Politique de protection des données

Auteur : Stéphane KLEIN, RSSI, DPO

Approuvé par : Alain CADOT, Président

Dernière date de mise à jour : 09 Octobre 2019

Le contexte

La protection des données, un enjeu majeur

Les menaces sur les systèmes d'informations ont évolué depuis quelques années. Les cibles des entités malveillantes s'orientent maintenant vers le vol de données monnayables sur le cyber marché noir. L'année 2017 a été caractérisée par de nombreux incidents liés à la fuite de données sensibles.

Dans le cadre de leurs activités, les entreprises conservent des informations à caractère personnel pour l'ensemble de leurs employés, de leurs clients et de leurs fournisseurs.

La loi RGPD (règlement général pour la protection des données) est venu renforcer les droits des personnes concernées par ces données.

En effet, en fonction du contexte et du niveau de sensibilité des données, l'impact d'un incident sur celles-ci pour les personnes concernées peut avoir des conséquences graves, voir fatales sur l'intégrité de ces personnes.

CIS Valley, en tant qu'hébergeur de données de santé depuis 2010, dispose d'une forte expérience sur la protection des données à caractère personnel. Il s'agit de protéger la disponibilité, l'intégrité et la confidentialité de ces données.

Définitions

Données à caractère personnel : Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée personne concernée) ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Traitement : Toute opération ou tout ensemble d'opérations effectués ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel, tels que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Fiche de traitement : Document décrivant le traitement et permettant de recenser les informations nécessaires à la qualification de son niveau de sensibilité. On y trouve notamment une description du traitement et de sa finalité, les bases légales, les coordonnées du personnel en charge du traitement, la liste des données à caractère personnel traitée, les mesures de sécurité…

Responsable de traitement : Le responsable de traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. Dans le cas de l'activité d'infogérance, il s'agit du client.

Sous-traitant : Le sous-traitant traite des données personnelles pour le compte, sur instruction et sous l'autorité d'un responsable de traitement. Dans le cadre de l'activité d'infogérance, CIS Valley fait partie des sous-traitants du client.

DPO ou DPD : Le Data Protection Officer (DPO) ou Délégué à la Protection des Données (DPD) est chargé de piloter la conformité au règlement européen au sein de l'organisme qui l'a désigné.

CIS Valley en tant que responsable de traitement

Dans le cadre de ses activités internes, CIS Valley est responsable de traitement.

Périmètre de collecte des données

CIS Valley collecte et conserve les types de données à caractère personnel suivants :

- Données RH des salariés
- Coordonnées professionnelles des salariés, clients et fournisseurs

Finalité de la collecte

Les traitements mis en œuvre répondent à des finalités explicites, légitimes et déterminées.

Les données sont traitées principalement pour les finalités suivantes :

- Gestion des métiers des ressources humaines (paie, déclarations légales,)
- Gestion technique et commerciale des métiers de l'infogérance, l'intégration et le développement
- Gestion de la crise

Destinataire des données

Les destinataires des données à caractère personnel sont les services concernés de la société CIS Valley.

Conservation des données

Chaque type de donnée fait l'objet d'une analyse afin d'évaluer les durées de conservation en lien avec les besoins métiers. Ces durées sont formalisées dans le registre de l'entreprise.

Sécurité

CIS Valley assure la sécurité des données à caractère personnel en mettant en place une protection des données renforcée par l'utilisation de moyens de sécurisation physiques et logiques.

Comment exercer vos droits

Conformément à la loi Informatique et libertés du 6 janvier 1978 modifiée, vous disposez d'un droit d'accès, d'interrogation, de modification et de rectification aux informations qui vous concernent.

Vous disposez également d'un droit d'opposition au traitement de vos données à caractère personnel pour des motifs légitimes, ainsi que d'un droit d'opposition à ce que ces données soient utilisées à des fins de prospection commerciale.

Vous disposez enfin du droit de définir des directives générales et particulières précisant la manière dont vous entendez que soient exercés, après votre décès, ces droits.

Pour exercer vos droits, vous devez adresser un courrier au DPD de CIS Valley, accompagné de la photocopie d'un titre d'identité comportant votre signature, à l'adresse postale suivante : CIS Valley, Mr le délégué à la protection des données, Rue de l'Hermite, 33520 BRUGES CEDEX, ou à l'adresse de courrier électronique dpd@cis-valley.fr.

Si vous êtes salarié de CIS Valley, vous pouvez prendre directement contact avec le DPD par mail.

Code de conduite

CIS Valley s'interdit d'utiliser les données des systèmes d'information de ses clients à des fins de profilage des personnes concernées par les données à caractère personnel, ou à des fins commerciales.

Dans le cadre de son informatique interne et en tant que responsable de traitement, CIS Valley a constitué un registre et effectué les analyses d'impact nécessaires à la protection des données à caractère personnel qu'il manipule.

Les collaborateurs de CIS Valley en charge de la gestion des données clients sont régulièrement sensibilisés à la sécurité des systèmes d'information. Au travers de l'agrément pour l'hébergement de données de santé, les collaborateurs travaillent au quotidien dans un environnement sensible et comprennent les enjeux liés à la protection des données.

