POLITIQUE DE PROTECTION DES DONNEES PERSONNELLES

GROUPE IDEX

Version 1.0

Octobre 2018

Version	Date	Rédacteur	Commentaires
1.0	04/09/2018	DPO	Version validée en Comité de Gouvernance des Données Personnelles du 13/12/18

POLITIQUE DE PROTECTION DES DONNEES PERSONNELLES

Le présent document a pour référentiel d'application les textes législatifs et réglementaires suivants :

- **Le règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016** relatif à la protection des personnes physiques à l'égard du Traitement des données à caractère personnel et à la libre circulation de ces données abrogeant la directive 95/46/CE ;

- **la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données ;

- **La loi n°78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés modifiée en dernier lieu par **la loi n° 2018-493 du 20 juin 2018** relative à la protection des données personnelles.

1. INTRODUCTION

1.1. Contexte

IDEX est attachée à la protection de la vie privée et des données à caractère personnel (« Données à Caractère Personnel », « Données Personnelles », « Données ») de ses contacts (établis dans le cadre de dossiers, missions, partenariats, prestations, rencontres professionnelles, candidatures, utilisateurs de son site internet, etc.) et s'applique à mettre en œuvre ainsi qu'à respecter une politique de Traitement des Données conforme à la réglementation en vigueur.

Les Données Personnelles déclaratives sont celles fournies par les Personnes Concernées (« Personnes Concernées » ou « Personnes ») via des formulaires, qu'ils soient dématérialisés via le site internet, sous format papier ou en réponse à des questions qui ont été posées par IDEX.

La présente Politique de Protection des Données Personnelles (la « Politique ») a pour objet d'informer de manière claire, simple et complète sur la manière dont IDEX, en sa qualité de Responsable de Traitement, collecte, conserve et utilise les Données Personnelles et sur les moyens dont les Personnes Concernées disposent pour contrôler cette utilisation et exercer leurs droits.

Dans la continuité de ses valeurs et pratiques responsables, IDEX met en œuvre ces nouvelles mesures et renforce ainsi la protection des Données Personnelles des Personnes Concernées. Il s'engage à fournir toutes les preuves de conformité exigibles par les autorités de contrôle (ex. : registre des Traitements, études d'impact sur la vie privée, procédure de gestion des droits des Personnes Concernées, mesures de sécurité techniques et organisationnelles, etc.).

1.2. Périmètre et objectifs

IDEX a pour objectif de se conformer aux lois applicables en matière de protection de la vie privée d'une manière transparente et fiable. Dans cette mesure, la Politique souligne la façon dont les principes et les droits en matière de confidentialité sont pris en compte au sein d'IDEX.

IDEX vise à assurer :

- Le respect et la protection des Données Personnelles des Personnes Concernées en se conformant au RGPD et aux lois locales applicables ;
- Que les principes et la Politique de protection des Données soient pris en compte dans chaque activité (à titre d'exemple : tout nouveau projet est porté à la connaissance du DPO).

La Politique de Protection des Données Personnelles permet aux membres d'IDEX de connaître les exigences à respecter en matière de Traitement des Données Personnelles et, par conséquent, réduire le risque de :

- Non-respect des exigences légales en raison d'un manque de règles claires à suivre, ce qui peut entraîner des amendes ou des poursuites administratives et nuire à la réputation de la marque d'IDEX ;
- D'actions malencontreuses en raison de l'incertitude des salariés d'IDEX quant à la bonne démarche à suivre.

La Politique de Protection des Données Personnelles s'applique à toutes les Données Personnelles traitées par IDEX ou par des Sous-traitants chargés de traiter les Données Personnelles au nom et pour le compte d'IDEX.

1.3. Données Personnelles

Le terme Données Personnelles renvoie à toute information relative à une personne. Une Personne Concernée peut être, par exemple, un salarié, un stagiaire, un fournisseur, un sous-traitant, un candidat, un prospect, un client ou le représentant d'une personne morale.

Il peut s'agir d'une personne qui pourrait être identifiée directement (ex. nom, numéro de sécurité sociale, adresse) ou grâce à son identité physique, physiologique, économique, culturelle ou sociale.

