant aux Clients** Le stockage des données Client est assuré sur des équipements hébergés dans un Data Center sécurisé de dernière génération, situé en région nantaise (HITS/NeoTELECOM). Les serveurs hébergés sont la propriété d'EDICIA et sont gérés par les personnels habilités d'EDICIA. Les accès sont sécurisés et soumis à identification biométrique. Tous les accès sont tracés : identité de la personne, date et heure de l'entrée, ainsi que de la sortie. Les accès au Data Center sont sécurisés. Le Data Center est protégé par des systèmes d'alarme. L'accès aux baies et cages est soumis à identification par code ou badge. L'hébergeur assure une prestation de télésurveillance 24h24 et 7j/7. Il garantit la sécurité incendie, et a équipé son Data Center de portes blindées et coupe-feu. Le personnel de l'hébergeur n'a pas accès aux serveurs. **Contrôle d'accès aux locaux EDICIA** Les accès aux bureaux sont sécurisés par une porte renforcée et verrouillée. L'accès au bâtiment est soumis à accès par badge ou digicode. Un dispositif de vidéosurveillance permet de sécuriser les couloirs du bâtiment. L'accès aux bureaux n'est possible que pour les personnels disposant d'un badge personnel. Tout visiteur doit sonner, et se présenter au vidéophone. Il est ensuite accueilli, puis est systématiquement accompagné par une personne salariée d'EDICIA (depuis son entrée, pendant sa visite et jusqu'à sa sortie des locaux).

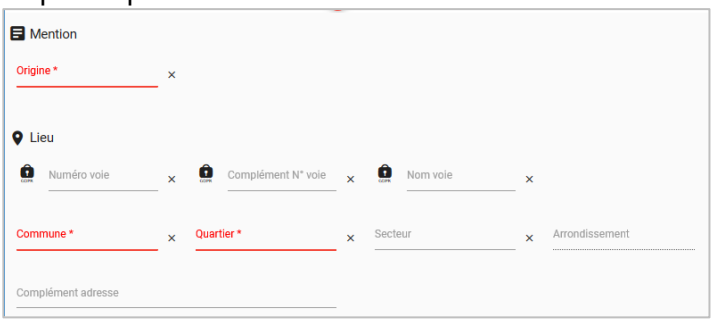
Sécurité des matériels Mesures de sécurité physique des serveurs et des postes clients	EDICIA met en œuvre les bonnes pratiques pour diminuer le risque que les caractéristiques des matériels soient exploitées pour porter atteinte aux données à caractère personnel. **Mesures génériques** • Les équipes en charge de l'infrastructure EDICIA tiennent à jour un inventaire des ressources informatiques utilisées (serveurs, équipements réseau, postes de travail, périphériques, etc…) • Le réseau local utilisé par les collaborateurs s'appuie sur des ressources réseau dédiées. • L'accès aux ressources informatiques est restreint au service en charge de l'informatique (salle serveur fermée à clé, accessible par badge). **Data Center Sécurisé** Les serveurs EDICIA sont hébergés dans un Datacenter de dernière génération situé en région nantaise (HITS/NeoTELECOM). Les caractéristiques principales du Datacenter sont listées ci-dessous: • Datacenter de conception Tiers III+ • Haute Disponibilité • Exploitation, supervision et maintenance 24h/24 et 7j/7 • Multi opérateurs, double adductions fibre, routage IP BGP • Onduleurs modulaires à hauts rendements • Double adduction électrique, groupes électrogènes durée 24h rechargeable à chaud. • Allées froides confinées • Bâtiment haute qualité environnementale HQE **Sécurisation de la plateforme** La plateforme physique est composée de 3 serveurs HP et la baie de stockage EMC. La redondance et la haute disponibilité des machines virtuelles (VM) est assuré par WMvare VSphere. En cas de panne d'un des serveurs, les 2 restants sont dimensionnés pour absorber de façon nominale la charge de l'ensemble des machines virtuelles (VM) en production. La sécurisation des données des machines virtuelles (VM) est assurée par le stockage des disques virtuels des machines virtuelles (VM) sur la baie EMC. La baie EMC composé d'un ensemble de 10 disques de 1 To en RAID

