wizville

Politique de traitement des données

Applicable à partir du 1er Juin 2022

Table des matières

1. Portée de la Politique de traitement des données

La présente Politique de traitement des données s'applique à l'ensemble des traitements de données réalisés pour le compte de ses clients par **WIZVILLE**, société par actions simplifiée au capital de 936,25 €, dont le siège social se situe au 51, rue de Chabrol - 75010 Paris, immatriculée au registre du commerce et des sociétés sous le numéro unique d'identification 751 226 606 R.C.S. PARIS.

Elle s'applique à tout contrat (ci-après le « Contrat ») portant sur la solution logicielle WizVille et/ou la suite **TrustVille** (ci-après la « Solution ») conclu entre **WIZVILLE** et le client (ci-après le « Client ») comportant des traitements de données, et notamment des traitements de données à caractère personnel du Client ou de ses propres clients (ci-après les « Clients Finaux »).

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après « RGPD ») et les dispositions de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

À ce titre, **WIZVILLE** intervient en qualité de sous-traitant du Client au sens du RGPD.

Le Client autorise expressément **WIZVILLE**, agissant en qualité de sous-traitant, à traiter pour son compte les données à caractère personnel nécessaires pour l'utilisation de la Solution.

La finalité du traitement des données est de permettre le suivi de la satisfaction des Clients Finaux ayant accepté de recevoir des sollicitations par courrier électronique, dans le cadre de leur utilisation des produits et services du Client.

Les catégories de personnes concernées sont :

- Les Clients Finaux, personnes physiques, ayant utilisé les produits et services du Client, ayant accepté de recevoir des sollicitations par courrier électronique, SMS, web ou push notification mobile, et ayant rempli un questionnaire de satisfaction ;
- Les collaborateurs du Client accédant à la Solution.

WIZVILLE s'engage à :

- Traiter les données uniquement pour la ou les seule(s) finalité(s) prévue(s) ci-avant,
- Traiter les données conformément aux instructions du Client. Si **WIZVILLE** considère qu'une instruction constitue une violation du RGPD ou de toute autre disposition du droit de l'Union ou du droit des États membres relative à la protection des données personnelles, elle en informe immédiatement le responsable de traitement. En outre, si **WIZVILLE** est tenue de procéder à un transfert de données vers un pays tiers, en vertu du droit de l'Union ou du droit de l'État membre

auquel elle est soumise, elle doit informer le Client de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.
- Garantir la confidentialité des données traitées dans le cadre du Contrat.
- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du Contrat :
    - o s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité,
    - o reçoivent la formation nécessaire en matière de protection des données,
- Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut.

Le Client s'engage à :

- Recueillir le consentement des Clients Finaux sur l'utilisation de leurs données à caractère personnel et le traitement qui en est fait dans le cadre de l'utilisation de la Solution (ou à s'assurer de la légitimité de la collecte et du traitement des données à caractère personnel ainsi que de la mise en place de mesures compensatoires, le cas échéant, en cas de collecte et de traitement fondé sur l'intérêt légitime du Client),
- Garantir **WIZVILLE** contre les préjudices directs consécutifs à la transmission par le Client de données à caractère personnel sans base légale ;
- Documenter par écrit toute instruction donnée à **WIZVILLE** concernant le traitement des données à caractère personnel confiées à cette dernière,
- Informer **WIZVILLE** de toute demande d'un Client Final relative au traitement de ses données personnelles dans les plus brefs délais.

WIZVILLE se réserve le droit d'apporter à la présente Politique de traitement des données toutes les modifications qu'elle jugera utiles et nécessaires, notamment en considération d'éventuelles évolutions légales, jurisprudentielles ou techniques.

En cas de projet de modification de la présente Politique de traitement des données, le Client sera informé au minimum trente (30) jours avant l'entrée en vigueur des projets de modifications et pourra au cours de ce délai faire part de ses observations ou de son refus des modifications envisagées.