Les Données Personnelles qu'IDEX possède concernent les catégories suivantes :

- Données d'identification ;
- Vie professionnelle ;
- Vie personnelle ;
- Données de connexion ou de localisation ;
- Données financières.

Les Données Personnelles restent des Données Personnelles indépendamment de leur nature, forme, stockage ou toute autre circonstance. Notamment, elles peuvent être :

- Chiffrées ou sécurisées (par exemple : dans un fichier protégé par un mot de passe) ;
- Disponibles publiquement (par exemple : des données rendues publiques sur les réseaux sociaux ou sur les sites internet). Le contexte de collecte ou de Traitement des données ne change pas le fait qu'il s'agisse de Données Personnelles ;
- Collectées par IDEX ou fournies par un tiers (par exemple : des données transmises par des clients dans le cadre des activités d'IDEX) ;
- Traitées pour le compte d'IDEX (par exemple : une société en charge du développement d'une application informatique).

1.4. Catégories spéciales de Données Personnelles

Les Données suivantes sont considérées comme sensibles :

- ID (CNI, passeport), carte vitale, attestation sécurité sociale, numéro de sécurité sociale, INSEE (enfant et conjoint), état de santé, taux d'incapacité, arrêt maladie, certificat médical, maladie professionnelle, infraction au code de la route, situation conflictuelle entre associés / collaborateurs / stagiaires / salariés ;

Le Traitement de ce type d'information est autorisé quand :

- Le consentement explicite de la Personne Concernée a été recueilli ;
- Il est nécessaire pour mener à bien des obligations contractuelles liées à l'emploi ou aux lois de protection et de sécurité sociales ;
- Il est nécessaire pour protéger les intérêts vitaux des Personnes Concernées ;
- Il est nécessaire pour des raisons juridiques (plainte, défense, etc.) ;
- Il est nécessaire pour la médecine préventive ou la médecine du travail, pour l'évaluation de la capacité de travail du salarié, pour l'exécution d'un contrat gouverné par le secret professionnel ;
- Il est nécessaire à des fins d'archivage, de recherche historique ou à des fins statistiques.

Ces Traitements doivent faire l'objet de mesures de sécurité organisationnelles et techniques appropriées, mises en évidence par une étude d'impact sur la vie privée.

1.5. Risques et enjeux

Le non-respect des obligations encadrées dans le RGPD lors des Traitements de Données Personnelles peut engager la responsabilité d'IDEX et engendrer des sanctions lourdes de conséquences.

Le défaut de conformité aux dispositions du RGPD entraine des sanctions graduelles, qui varient en fonction de la gravité des manquements constatés. Le RGPD met à la disposition de la CNIL différents moyens pour contraindre IDEX à se conformer au RGPD. La CNIL peut ainsi :

- Prononcer un avertissement ;
- Mettre en demeure IDEX ;
- Limiter temporairement ou définitivement un Traitement de données ;
- Suspendre les flux de données ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- Ordonner la rectification, la limitation ou l'effacement des données.

Après injonction de la CNIL, si les manquements demeurent, la CNIL peut prononcer à l'encontre d'IDEX les sanctions prévues par le RGPD qui sont de deux types :

Sanctions administratives

Les sanctions[1] sont extrêmement dissuasives :

- Jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial (ex : défaut de réalisation de EIVP, absence de registre des Traitements, défaut de sécurité des Traitements, etc.) ;
- Jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial (ex : défaut de recueil du consentement, défaut d'encadrement des transferts hors UE, non-respect des droits des personnes et des injonctions de la CNIL, etc.).

Dans les deux cas, c'est le montant le plus élevé qui est retenu.

Sanctions pénales

Les sanctions pénales[2] complètent les sanctions administratives en cas de violation du RGPD. Elles consistent à réprimander les violations qui ne font pas l'objet d'amendes administratives au sens de l'article 83 du RGPD, par exemple la possibilité pour la CNIL de prononcer une sanction pénale en cas de détournement de la finalité des Données Personnelles lors d'un Traitement de Données[3].