Au-delà, ils disposent dans leur contrat de travail d'une clause de confidentialité en rapport avec la nécessité d'accès à certaines données dans le cadre de leurs missions.

Les ingénieurs des centres d'infogérance doivent remonter régulièrement des informations au délégué à la protection des données et au RSSI concernant de potentielles failles détectées ou des demandes inhabituelles qui pourraient comporter un risque pour le droit des personnes.

CIS Valley en tant que sous-traitant

1. Les aspects juridiques

Rôles et responsabilités

1. DPD : Il est fortement conseillé de nommer un DPD dans toute entreprise qui sera responsable de la gouvernance de la sécurité des données à caractère personnel. Dans les cas suivants, cette nomination est obligatoire :

    - Autorité publique (personnes morales de droit public) comme l'État, les collectivités territoriales (communes, départements, régions), ainsi que les établissements publics (hôpitaux, universités…)
    - Opérations de traitement exigeant un suivi régulier et systématique à grande échelle des personnes concernées
    - Traitement à grande échelle de données à caractère personnel ou de données personnelles relatives à des condamnations pénales et à des infractions.

2. Responsables de traitement : Au sein de chaque entreprise, des responsables de traitement doivent être nommés, ce sont souvent les responsables de chaque métier de l'entreprise qui maîtrisent les traitements opérés sur les données en relation avec le métier.

3. Les contrats avec les clients et les fournisseurs doivent contenir les clauses spécifiques au RGPD afin de bien définir la répartition des responsabilités.

Pour CIS Valley :

CIS Valley a nommé un DPD qui est chargé de contrôler la prise en compte de la loi RGPD et le respect des mesures de sécurité convenues avec les clients (voir plus haut pour la procédure permettant d'exercer vos droits).

2. La gouvernance

Identification des données et des traitements

La loi RGPD indique que le responsable de traitement doit procéder au recensement des données et des traitements effectués sur ces données. Il doit vérifier la licéité du traitement avant d'autoriser sa mise en œuvre. Le recensement des données et des traitements consiste à identifier les flux de données provoqués par les traitements, les biens supports associés à ces traitements et le niveau de sensibilité des données associées. Les questions qui seront posées lors de ce recensement sont :

- Qui : Qui est responsable de traitement, qui est responsable d'exploitation des données et traitements ?

- Quoi : Quelles sont les catégories de données, on identifiera ici le niveau de sensibilité de la donnée ?
- Pourquoi : Quelle est la légitimité, la finalité du traitement ?
- Où : Où sont positionnées les données : Biens supports, pays… ?
- Jusqu'à quand : La conservation des données doit être limitée au strict nécessaire
- Comment : Quelles sont les mesures de sécurité à déployer pour protéger les données ?

Le résultat du recensement doit être intégré dans un registre contenant la plupart des informations proposée par la loi RGPD (nom du responsable de traitement, nom du sous-traitant éventuel, type de traitement, finalité, interlocuteurs, base légale, catégories de données, catégories de personnes concernées …).

Pour CIS Valley :

Bien que la responsabilité de recensement des données à caractère personnel soit positionnée côté client en sa qualité de responsable de traitement, CIS Valley peut proposer au client un accompagnement méthodologique et technique sur cette collecte.

De son côté, CIS Valley identifie les traitements courants proposés à ses clients et adapte les mesures de sécurité afin de protéger les données à caractère personnel. Les traitements courants sont :

- Stockage primaire de données
- Réplication/miroir de données
- Sauvegarde des données
- Externalisation des sauvegardes
- Restauration de données
- Traçabilité des connexions nominatives sur les environnements systèmes (notamment pour l'hébergement de données de santé)

Au-delà, le client en tant que responsable de traitement doit fournir à CIS Valley les fiches des traitements qu'il lui confie et formaliser des consignes pour la mise en œuvre de ces traitements. La fourniture de ces fiches concerne à la fois les traitements existants et les traitements à venir. Dans le cadre de la loi, CIS Valley ne peut intervenir que sur instruction documentée du client.

Identification des données sensibles et analyse d'impact

Des mesures particulières peuvent s'appliquer si les traitements répondent aux caractéristiques ci-dessous (exemple : étude d'impact sur la protection des données, information renforcée, recueil du consentement, autorisation préalable, clauses contractuelles,…). Le responsable de traitement doit se préoccuper de ces cas de figure.

Vous traitez certains types de données

- des données qui révèlent l'origine prétendument raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale,
- des données concernant la santé ou l'orientation sexuelle,
- des données génétiques ou biométriques,
- des données d'infraction ou de condamnation pénale,
- des données concernant des mineurs.

Votre traitement a pour objet ou pour effet

- la surveillance systématique à grande échelle d'une zone accessible au public ;
- l'évaluation systématique et approfondie d'aspects personnels, y compris le profilage, sur la base de laquelle vous prenez des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative.

Vous transférez des données hors de l'Union européenne

- vérifiez que le pays vers lequel vous transférez les données est reconnu comme adéquat par la Commission européenne.
- dans le cas contraire, encadrez vos transferts.