2. Catégories de données collectées

L'utilisation de la Solution implique la collecte et le traitement des données du Client et/ou des Clients Finaux suivantes :

Catégories	Types
Données personnelles directes	Nom
	Prénom
	Adresse email
	Numéros de téléphone (fixe ou mobile)
	Date de naissance
	Numéro de client
Données personnelles indirectes	Civilité
	Catégorie client (VIP, Nouveau…)
Données transactionnelles	Date de transaction
	Montant transaction
	Type de transaction (achat, prestation, livraison, appel, contact, visite…)
	Produits ou services concernés par les transactions et toutes leurs caractéristiques
	Agence, point de vente ou point de contact lié à la transaction
	Numéro unique de transaction
Données personnelles des collaborateurs du Client	Email collaborateur
	Rôle du collaborateur

3. Modalités et délais de conservation des données collectées

Sauf instructions contraires du Client (agissant en qualité de responsable du traitement), les données collectées et traitées par **WIZVILLE** sont conservées selon les modalités et les délais suivants :

A. Données relatives aux Clients Finaux

- Les Données personnelles directes, les Données personnelles indirectes et les Données transactionnelles relatives à un Client Final sont conservées pendant un délai de vingt-quatre (24) mois à compter de leur transmission par le Client ; toute nouvelle transmission de données relatives à un Client Final par le Client dans ce délai fait courir un nouveau délai de vingt-quatre (24) mois avant la mise en œuvre des opérations d'anonymisation des données.

- En l'absence de transmission de nouvelles données concernant un Client Final par le Client dans le délai de vingt-quatre (24) mois susvisé, **WIZVILLE** procède à une opération d'anonymisation irréversible consistant à :
    - Supprimer de ses bases de données les Données personnelles directes du Client Final ;
    - Conserver uniquement, sans limite de temps, les Données personnelles indirectes et les Données transactionnelles, ne permettant pas à **WIZVILLE** d'identifier le Client Final concerné.

B. Données personnelles des collaborateurs du Client

- Les **Données personnelles des collaborateurs du Client** et les **Données de navigation web** sont conservées pendant toute la durée du Contrat ;
- En cas de résiliation ou d'expiration du Contrat, les Données personnelles des collaborateurs du Client et les Données de Navigation web sont définitivement supprimées dans un délai de trente (30) jours calendaires.

4. Assistance du Client pour l'exercice des droits des Clients Finaux

WIZVILLE s'engage à assister le Client pour l'exercice des droits des Clients Finaux, dans les conditions suivantes :

Droits du Client Final	Délais
Droit d'accès	Contact via e-mail à data@wizville.fr
	Extraction des données en format CSV sous 48h
Droit de rectification	Contact via e-mail à data@wizville.fr
	Modification des données sous 48h
Droit à l'oubli et à l'effacement	Contact via e-mail à data@wizville.fr
	Suppression des données de la base active sous 48h
	Suppression des données sauvegardées et archivées sous 30 jours
Droit à la limitation du traitement	Contact via e-mail à data@wizville.fr
	Limitation du traitement des données sous 7 jours
Droit de notification	Contact via e-mail à data@wizville.fr
	Notification aux tiers sous 48h
	Confirmation au Client sous 72h

Droit de portabilité des données	Contact via e-mail à data@wizville.fr
	Extraction des données en format CSV sous 5 jours
	Communication des données en format CSV sous 7 jours

Lorsque les demandes d'exercice de droits sont transmises directement à **WIZVILLE** par les Clients Finaux, **WIZVILLE** exécute les demandes puis en informe le Client sous 48h.

5. Sauvegarde des données et rétablissement

Les données du Client, en ce compris les données personnelles des Clients Finaux, sont hébergées chez **IGUANE SOLUTIONS**, qui assure :

- Un dispositif de monitoring des serveurs ;
- Une notification en cas d'incident ;
- Une sauvegarde redondante des données sur un serveur séparé toutes les 24 h avec possibilité d'accéder aux sauvegardes antérieures en cas difficulté sur une durée de 30 jours ;
- Un rétablissement des accès aux données dans un délai maximum de 4 heures (du lundi au vendredi aux heures ouvrées) et de 6 h (week-end, nuit et jours fériés) sauf cas de force majeure.