Ces sanctions peuvent aller jusqu'à 5 ans d'emprisonnement et 300 000 euros d'amende[4].

Par ailleurs, le RGPD prévoit la possibilité, pour une personne ayant subi un préjudice lié au non-respect de la règlementation en matière de protection des données, d'en demander la réparation[5] .

Par conséquent, les Sous-traitants devront s'engager formellement sur ces règles de sécurité et de conformité au RGPD mais, également, apporter tout document ou preuve de la mise en œuvre de procédures techniques et organisationnelles et accepter tout audit ou inspection diligentés par IDEX. La communication de Données Personnelles à un partenaire devra également respecter des règles de sécurité et de conformité au RGPD.

1.6. Définitions

Les termes dont la première lettre figure en majuscule ont, dans le présent document, le sens qui leur est attribué ci-dessous.

[1] Art. 83 du RGPD

[2] Art. 84.1 du RGPD

[3] Art. 226-21 du Code pénal

[4] Art. 226-16 du Code pénal

[5] Art.82 du RGPD

- « **Données Personnelles** » ou « **Données à Caractère Personnel** » ou « **DCP** » désigne toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant.

  Par exemple, un nom, numéro de téléphone, courriel, numéro d'identification, données de localisation, identifiant en ligne, ou un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

- « **DPO** » : Data Protection Officer ou DPD en français pour Délégué à la Protection des Données.

- « **Fichier** » : désigne tout ensemble structuré de Données Personnelles, accessible selon les critères déterminés dans le présent document, que cet ensemble soit centralisé, décentralisé, ou réparti de manière fonctionnelle ou géographique.

- « **Traitement** », toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel

  Par exemple, 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.

- « **Responsable de Traitement** » désigne 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 (article 4 RGPD) ; dans le cadre de cette politique, le responsable de Traitement est IDEX.

- « **Sous-Traitant** » : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données Personnelles pour le compte du Responsable du Traitement ; dans le cadre de cette procédure, le Sous-Traitant est le Prestataire.

- « **Transfert de données** » : toute communication, copie ou déplacement de DCP qui fera l'objet d'un Traitement dans le pays destinataire. Des dispositions spécifiques sont prévues si le pays destinataire n'est pas un état de l'Union européenne.

- « **Personne Concernée** » : Personne physique à laquelle se rapporte des DCP permettant d'identifier directement ou indirectement son état civil ou des aspects de sa personnalité.

- « **RGPD** » : le Règlement européen n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du Traitement des données à caractère personnel et à la libre circulation de ces données, Règlement Général sur la Protection des Données (dit « RGPD ou GDPR, pour General Data Protection Régulation en anglais »).
- « **CNIL** » : la Commission Nationale de l'Informatique et des Libertés est l'autorité chargée du contrôle du RGPD et de veiller au respect et à l'application conforme du RGPD.
- « **PSSI** » : la Politique de Sécurité des Systèmes d'Information décrit les règles du Groupe en matière de sécurité des systèmes d'Information.
- « **EIVP** » : l'Étude d'Impact sur la Vie Privée vise à identifier et à mesurer les risques d'un Traitement.
- « **PCA** » : le Plan de Continuité d'Activité a pour but de garantir la survie de l'entreprise après un sinistre important.

2. RESPONSABILITES D'IDEX ET DROITS DES PERSONNES CONCERNEES

Le RGPD prévoit de nombreuses obligations à la charge des Responsables de Traitement. A cet égard, IDEX doit préalablement à la mise en œuvre d'un Traitement de Données Personnelles tenir compte des principes du RGPD, à savoir :

2.1. Définir la finalité des Traitements

L'utilisation et le Traitement de Données Personnelles par IDEX doivent s'inscrire dans un but précis. La finalité indique à quoi les Données Personnelles collectées vont servir.

La finalité doit être déterminée, légitime et explicite[6]. Cette finalité doit être documentée et également communiquée aux personnes dont les Données Personnelles sont utilisées. Aucun Traitement de Données ne peut être entrepris sans une finalité spécifique, claire et compréhensible.