	6 (2 disques de parité), d'une alimentation redondante. L'ensemble du matériel bénéficie d'un contrat de maintenance matériel avec une GTR 4h 24x7x365 Une sauvegarde externe vers le siège Edicia est effectuée quotidiennement. Cette sauvegarde a pour but de permettre une restauration de la production en minimisant les pertes de données en cas d'incident majeur provoquant la destruction complète du matériel chez l'hébergeur. <u>Accès privé</u> • Un lien et des équipements sont dédiés à l'administration et à l'export des sauvegardes vers le siège EDICIA. Seule l'adresse IP publique du site EDICIA est autorisée à accéder à ces équipements. • Les accès à l'architecture sont effectués par des ingénieurs systèmes qualifiés avec des identifiants uniques et sécurisés par clefs le tout sur une connexion de type tunnel VPN. Tous les accès sont logués. <u>Accès public</u> • Les clients se connectent via un site web sécurisé par certificats (issue d'une autorité de certification). Les flux sont filtrés et logués par le cluster de firewall. En cas de défaillance d'un routeur, l'autre prend le relais. **Sécurité des équipements chez le Client** EDICIA n'est pas responsable des incidents en lien avec les matériels du client (postes de travail, imprimantes, etc…). Le Client doit s'assurer que toutes les mesures sont prises pour assurer la sécurité sur ses matériels.

Éloignement des sources de risques Caractéristiques de la zone d'implantation	EDICIA met en œuvre les bonnes pratiques pour éviter que des sources de risques ne portent atteinte aux données à caractère personnel. La zone d'implantation n'est pas sujette à des sinistres environnementaux (zone inondable, proximité d'industries chimiques, zone sismique ou volcanique, etc...) et ne contient pas de produits dangereux. Les données sont stockées en France, à moins de 20km du siège, dans une zone non sujette à des sinistres environnementaux.
Protection contre les sources de risques non humaines Moyens de prévention, de détection et de lutte contre l'incendie, les dégâts des eaux, etc	EDICIA met en œuvre les bonnes pratiques pour éviter les risques liés à des sources non humaines (phénomènes climatiques, incendie, dégât des eaux, accidents internes ou externes, animaux, etc.). La zone d'implantation n'est pas sujette à des sinistres environnementaux (zone inondable, proximité d'industries chimiques, zone sismique ou volcanique, etc...) et ne contient pas de produits dangereux. Les données sont stockées en France, à moins de 20km du siège, dans une zone non sujette à des sinistres environnementaux. **Data Center Sécurisé** Les serveurs EDICIA sont hébergés dans un Datacenter de dernière génération situé en région nantaise (HITS/NeoTELECOM). Les caractéristiques principales du Datacenter sont listées ci-dessous: • Datacenter de conception Tiers III+ • Exploitation, supervision et maintenance 24h/24 et 7j/7 • Double adduction électrique, groupes électrogènes durée 24h rechargeable à chaud. • Allées froides confinées • Bâtiment haute qualité environnementale HQE • Sécurité incendie • Portes blindées et coupe-feu La sécurité du lieu de stockage des données est garantie contractuellement avec l'hébergeur.

Mesures organisationnelles (gouvernance)

Organisation de la protection des données DPO et RSSI, comité de suivi…	**Pour ce qui est des données EDICIA (données internes, fichiers clients, etc…)** Nom / Coordonnées du DPO : Philippe Dupuis, siège EDICIA Nom / coordonnées du RSSI : Cormerais Christian, siège EDICIA **Pour ce qui est des données du CLIENT (données métiers.)** Le client est seul responsable des données. Il doit mettre en place les traitements appropriés pour assurer : • Le respect de la vie privée des personnes, si des informations personnelles sont conservées au sein de votre progiciel, • L'évaluation des risques pour les droits et les libertés. Indiquer les mesures pour faire face aux risques identifiés. <u>Les obligations de la collectivité :</u> • Nommer un DPO : si la nomination d'un DPO est conseillée pour les entreprises privées, elle est obligatoire pour les structures publiques. Le DPO peut être nommé au sein même de la structure, il peut donc s'agir d'un employé, mais il peut être également être désigné en externe (organisme tierce, prestataire, ou cabinet d'avocat par exemple). • Mise en place d'un registre des traitements des données personnelles : pour cartographier les différents types de données exploitées, les finalités de ces données, les personnes pouvant y accéder, les types de données exploitées ou encore la durée de conservation de ces données. • Réalisation d'une étude d'impact sur la vie privée : les organismes publics sont tenus d'effectuer une étude afin de déterminer les impacts de ces traitements des données sur la vie privée des personnes concernées et d'identifier les mesures techniques et organisationnelles nécessaires pour assurer la pleine protection de cette vie privée. • Mise en conformité en matière de récolte de données : les établissements publics disposent de conditions particulières, et le consentement préalable des personnes concernées n'est pas toujours obligatoire. L'organisation publique peut se passer de ce consentement lorsque le traitement des données est nécessaire à l'exécution d'une mission d'intérêt public et relève de l'autorité légale de la structure.