En cas d'indisponibilité du serveur actif, un serveur de secours est activé dans un délai maximum de 4 heures sauf cas de force majeure.

Par ailleurs, certaines données documentaires peuvent être hébergées sur le service Google Cloud (prestataire d'hébergement documentaire – PDF, fichiers Excel et images envoyés à et générés par la Solution).

6. Sécurité des données

WIZVILLE assure la sécurité des données communiquées par le Client en mettant en œuvre les moyens suivants :

A. Sécurité physique

Les données du Client sont hébergées sur un serveur distant géré par la société **IGUANE SOLUTIONS**[1] et hébergé par la société **SCALEWAY (ILIAD)**, dans un data center (**DC3**) sécurisé, situé en France, à Vitry-sur-Seine, à la date des présentes. Ces données sont susceptibles d'être hébergées dans d'autres data centers exploités par **IGUANE SOLUTIONS** et situés en France.

IGUANE SOLUTIONS assure la sécurité physique des serveurs 24 h/24 et 7j/7.

[1] 1 IGUANE SOLUTIONS, société par actions simplifiée au capital de 244 760,80 euros, immatriculée au RCS de Paris sous le numéro B 432 269 165, dont le siège social est sis 17, rue de Surène, 75008 Paris.

L'accès aux centres de données est strictement contrôlé et surveillé.

La sécurité est gérée par :

- Une présence permanente de gardes de sécurité (24h/24 et 7j/7) ;
- Un accès limité aux seuls salariés d'**IGUANE SOLUTIONS** ou de **WIZVILLE** devant accéder physiquement aux serveurs informatiques ;
- Des accès contrôlés par badge et scanners biométriques ;
- Une surveillance vidéo 24 h /7 ;
- Des salles équipées de systèmes de détection de fumée et d'humidité ;
- Un personnel technique présent 24 h /7.

Le data center (**DC3**) dispose des certifications suivantes :

- Certification **ISO 27001**, garantissant la mise en œuvre effective d'un système de management de la sécurité de l'information (maîtrise des risques et gestion de la sécurité de l'information) ;
- Certification **ISO 50001** (ENMS609673), garantissant la mise en œuvre effective d'un système de management de l'énergie optimisé ;
- Certification **TIER III Design** délivré par **Uptime Institute** (2014), garantissant que la topologie physique de l'infrastructure du centre de données évite les risques de pénurie ou de liens faibles ;
- **Norme PCI-DSS** (en cours d'acquisition), permettant d'assurer la conformité des infrastructures réseau à la norme de sécurité **PCI DSS** en matière de sécurité des données pour l'utilisation de cartes de paiement.

Les données documentaires hébergées sur Google Cloud dépendent de data centers exploités par **GOOGLE IRELAND LIMITED** et situés en Union Européenne, hors de France. A la date des présentes, ces data centers sont situés dans les villes et pays suivants :

- St. Ghislain, Belgique
- Frankfurt, Allemagne
- Eemshaven, Pays Bas

Les données sont susceptibles d'être hébergées dans d'autres data centers exploités par **GOOGLE IRELAND LIMITED** situés en Union Européenne.

B. Sécurité serveur

Les accès aux serveurs sont sécurisés par des processus d'authentification forts grâce à une politique stricte de gestion des mots de passe et le déploiement de mesures de double authentification (clefs SSH privées et sécurisées).

Les serveurs utilisés pour la Solution ne sont pas adressables directement sur Internet.

Seuls les membres du personnel de **WIZVILLE** habilités ainsi que les collaborateurs du Client ont accès aux données.