Selon les cas, les Données Personnelles pourront être utilisées dans le but de :

- Gérer les données des salariés ;
- Coordonner les devis et la facturation des prestations ;
- Fournir des informations sur IDEX ou sur les services proposés par celle-ci ou ses partenaires;
- Participer à des actions de communications, newsletters et organisation d'évènements ;
- Traiter des candidatures à un poste ;
- Assurer un service aux clients.

IDEX est également susceptible d'utiliser des Données Personnelles à des fins administratives ou pour tout autre objectif imposé par la législation en vigueur.

Si les Données Personnelles sont nécessaires à d'autres fins que celles initialement déterminées, elles ne pourront être utilisées que si la nouvelle finalité est compatible avec la finalité initiale.
Exemple d'une finalité spécifique, explicite et légitime :

- Mise en place d'une relation contractuelle avec un client.
  Exemple de finalités compatibles : Envoi d'informations thématiques à un client.

2.2. Etablir un fondement juridique licite

Le RGPD exige un fondement juridique pour tout Traitement de données. Le Traitement n'est licite que si au moins une des 5 conditions[7] Suivantes sont remplies :

- La Personne Concernée a consenti de manière libre, spécifique, éclairée et univoque au Traitement de ses DCP pour une ou plusieurs finalités spécifiques ;

[6] Art. 5.1.b du RGPD

[7] Art.6 du RGPD

- Le Traitement est nécessaire à l'exécution d'un contrat auquel la Personne Concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci

  Ex : Traitement des Données de salariés par un employeur pour procéder à des rémunérations.
- Le Traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du Traitement est soumis

  Ex : Traitement des données relatives aux rémunérations des salariés par les employeurs pour pouvoir les communiquer à la sécurité sociale ou à l'administration fiscale.
- Le Traitement est nécessaire à la sauvegarde des intérêts vitaux de la Personne Concernée ou d'une autre personne physique
- Le Traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du Traitement ;

La base juridique justifiant la licéité d'un Traitement ne peut pas être modifiée librement au cours du Traitement. Lorsque la licéité du Traitement est fondée sur la base du consentement, IDEX ne pourra pas se fonder sur une autre base légale en l'absence de recueil du consentement ou de preuve du consentement des Personnes Concernées.

IDEX doit :

- S'assurer au stade de la conception des projets de leur licéité au regard des 5 bases juridiques prédéfinies ;
- Prendre compte du fondement juridique des Traitements, pour l'exercice de certains droits d'accès [8] ;
- Signaler le fondement juridique du Traitement de façon transparente, en des termes clairs et simples dans des mentions CNIL ; obligatoires (mentions CNIL des formulaires, Charte site internet)[9].

2.3. Recueillir le consentement

Le recueil du consentement[10] peut servir de base juridique aux Traitements de données à des fins de marketing.

[8] Art. 13.1.c du RGPD

[9] Art. 15 à 22 et de l'article 34 du RGPD.

[10] Art. 4. 11 du RGPD

Conditions de validité du consentement

En application du RGPD, le consentement n'est valable qu'en présence d'une manifestation de volonté, libre, spécifique, éclairée et univoque : la Personne Concernée accepte, par une déclaration ou par un acte positif clair, que ses DCP fassent l'objet d'un Traitement à des fins prédéfinies.

Caractéristique du consentement	**Définition**
Positif	Le consentement préalable des Personnes Concernées doit être recueilli sans ambiguïté pour la collecte des Données transmises ou émises par un équipement ou sur support papier. Le consentement présumé (Opt-out actif ou passif) même éclairé est à exclure sauf intérêt légitime du responsable de Traitement dans le respect des droits des Personnes Concernées (ex : lutte contre la fraude)
Libre	Le consentement doit être inconditionné et préalable à toute activité de Traitement. Le refus de la Personne Concernée à un Traitement marketing ne doit pas la priver du bénéfice d'un droit et/ou de la conclusion d'un contrat. Le consentement n'est pas valide si la Personne Concernée n'a pas de véritable choix ou que l'absence de consentement entraîne des conséquences négatives pour elle.
Spécifique	Le consentement doit être propre à une opération ou catégorie de Traitements prédéfinie en fonction de sa finalité spécifique. Lorsque le Traitement des DCP est effectué pour plusieurs finalités, chaque finalité doit être distincte et le consentement doit être obtenu pour chacune d'entre elles.
Eclairé	Le consentement doit être informé par des mentions CNIL obligatoires claires, transparentes, compréhensibles, aisément accessibles et préalables à la collecte de Données. La notion de consentement éclairé peut inclure un rappel obligatoire tous les 6 mois du droit de retirer le consentement donné
Explicite	Le consentement dilué dans des conditions générales d'utilisation (CGU) est à exclure. Un consentement informé non présumé, non conditionné et propre à chaque objectif de Traitement ou modalités spécifique doit être tracé.