Politique de sécurité Formation des personnels à la protection des données et la bonne utilisation des moyens informatiques	Seuls les collaborateurs sont habilités et autorisés à intervenir sur la plate-forme Saas utilisée par nos clients. Tous les accès sont nominatifs et encadrés par des règles strictes (accès restreint, mot de passe complexes et changés régulièrement, ...). La liste et les autorisations d'accès sont mises à jour à chaque départ ou arrivée d'un collaborateur. De manière générale, l'ensemble des collaborateurs d'Edicia est régulièrement sensibilisé à la sécurité. Chaque nouvel arrivant assiste à une présentation des règles essentielles de sécurité à suivre dans l'entreprise. Celles-ci sont consignées dans la charte informatique signée par chaque collaborateur. Sensibilisation des salariés sur la protection des données Signature d'avenants RGPD aux contrats de travail Une veille technologique permanente est assurée autour des failles de sécurité des différents composants matériels et logiciels de la plate-forme Saas. Les alertes de sécurité concernant ces éléments sont traitées dans les plus brefs délais.
Gestion des risques Cartographie des risques	Voir cartographie des risques fournie en fin de tableau
Cartographie des données Cartographie des données	Les données sensibles sont des noms, apparaissant dans les mains-courantes, ou dans les modules de gestion (Fourrière, Animaux dangereux.....), ainsi que potentiellement des photos jointes. Ces données sont isolées dans des champs spécifiques de manière à pouvoir être identifiées lors des traitements. Nous avons cartographié les données de nature « personnelles » dans nos applications. Dans les prochaines versions, chaque champ de saisie destiné à la saisie de données personnelles (au sens du RGPD) sera identifié par une icône spécifique.  Le manuel du logiciel sera amendé avec la liste des champs de saisie destiné à la saisie de données personnelles (liste classée par module).

Cartographie des risques Cartographie des risques	Voir cartographie des risques fournie en fin de tableau
Gestion des projets Tests des dispositifs	Les équipes EDICIA réalisent les tests et recettes dans un environnement avec une base de données interne. Chez le Client, les équipes souhaitent généralement effectuer leurs tests/recette sur des données identiques à celles de production ; dans ce cas, pour les Clients qui disposent d'une plateforme de tests, une copie de la base de production peut être chargée sur l'environnement de tests du Client. S'agissant de données dont il est propriétaire, il n'y a pas d'anonymisation des données. Il appartient au Client de s'assurer que les personnels qui accèdent à la plateforme de tests disposent bien des habilitations nécessaires pour accéder aux données. Pour ce qui est des exports EXCEL, dans les dernières versions du logiciel Smart POLICE, le client peut paramétrer ses fichiers d'export et restreindre les données aux seules données autorisées (fonction de paramétrage accessible uniquement aux administrateurs de l'application).
Gestion des incidents et des violations de données Gestion des incidents de violation de données à caractère personnel	EDICIA a entrepris une action de refonte des procédures de remontées d'informations et de réaction, en cas de violation de données : définition des indicateurs et niveaux d'alerte, mesures permettant de gérer les incidents et violations de données, conformément aux textes en vigueur, etc… En parallèle, nous revoyons l'organisation opérationnelle de manière à améliorer la détection et le traitement des événements susceptibles d'affecter les libertés et la vie privée des personnes concernées. Le process initié comprend : - la formalisation des rôles et responsabilités du référent « Informatique et libertés » (DPO) ; - la consignation des incidents dans une main courante interne; - les procédures d'escalade ; - les interactions avec la CNIL, et avec les référents chez le Client ; - la possibilité de constituer une cellule de crise en cas de sinistre.