Mesures de sécurité de CIS Valley

CIS Valley propose d'emblée des mesures de sécurité pour la protection des données

- Cloisonnement des réseaux
- Protection antivirale
- Mise à jour de patchs systèmes
- Sauvegarde
- …

Phase d'évaluation de la charge

Afin d'obtenir une évaluation de la charge des prestations liées à la RGPD que le client souhaite confier à CSI Valley, nos ingénieurs avant-vente demandent aux clients :

- La liste, le positionnement et le niveau de sensibilité des données
- La liste et les fiches des traitements confiés à CIS Valley
- Le niveau de sécurité attendu pour la protection des données

Mesures de sécurité spécifiques pour le client

A l'issue de la constitution de son registre et des éventuelles analyses d'impact, le client doit fournir à CIS Valley les fiches des traitements qu'il lui confie et les consignes associées.

Au vu des fiches des traitements fournies par le client, du niveau de sensibilité des données, du contexte dans lequel les données sont utilisées, des résultats des analyses d'impact, il peut être nécessaire d'envisager des mesures de sécurité complémentaires sur certains biens. Suivant la répartition des

responsabilités entre le client et CIS Valley, le déploiement des mesures de sécurité sera sous la responsabilité d'un des deux acteurs.

Maintien de la sécurité

En phase d'exploitation des systèmes d'information, les changements opérés sur les équipements peuvent compromettre l'efficacité des mesures de sécurité appliquées.

Les processus en place chez CIS Valley permettent de maintenir la sécurité des infrastructures et des services communément proposés au client grâce à :

- Des actes d'exploitation, de surveillance
- Du pilotage des indicateurs de suivi
- Des audits internes et plans d'actions associés

La description des services mutualisés et spécifiques liés au client est effectuée dans le plan d'assurance qualité en phase d'exploitation (PAQ RUN). Ce document consigne l'ensemble des actes à opérer pour un client spécifique. Ces actes sont ensuite planifiés et tracés.

Mise à disposition et restitution des données hébergées

La restitution de données hébergées pour le client est encadrée pour garantir la sécurité des données. Deux méthodes de transfert d'informations sont possibles :

Transfert via disque dur externe : Un chiffrement du disque externe est opéré en amont pour garantir la sécurité des données pendant leur transit. Dans le cas d'une réversibilité, un disque externe dédié au client est utilisé pour la restitution des données.

Transfert via le réseau : Les infrastructures de sauvegarde et de réplication à distance disponibles chez CIS Valley peuvent être utilisées pour récupérer ou restituer les données aux clients. Les données en transit sont systématiquement chiffrées.

La méthode à sélectionner est convenue avec le client en fonction de la taille des données à transférer et des bandes passantes disponibles sur les liens de télécommunication.

Ce tableau présente les méthodes utilisables suivant les cas :

Mises à disposition des données	Transfert via disque dur externe ou via le réseau
Restitution des données	Transfert via disque dur externe uniquement

Destruction des données hébergées

Les enveloppes des machines virtuelles présentes sur les espaces de stockage des baies de disques sont supprimées.

Les données stockées dans les sauvegardes sont supprimées en dehors de celles présentes sur les cartouches mutualisées.

En cas de décommissionnement de matériel, les biens contenant de la donnée de santé à caractère personnel sont rendus inutilisables avant mise au rebut. C'est ainsi que les disques des baies de disques et les cartouches de sauvegarde sont détruits avant leur recyclage. La destruction de ces données à caractère personnel est encadrée comme suit :

- Surveillance de la liste des disques à détruire.

- Destruction des disques et stockage avant mise au rebus.

- Validation des opérations par le RSSI.

Sous-traitance

Dans le cas où CIS Valley souhaiterait sous-traiter les traitements qui lui sont confiés, il préviendrait le client par écrit et s'assurerait de la capacité du sous-traitant à protéger les données dudit client.

3. La communication

Relation avec les autorités

En cas d'incident avéré sur les données à caractère personnel, le responsable de traitement doit notifier la violation à l'autorité de contrôle compétente dans les meilleurs délais et, si possible, dans les 72 heures après avoir pris connaissance (article 33 de la loi RGPD).

Si l'incident est détecté par CIS Valley, il en informe le client dans les meilleurs délais après en avoir pris connaissance (article 33 de la loi RGPD).

Demandes des personnes intéressées

Les personnes intéressées par les données à caractère personnel doivent pouvoir exercer leurs droits d'informations et d'accès aux données personnelles, droit de rectification et d'effacement, droit à la limitation du traitement des données, droit à la portabilité, droit d'opposition.

Ces personnes s'adressent au responsable de traitement. CIS Valley se met à disposition du client (en réaction à l'ouverture par le client d'un ticket de demande dans notre outil dédié à la gestion des incidents et des demandes) et lui fournit toutes les informations en sa possession. Dans le périmètre de responsabilité des traitements qui lui sont confiés, CIS Valley opère les changements qui sont réclamés par le client.

Historique des mises à jour de la politique

Date	Objet des modifications	Version
15/02/2018	Initialisation du document	V01
09/10/2019	Ajout de la politique de mise à disposition et restitution des données hébergées	V02