Documentation de la preuve des consentements recueillis

IDEX doit être en mesure de démontrer que la Personne Concernée a donné son consentement au Traitement de Données[11].

Un écrit doit pouvoir prouver le recueil du consentement exprès de la Personne Concernée

- Formulaire papier à signer[12] ;
- Case à cocher, et Opt- in horodatés y compris en matière de Tag ;
- Enregistrement vocal ;
- Envoi d'un message de confirmation avec un lien de validation (« Re-Opt- in »).

Cette preuve doit être conservée dans des conditions préservant son intégrité et son authenticité.

Cette obligation est également valable en cas de sous-traitance afin qu'IDEX puisse répondre aux demandes d'une autorité de régulation et /ou faire droits aux demandes des Personnes Concernées.

2.4. Collecter et traiter les données loyalement manière loyale, licite et transparente

Les données doivent être traitées de manière loyale, licite et transparente[13].

La licéité du Traitement fait référence à son fondement juridique (obligation légale, obligation contractuelle etc.).

La loyauté du Traitement désigne les modalités selon lesquelles les données sont collectées. Ce principe fait référence au droit à l'information des Personnes Concernées. IDEX doit toujours fournir une information complète en termes clairs sur les Traitement de Données (ex : mise en ligne d'une politique ou charte Données Personnelles, panneau d'information pour la vidéosurveillance).

Des Données Personnelles ne peuvent être collectées et traitées à l'insu des Personnes Concernées (ex : un data broker vendant des profils de consommateurs détaillés : catégorie sociaux-professionnel et/ou composition familiale accompagnée d'un score) à leur insu et sans leur consentement éclairé réalise une collecte déloyale et illicite.

Le détournement de finalité de celle initialement portée à la connaissance des Personnes Concernées constitue un « détournement de finalité » sanctionnée par le RGPD, sauf Traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

[11] Art.7-1 du RGPD

[12] Délibération CNIL du 06/10/2011

[13] Art.5.1.a

2.5. Respecter le principe de minimisation des données

IDEX ne traite que les données qui sont indispensables aux finalités déterminées. Seules les données qui sont strictement nécessaires (et non seulement utiles) à la réalisation des finalités[14] doivent être traitées (ex : lors de l'inscription à une lettre d'information, IDEX doit uniquement collecter l'adresse mail de la Personne Concernée). Si des Données Personnelles ne sont pas nécessaires pour permettre la réalisation de la finalité, elles ne doivent pas être collectées, utilisées ou traitées de quelque manière que ce soit.

IDEX doit être en mesure de démontrer pourquoi certains types de Données Personnelles sont utilisés et en quoi les Données traitées sont adéquates, pertinentes et non excessives, au regard des finalités pour lesquelles elles ont été collectées.

2.6. Définir une durée de conservation des données

Les Données Personnelles ne peuvent pas être conservées indéfiniment dans les Fichiers[15]. **La durée doit être définie en fonction de la nature des données, de leur utilité et de l'objectif poursuivi. Elle ne doit pas être** pas excessive par rapport à l'objectif de la collecte.

Au terme de la réalisation de l'objectif, les données doivent être :

- Supprimées ou ;
- Archivées ou ;
- Faire l'objet d'un processus d'anonymisation des données, afin de rendre impossible la « ré-identification » des personnes.