Gestion des personnels Mesures prises à l'arrivée d'une personne dans sa fonction (sensibilisation) et au départ d'une personne (sécurisation)	EDICIA met en œuvre les bonnes pratiques pour diminuer la possibilité que les caractéristiques des personnels soient exploitées pour porter atteinte aux données (ressources et compétences adéquates, sensibilisation, etc.). • Elle vérifie systématiquement que les personnes ayant accès aux données et au traitement sont aptes à exercer leur fonction. • Elle vérifie systématiquement que les personnes ayant accès aux données et au traitement ont été formées et disposent des compétences appropriées aux conditions d'exercice de leurs fonctions. • Elle s'assure que les conditions de travail des personnes ayant accès aux données et au traitement sont satisfaisantes. De manière générale, l'ensemble des collaborateurs d'Edicia est régulièrement sensibilisé à la sécurité. Chaque nouvel arrivant assiste à une présentation des règles essentielles de sécurité à suivre dans l'entreprise. Les personnels sont sensibilisés aux risques liés à l'exploitation de leurs vulnérabilités. Seules les personnes ayant nécessité d'accéder aux applications pour mener à bien l'exercice de leur fonction disposent des droits associés. Au départ d'un salarié, les mots de passe d'accès aux données sensibles sont intégralement renouvelés.
Relations avec les tiers Modalités et mesures de sécurité mises en œuvre pour les éventuels accès sous-traitants	EDICIA met en œuvre les bonnes pratiques dans le but de réduire les risques que les accès légitimes aux données par des tiers peuvent faire peser sur les libertés et la vie privée des personnes concernées. Parmi ces mesures : la formalisation des règles que les personnes doivent respecter durant tout le cycle de vie de la relation liée au traitement ou aux données, selon la catégorie de personnes et les actions qu'elles vont réaliser. **Spécificités pour les tiers prestataires de service travaillant dans les locaux de l'organisme** Les éventuels prestataires se voient appliquer les mêmes mesures que pour les salariés EDICIA : formation aux enjeux Informatique et libertés, obligation de respecter les règles d'usage des ressources informatiques de l'organisme annexées contrat de travail.

	Les prestataires sont engagés par une clause de confidentialité. Les habilitations des prestataires sont gérées spécifiquement (habilitations limitées dans le temps prenant fin automatiquement à la date prévisionnelle de la fin de leur mission).
Supervision Contrôle de l'effectivité et l'adéquation des mesures touchant à la vie privée	EDICIA met en œuvre les mesures nécessaires pour disposer d'une vision globale et à jour de l'état de protection des données et de la conformité à la loi informatique et libertés. **Contrôles** Nos équipes effectuent régulièrement des contrôles des traitements de données afin de vérifier leur conformité à la loi informatique et libertés ainsi que l'effectivité et l'adéquation des mesures prévues. **Indicateurs** La mise en place d'indicateurs permettant de vérifier l'atteinte des objectifs dans le domaine « Informatique et libertés » est en cours. Une cartographie des traitements de données et des risques associés a déjà été mise en place.

Cartographie des risques & Réponses aux questions les plus courantes dans le cadre de l'anticipation des risques en conformité avec la RGPD

Accès illégitime à des données	
Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?	Risque commun à toute divulgation de données personnelles sensibles : impact de niveau « 2.Limitéé » selon l'échelle CNIL pour estimer la gravité Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans grande difficulté Exemples d'impacts moraux : Simple contrariété par rapport à l'information reçue ou demandée
Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?	Les cyberattaques, Négligence du personnel, des sous-traitants ou des utilisateurs, Malveillance du personnel, des sous-traitants ou des utilisateurs
Quelles sources de risques pourraient-elles en être à l'origine ?	· Piratage de la plateforme · Divulgation volontaire ou non par des informations ou des accès par une personne habilité d'EDICIA · Divulgation volontaire ou non par des informations ou des accès par une personne habilité de la ville · Piratage du poste informatique d'une personne habilité de la ville
Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?	· Mesure de cyber sécurité au niveau de la plateforme EDICIA o Architecture Physique redondante et sauvegardée avec cluster de serveurs physique et baie de stockage o Architecture Système avec Firewall applicatif, Reverse proxy et VirtualMachine dédiée par ville o Architecture logicielle sécurisée (TLS 1.2, SpringSecurity, Authentification JWT, Authentification forte mobile avec carte à puce) et Tests de vulnérabilités · Traçabilité des accès à l'application · Accès à la production uniquement par VPN nominatif · Faire prendre conscience à chaque utilisateur des enjeux en matière de sécurité et de vie privée et implication contractuelle dans le contrat de travail