Les transferts de données du Client à **WIZVILLE** se font au moyen d'un serveur SFTP impliquant le chiffrement des échanges de données, avec un login et mot de passe.
Les transferts de données réalisés par **WIZVILLE** à ses sous-traitants sont réalisés au moyen du protocole HTTPs.

Les données du Client ne sont jamais conservées sur des périphériques USB, des CD, des DVD ou tout autre type de périphérique de stockage amovible.

Le chiffrement au niveau du disque est activé sur tous les postes de travail, ordinateurs portables et appareils mobiles utilisés par le personnel de **WIZVILLE**, avec identification par login et mot de passe.

C. Sécurité Client

L'accès à la Solution est sécurisé en HTTPs avec un login et un mot de passe.

La création des mots de passe des collaborateurs du Client est réalisée au moyen d'un courrier électronique adressé directement sur la ou les adresses email fournie(s) par le Client.

Les collaborateurs du Client peuvent créer des mots de passe avec des critères de force minimale.

Les connexions du Client au moyen de ses login/mot de passe font l'objet d'un suivi, sont horodatées et enregistrées.

La Solution offre des fonctionnalités de gestion des droits d'utilisateur précises, garantissant que les collaborateurs du Client ne peuvent accéder qu'aux données auxquelles ils doivent avoir accès.

D. Protection contre les attaques, les virus informatiques et les logiciels malveillants

Les accès aux serveurs sont protégés par un dispositif *fail2ban* en cas de tentative répétée d'accès aux serveurs sans les accès adaptés.

WIZVILLE utilise également des dispositifs de sécurité, tels que pare-feu, etc. Le pare-feu filtre le trafic entrant, assurant la sécurité du périmètre et empêchant l'accès non autorisé à partir d'Internet. Il intègre également des mécanismes de prévention d'intrusion.

Le réseau et le fonctionnement de la Solution font l'objet d'une surveillance permanente. La surveillance comprend des alertes en temps réel en cas de tentative d'intrusion.

7. Gestion des incidents

La procédure de gestion des incidents de **WIZVILLE** comprend les étapes suivantes :

1. Alertes : Les équipes support de **WIZVILLE** sont informées de l'incident soit par les outils de surveillance des serveurs, soit par les outils de surveillance de la Solution, soit par les collaborateurs du Client.

2. Identification : Les équipes support de **WIZVILLE** déterminent les conditions de survenance de l'incident et ses impacts sur la Solution, les serveurs et les données. Si cela s'avère nécessaire, ils tentent de reproduire l'incident sur un environnement de test. Lorsque la survenance de l'incident a été détectée par le Client, ce dernier doit fournir à **WIZVILLE** l'ensemble des données en sa possession pour permettre de reproduire l'incident.

3. Isolement : Les équipes support s'assurent de limiter l'impact de l'incident en bloquant son éventuelle propagation et en protégeant les données.

4. Sauvegarde : Les équipes support procèdent à des sauvegardes afin de préserver des preuves de l'incident et de ses conséquences pour l'investigation.

5. Investigation : Les équipes support étudient les incidents et vérifient les ressources qui ont été volées, altérées ou détruites, ainsi que la durée des incidents. Cette phase permet notamment de qualifier la gravité de l'incident et d'écarter d'éventuelles anomalies sans conséquences.

6. Traitement : Les équipes support restaurent les systèmes touchés le cas échéant, ou les retirent. Des outils de vérification sont utilisés pour vérifier que le risque de renouvellement de l'incident est limité ou écarté.

7. Restauration : La Solution, les serveurs ou les données sont restaurés et l'intégrité du système est vérifiée et testée.

8. Reporting : Les équipes support établissent un rapport complet de l'incident, comprenant la date et l'heure de survenance, les informations contenues dans les registres, les systèmes ou données affectés. Ce rapport comprend notamment les modalités de résolution de l'incident mises en œuvre, leur caractère pérenne ou temporaire et le risque de reproductibilité de l'incident.