Pour chaque projet ou processus opérationnel, IDEX doit définir des durées de conservation spécifiques, sauf si un texte de loi impose une durée précise à savoir :

- Un (1) mois maximum dans le cas d'un dispositif de vidéosurveillance poursuivant un objectif de sécurité des biens et des personnes ;
- Deux (2) ans après le dernier contact pour les données relatives au Traitement des candidatures ;
- Deux (2) ans après la fin de la relation de travail pour les données de rémunération ;
- Deux (2) ans après la fin de la relation de travail pour les Données de santé et les Données juridiques ;
- Cinq (5) ans concernant les données relatives à gestion de la paie ou au contrôle des horaires des salariés ;

[14] Art.5.1.c du RGPD

[15] Art. 5.1. e du RGPD

- Trois (3) ans après le dernier contact avec les clients/prospects/partenaires d'affaires ;
- Sept (7) ans après la fin de la relation de travail pour les Données concernant les retraites, congés etc. ;
- Douze (12) mois après la collecte de Données Personnelles pour des raisons de sécurité ou pour des raisons informatiques (inclus les Données Personnelles dans les réseaux informatiques, les serveurs, les caméras de surveillance).

Préalablement à la collecte de Données Personnelles, la question suivante doit toujours être posée : « De quelles Données Personnelles ai-je vraiment besoin pour fournir mon service ou mon produit ? » (Ex : dans le cas d'un formulaire en ligne, il convient de supprimer tous les champs facultatifs, afin de ne pas obtenir plus de données que nécessaire).

2.7. Fournir une information transparente

Il incombe à IDEX de fournir une information complète, facilement accessible et compréhensible aux Personnes Concernées par les opérations de Traitement.[16]

Moment de l'information

- Avant la collecte
- À titre exceptionnel lors de la première relation avec la Personne Concernée lorsque la donnée est collectée par un tiers

Mentions obligatoires

Le RGPD ne définit pas ce qu'est une information transparente directement[17] car chaque information CNIL doit être rédigée au cas par cas en fonction des objectifs et des modalités du Traitement en cause.

La Personne Concernée doit avoir accès à une information transparente, en des termes clairs et simples concernant les données la concernant traitées par IDEX[18].

Les mentions d'informations doivent dans des termes aisément accessibles préciser :

- Son identité et ses coordonnées ;
- Les coordonnées du Délégué à la Protection des Données (DPO) ;
- Les finalités du Traitement (à quoi vont servir les données collectées) ;

[16] Exception : Impossibilité pratique d'identifier les personnes concernées ; effort disproportionné, Traitements de données particulièrement sensibles

[17] Considérant 29 du RGPD

[18] Art. 15 à 22 et de l'article 34 du RGPD. La mise en place d'icônes normalisées et d'allégement de l'affichage de ces mentions légales sur tous les supports de collecte de DCP est en projet au niveau européen

- Le caractère obligatoire ou facultatif du recueil des données et les conséquences pour la personne en cas de non-fourniture des données ;
- Les catégories de Données Personnelles concernées ;
- Les destinataires ou catégories de destinataires des données (qui a besoin d'y accéder ou de les recevoir au vu des finalités définies) ;
- La durée de conservation des données (ou critères permettant de la déterminer) ;
- Les droits des Personnes Concernées (opposition, accès, rectification, effacement, limitation, portabilité) ;
- Les éventuels transferts de leurs Données vers des pays hors de l'Union européenne (ou vers une organisation internationale) et garanties associées ;
- La procédure de prise de décision automatisée le cas échéant ;
- Le droit d'introduire une réclamation (plainte) auprès de la CNIL.

Cela garantit la transparence et l'équité dans les activités de Traitement effectuées. La complexité d'un Traitement, la multiplication des finalités et des destinataires ne justifie pas une moindre transparence, au contraire.