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?	Gravité de niveau « 2.Limitéé » selon l'échelle CNIL pour estimer la gravité
Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?	Vraisemblance de niveau « 2.Limitée » selon l'échelle CNIL pour estimer la vraisemblance : il semble difficile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports. Attention : l'estimation ci-dessus concerne le risque au niveau du prestataire. Elle ne prend pas en compte le risque de divulgation de données par une personne habilitée par la ville à accéder à ces données

Modification non désirées de données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?	Impact de niveau « 1. Négligeable » à «2.Llimitée » selon l'échelle CNIL pour estimer la gravité Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans grande difficulté
Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?	Les cyberattaques, Négligence du personnel, des sous-traitants ou des utilisateurs, Malveillance du personnel, des sous-traitants ou des utilisateurs
Quelles sources de risques pourraient-elles en être à l'origine ?	· Piratage de la plateforme · Divulgation volontaire ou non par des informations ou des accès par une personne habilité d'EDICIA · Divulgation volontaire ou non par des informations ou des accès par une personne habilité de la ville · Piratage du poste informatique d'une personne habilité de la ville
Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?	· Mesure de cyber sécurité au niveau de la plateforme EDICIA o Architecture Physique redondante et sauvegardée avec cluster de serveurs physique et baie de stockage o Architecture Système avec Firewall applicatif, Reverse proxy et VirtualMachine dédiée par ville o Architecture logicielle sécurisée (TLS 1.2,

	SpringSecurity, Authentification JWT, Authentification forte mobile avec carte à puce) et Tests de vulnérabilités · Traçabilité des accès à l'application · Accès à la production uniquement par VPN nominatif · Faire prendre conscience à chaque utilisateur des enjeux en matière de sécurité et de vie privée et implication contractuelle dans le contrat de travail
Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?	Gravité de niveau « 1. Négligeable » à «2.Llimitée » selon l'échelle CNIL pour estimer la gravité
Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?	Vraisemblance de niveau « 2.Limitée » selon l'échelle CNIL pour estimer la vraisemblance : il semble difficile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports. Attention : l'estimation ci-dessus concerne le risque au niveau du prestataire. Elle ne prend pas en compte le risque de divulgation de données par une personne habilitée par la ville à accéder à ces données
Disparition de données	
Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?	Impact de niveau « 1. Négligeable » à «2.Llimitée » selon l'échelle CNIL pour estimer la gravité Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans grande difficulté
Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?	Les cyberattaques, Négligence du personnel, des sous-traitants ou des utilisateurs, Malveillance du personnel, des sous-traitants ou des utilisateurs
Quelles sources de risques pourraient-elles en être à l'origine ?	· Piratage de la plateforme · Divulgation volontaire ou non par des informations ou des accès par une personne habilité d'EDICIA · Divulgation volontaire ou non par des informations ou des accès par une personne habilité de la ville

	· Piratage du poste informatique d'une personne habilité de la ville
Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?	· Mesure de cyber sécurité au niveau de la plateforme EDICIA o Architecture Physique redondante et sauvegardée avec cluster de serveurs physique et baie de stockage o Architecture Système avec Firewall applicatif, Reverse proxy et VirtualMachine dédiée par ville o Architecture logicielle sécurisée (TLS 1.2, SpringSecurity, Authentification JWT, Authentification forte mobile avec carte à puce) et Tests de vulnérabilités · Traçabilité des accès à l'application · Accès à la production uniquement par VPN nominatif · Faire prendre conscience à chaque utilisateur des enjeux en matière de sécurité et de vie privée et implication contractuelle dans le contrat de travail
Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?	Gravité de niveau « 1. Négligeable » à «2.Llimitée » selon l'échelle CNIL pour estimer la gravité
Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?	Vraisemblance de niveau « 2.Limitée » selon l'échelle CNIL pour estimer la vraisemblance : il semble difficile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports. Attention : l'estimation ci-dessus concerne le risque au niveau du prestataire. Elle ne prend pas en compte le risque de divulgation de données par une personne habilitée par la ville à accéder à ces données