9. Amélioration : Lorsque cela s'avère nécessaire, la Solution fait l'objet d'une mise à jour documentée afin d'éviter le renouvellement de l'incident.

8. Violation de sécurité

WIZVILLE notifie au Client toute violation de sécurité des données dans un délai maximum de 48 heures ouvrées après en avoir pris connaissance et par courrier électronique.

Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

La notification contient les informations suivantes :

- La description de la nature de la violation de données y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données concernés ;
- Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- La description des conséquences probables de la violation de données ;
- La description des mesures prises ou à prendre pour remédier à la violation de données, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

9. Restitution des données

À l'expiration du Contrat, les données du Client sont restituées dans leur ensemble à ce dernier par **WIZVILLE** dans un délai de trente (30) jours, dans le ou les formats d'export disponibles dans la solution **WIZVILLE**, et sans surcoût. À date, le format disponible est le format Excel, « .xslx » ou « .xls».

Elles sont supprimées de la base de données active dans le même délai.

Elles sont supprimées des sauvegardes archivées dans un délai de trente (30) jours.

La suppression des données de sauvegarde est rendue irréversible par la réécriture des secteurs des disques utilisés.

A l'issue des délais susvisés, **WIZVILLE** :

- Procède à un test de suppression des données, confirmant que les données supprimées ne peuvent être intégralement ou partiellement reconstituées au moyen d'un logiciel de reconstitution de données ;
- Fournit au Client une attestation écrite de destruction ;
- Conserve les détails des opérations de restitution et de suppression, ainsi que les rapports de tests, qui sont enregistrés et conservés.

10. Transferts de données hors Union Européenne

Les données du Client sont hébergées en France et en Union Européenne et ne sont pas transférées hors de l'Union Européenne, sauf demande spécifique du Client et sous réserve des règles applicables, conformément au RGPD.

11. Sous-traitance

À la date des présentes, **WIZVILLE** fait appel aux sous-traitants suivants pour le traitement des données qui lui sont confiées par le Client :

Sous-traitants	Finalité
Mailjet 13-13 bis, rue de l'Aubrac – 75012 Paris, France RCS Paris 524 536 992 00059	Prestataire d'envoi d'emails
SINCH (ex-CLX) Sinch Sweden AB, Legal Dept. Lindhagensgatan 74, 112 18 Stockholm, Sweden	Prestataire d'envoi de SMS
IGUANE SOLUTIONS 17 RUE DE SURENE 75008 PARIS SIRET : 43226916500051	Hébergeur des données
SCALEWAY (ILIAD) 8 RUE DE LA VILLE L EVEQUE 75008 PARIS SIRET : 43311590400057	Gestion du datacenter pour IGUANE SOLUTIONS
Google Cloud BARROW STREET 99132 DUBLIN SIRET : 79976916100016	Hébergeur de données documentaires

En cas de changement de sous-traitant, **WIZVILLE** s'engage à en informer le Client préalablement, en précisant les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance.

Le Client dispose d'un délai minimum de trente (30) jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le Client n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant de **WIZVILLE** est tenu de respecter les obligations des présentes pour le compte et selon les instructions du Client. Il appartient à **WIZVILLE** de s'assurer que ses sous-traitants présentent les garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences de la législation en vigueur.

Si un sous-traitant de **WIZVILLE** ne remplit pas ses obligations en matière de protection des données, cette dernière demeure pleinement responsable à l'égard du Client de ses obligations.

12. Délégué à la Protection des Données (DPO)

WIZVILLE a désigné en qualité de Délégué à la Protection des Données (DPO) :

- Le cabinet **SMARTUP AVOCATS**, société à responsabilité limitée au capital de 30.000 €, dont le siège social est situé 3, rue Anatole de la Forge – 75017 Paris, immatriculée au registre du commerce et des sociétés sous le numéro unique d'identification 821 811 700 R.C.S. PARIS.