Caractéristiques de l'information,

Pour être conforme un Traitement doit présenter chacun des critères suivants :

Concise	L'utilisation d'icônes est recommandée. Une politique de confidentialité présentant les différents thèmes par section, doivent être distincte des autres mentions légales
Transparente	L'information doit comprendre toutes mentions légales obligatoires Ex : Information sur l'existence d'un Transfert de Données hors UE et les garanties qui l'encadrent
Claire	L'information doit être fournie dans un langage accessible et précis Exclusion de formule évoquant l'utilisation de Données pour « développer de nouveaux services » (quels services et comment ?) ou « À des fins statistiques ou de recherches » ou « vous offrir des services personnalisés »
Aisément accessible	En cas de demande d'information, elle peut être communiquée par orale Ex : Page dédiée à la charte figurant sur chacune des pages d'un site Web, Bandeau Cookies

Modalités pratiques

IDEX doit indiquer l'information sur chaque support de collecte de données papier et numérique (sites institutionnels, page de réseaux sociaux officiels, etc.).

L'information doit se décliner en une mention de bas de page de formulaire ainsi que dans une charte de protection des données à laquelle les autres mentions légales doivent renvoyer.

L'information CNIL doit contenir des éléments d'informations renforcées (ex : coordonnées du délégué, durée de conservation). La mise en place d'icônes normalisées est fortement recommandée pour favoriser l'accès et la compréhension des informations.

En cas d'évolution significative des traitements, IDEX s'engage à la mettre à jour ce document et à recueillir les consentements de ses clients/prospects.

2.8. Mettre à jour les données traitées

Les Données Personnelles traitées par IDEX doivent être exactes et à jour. Des Données précises permettent de prendre de meilleures décisions et d'éviter les effets préjudiciables des décisions fondées sur des Données incorrectes.

2.9. Sécuriser les Traitement de Données

IDEX engage sa responsabilité pénale toutes les fois où elle ne prend pas de manière opérationnelle toutes les précautions utiles pour garantir la sécurité des Données qu'elle a collectées mais aussi leur confidentialité[19], c'est-à-dire s'assurer que seules les personnes autorisées y accèdent. Ces mesures pourront être déterminées en fonction des risques pesant sur les Fichiers :

- Sécurisation des postes de travail
- Chiffrement des flux de Données
- Sauvegardes quotidiennes
- Engagement de confidentialité des salariés et des Sous-traitants

2.10. Tenir un registre des Traitements

La tenue du registre des Traitements est l'une des principales obligations de conformité incombant à IDEX[20]. Cette obligation concerne toute entreprise ou organisation comptant plus de 250 employés. Toutefois, l'entreprise y est tenue, lorsqu'elle compte moins de 250 salariés si :

- Le Traitement n'est pas occasionnel (ex : gestion des clients, gestions des salariés, etc.) ;

[19] Art. 32 du RGPD

[20] Art. 30 du RGPD

- Le Traitement est susceptible de comporter un risque pour les droits et libertés des personnes (ex : vidéosurveillance) ;
- Le Traitement porte notamment sur des données « sensibles[21] » ou des données relatives à des condamnations pénales ou à des infractions.

En pratique, ce registre des Traitements permet à IDEX de :

- Recenser et avoir une visibilité de tous les Traitements de Données Personnelles mis en œuvre ;
- Prouver sa conformité aux exigences du RGPD ;

Le Registre des Traitements doit être complété à chaque mise en place d'un nouveau traitement et mis à jour régulièrement selon les modifications apportées aux conditions de mises en œuvre des Traitements (nouvelle donnée, allongement de la durée de conservation, nouveau destinataire, etc.)

La fiche du registre doit comporter à minima les informations suivantes :

- Le nom et les coordonnées du Responsable de Traitement et du DPO ;
- Les finalités du Traitement, l'objectif en vue duquel les données ont été collectées ;
- Les catégories de Personnes Concernées (ex : clients, collaborateurs, salariés, etc.);
- Les catégories de Données Personnelles (ex : identité, situation familiale, vie professionnelle, etc.);
- Les transferts de données vers un pays tiers ou à une organisation internationale et les garanties prévues pour ces transferts ;
- Les délais prévus pour l'effacement des données, ou à défaut les critères permettant de la déterminer ;
- Une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre.
- La base juridique du Traitement[22]

Le Registre des Traitements est mis à disposition de la CNIL sur demande à des fins de contrôle des opérations de Traitement.