Le Délégué à la Protection des Données peut être contacté à l'adresse suivante :
contact@smartup-avocats.fr

13. Registre des activités de traitement

WIZVILLE déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Client comprenant :

- Le nom et les coordonnées du responsable de traitement pour le compte duquel elle agit,
- Les catégories de traitements effectués pour le compte du Client,
- Si le Client l'autorise au préalable, les transferts de données vers un pays tiers, y compris l'identification de ce pays tiers et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du RGPD, les documents attestant de l'existence de garanties appropriées ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
    - La pseudonymisation et le chiffrement des données à caractère personnel ;
    - Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
    - Des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
    - Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

14. Procédure d'analyse d'impact préalable

À la demande du Client, sauf disposition contractuelle contraire entre le Client et **WIZVILLE**, et sous réserve de l'accord de ce dernier sur les conditions financières applicables, **WIZVILLE** participe à toute analyse d'impact préalable. À date, les taux journaliers moyens de **WIZVILLE** pour cette prestation sont de 800€ HT.

À défaut de procédure spécifique du Client, la procédure mise en place par WIZVILLE comprend les étapes suivantes :

1. **Étude du contexte**

Cette phase consiste à identifier les traitements de données personnelles considérés en :

- Présentant le traitement considéré, sa nature, sa portée, son contexte, ses finalités et ses enjeux de manière synthétique ;
- Identifiant le responsable du traitement et les éventuels sous-traitants ;
- Recensant les référentiels applicables au traitement, utiles ou à respecter, notamment les codes de conduite approuvés (art. 40 du RGPD) et certifications en matière de protection des données (art. 42 du RGPD) ;
- Délimitant et décrivant le périmètre de manière détaillée :

    - Les données personnelles concernées, leurs destinataires et durées de conservation ;
    - Une description des processus et des supports de données pour l'ensemble du cycle de vie des données (depuis leur collecte jusqu'à leur effacement).

2. **Étude des principes fondamentaux**

Cette phase consiste à bâtir le dispositif de conformité aux principes de protection de la vie privée en :

- Évaluant les mesures garantissant la proportionnalité et la nécessité du traitement, impliquant de :
    - Expliciter et justifier les choix effectués pour respecter les exigences suivantes :
        - Finalité : déterminée, explicite et légitime (art. 5.1 (b) du RGPD) ;
        - Fondement : licéité du traitement, interdiction du détournement de finalité (art. 6 du RGPD) ;
        - Minimisation des données : adéquates, pertinentes et limitées (art. 5.1 (c) du RGPD) ;
        - Qualité des données : exactes et tenues à jour (art. 5.1 (d) du RGPD) ;
        - Durée de conservation : limitée (art. 5.1 (e) du RGPD).

    - Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer la manière dont chaque point est prévu, explicité et justifié, conformément au RGPD ;

- Le cas échéant, revoir leur description ou proposer des mesures complémentaires.

- Évaluant les mesures protectrices des droits des personnes concernées, impliquant de :

  - Identifier ou déterminer, et décrire, les mesures retenues (existantes ou prévues) pour respecter les exigences suivantes (nécessitant d'expliquer comment il est prévu de les mettre en œuvre) :

    - Information des personnes concernées (traitement loyal et transparent, art. 12, 13 et 14 du RGPD) ;
    - Recueil du consentement, le cas échéant : exprès, démontrable, retirable (art. 7 et 8 du RGPD) ;
    - Exercice des droits d'accès et à la portabilité (art. 15 et 20 du RGPD) ;
    - Exercice des droits de rectification et d'effacement (art. 16 et 17 du RGPD) ;
    - Exercice des droits de limitation du traitement et d'opposition (art. 18 et 21 du RGPD) ;
    - Sous-traitance : identifiée et contractualisée (cf. art. 28 du RGPD) ;
    - Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne (art. 44 à 49 du RGPD).

  - Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer chaque mesure et sa description, conformément au RGPD ;

  - Le cas échéant, revoir leur description ou proposer des mesures complémentaires.

3. Étude des risques liés à la sécurité des données

Cette phase consiste à identifier les risques et leurs conséquences en matière de sécurité des données et à évaluer les mesures de sécurité existantes ou prévues, afin d'obtenir une bonne connaissance des mesures contribuant à la sécurité, en :

- Déterminant les types de risques auxquels les données peuvent être confrontées (accès illégitime à des données, modification non désirée de données, disparition de données) ;

- Appréciant comment pourraient être exploitées les vulnérabilités des supports de données ;

- Identifiant les données susceptibles d'être compromises ;

- Appréciant la gravité du risque en considération de son ampleur et du caractère préjudiciable des impacts potentiels ;

- Estimant les impacts éventuels sur la vie privée des personnes concernées et l'utilisation qui

pourrait être faite des données compromises, impliquant de :

- Déterminer les impacts potentiels sur la vie privée des personnes concernées s'ils survenaient ;
- Estimer leur gravité, notamment en fonction du caractère préjudiciable des impacts potentiels et, le cas échéant, des mesures susceptibles de les modifier ;
- Identifier les menaces sur les supports des données et les sources de risques qui pourraient en être à l'origine ;
- Estimer leur vraisemblance, notamment en fonction des vulnérabilités des supports de données, des capacités des sources de risques à les exploiter et des mesures susceptibles de les modifier.

- Identifiant ou déterminant les mesures existantes ou prévues (déjà engagées), qui peuvent être de trois natures différentes :

  - Mesures portant spécifiquement sur les données du traitement : chiffrement, anonymisation, cloisonnement, contrôle d'accès, traçabilité, etc. ;
  - Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre : sécurité de l'exploitation, sauvegardes, sécurité des matériels, etc. ;
  - Mesures organisationnelles (gouvernance) : politique, gestion des projets, gestion des personnels, gestion des incidents et violations, relations avec les tiers, etc.

- Vérifiant qu'il n'est pas utile, ou pas possible, d'améliorer chaque mesure et sa description, conformément aux bonnes pratiques de sécurité ;
- Le cas échéant, précisant leur description ou proposant des mesures complémentaires ;
- Déterminer si les risques ainsi identifiés peuvent être jugés acceptables compte tenu des mesures existantes ou prévues ;
- Dans la négative, proposant des mesures complémentaires et réestimant le niveau de chacun des risques en tenant compte de celles-ci, afin de déterminer les risques résiduels.

4. Validation du Privacy Impact Assessment (PIA)

Cette phase permet de décider d'accepter ou non le PIA au regard des résultats de l'étude, en :

- Consolidant et mettant en forme les résultats de l'étude, impliquant :
  - D'élaborer une représentation visuelle des mesures choisies pour respecter les principes fondamentaux, en fonction de leur conformité au RGPD ;
  - D'élaborer une représentation visuelle des mesures choisies pour contribuer à la sécurité des données, en fonction de leur conformité aux bonnes pratiques de sécurité ;
  - D'élaborer une cartographie visuelle des risques résiduels en fonction de leur gravité et vraisemblance ;
  - D'élaborer un plan d'action à partir des mesures complémentaires identifiées lors des

étapes précédentes et, pour chaque mesure, de déterminer au moins le responsable de sa mise en œuvre, son coût (financier et/ou en termes de charge) et son échéance prévisionnelle.

- Formalisant la prise en compte des parties prenantes :
    - Le conseil du délégué à la protection des données (art. 35 (2) du RGPD) ;
    - L'avis des personnes concernées ou de leurs représentants, le cas échéant (art. 35 (9) du RGPD).

- Validant formellement le PIA, en décidant de l'acceptabilité des mesures choisies, des risques résiduels et du plan d'action, de manière argumentée, au regard des enjeux préalablement identifiés et de l'avis des parties prenantes ;

- Ou, le cas échéant, en exécutant à nouveau les étapes précédentes pour que le PIA puisse être validé.