2.11. Notifier les violations de sécurité

A titre d'exemple, une violation peut se produire lorsqu'un salarié d'IDEX du perd des documents (sous format électronique ou papier) ou lorsqu'un système d'information est compromis par un attaquant.

[21] Article 30.1 du RGPD

IDEX a l'obligation[23] de notifier à la CNIL toute violation impactant des Données Personnelles.

Une violation de Données Personnelles est une faille de sécurité entraînant, de manière accidentelle ou illicite :

- La destruction,
- La perte,
- L'altération,
- La divulgation non autorisée de Données Personnelles transmises, conservées ou traitées d'une autre manière,
- L'accès non autorisé à de telles Données[24].

Cette notification à la CNIL s'effectue dans les meilleurs délais et si possible 72 heures au plus tard après en avoir pris connaissance. Au-delà du délai de 72 heures, IDEX doit justifier son retard. Les sous-traitants d'IDEX doivent notifier toute violation de Données Personnelles dans les meilleurs délais, après en avoir pris connaissance.

Toute violation de Données Personnelles doit faire l'objet d'une documentation, afin de permettre à la CNIL de vérifier le respect de cette obligation. Cette documentation doit indiquer :

- Les faits concernant la violation des Données Personnelles,
- Ses effets et les mesures prises pour y remédier.

Communication à la Personne Concernée

En cas de risque élevé, IDEX à l'obligation[25] de communiquer la violation à la Personne Concernée en des termes simples et clairs dans les meilleurs délais afin qu'elle puisse prendre les précautions qui s'imposent (par exemple, changement de mot de passe). Le risque est élevé pour les droits et libertés d'une personne physique s'il entraîne des conséquences préjudiciables relatives à :

- La confidentialité,
- La disponibilité,
- L'intégrité des Données Personnelles.

Exception à la communication

IDEX n'est pas tenue (article 33 du RGPD) de communiquer la violation à la Personne Concernée, dans les cas suivants[26] :

[23] Article 33 du RGPD

[24] Art.4.12 du RGPD

[25] Article 34.1 du RGPD

[26] Article 34.3 du RGPD

- Des mesures de protection techniques et organisationnelles appropriées en particulier, celles qui rendent les Données Personnelles incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;
- Des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des Personnes Concernées n'est plus susceptible de se matérialiser ;
- La communication exigerait des efforts disproportionnés. Dans ces cas, IDEX doit procéder à une communication publique ou une mesure similaire permettant aux Personnes Concernées d'être informées de manière tout aussi efficace.

Si IDEX ne communique pas la violation de Données Personnelles aux Personnes Concernées, la CNIL peut, après examen de la violation, exiger d'IDEX qu'elle en informe les Personnes Concernées.

2.12. Réaliser une évaluation d'impact sur la vie privée (EIVP / DPIA)

Lorsqu'un Traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des Personnes Concernées, IDEX doit effectuer, préalablement au Traitement envisagé une EIVP[27] sur la protection des Données Personnelles.

Un risque élevé est un scénario décrivant[28] :

- Un évènement redouté (accès non autorisé, modification non désirée, disparition des données, et ses impacts potentiels sur les droits et libertés des personnes) ;
- Toutes les menaces qui permettraient qu'il survienne.

La gravité du risque doit être apprécié pour les Personnes Concernées et non pour IDEX et sa vraisemblance, à savoir la probabilité de réalisation du risque.

L'analyse d'impact permet à IDEX de :

- Mettre en œuvre des Traitements de données respectueux de la vie privée ;
- Démontrer sa conformité au RGPD.

Les éléments de l'EIVP

L'analyse d'impact doit contenir à minima :

- Une description systématique des opérations de Traitement envisagée et les finalités du Traitement ;

[27] Article 35 du RGPD

[28] https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

- Une évaluation de la nécessité et de la proportionnalité des opérations de Traitement au regard des finalités ;
- Une évaluation des risques sur les droits et libertés des Personnes Concernées ;
- Les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du RGPD.

Les conditions de réalisation de l'EIVP

Une EIVP est nécessaire si le Traitement envisagé remplit au moins deux des critères suivants :

- Une évaluation d'aspects personnels ou notation d'une personne (ex : scoring financier) ;
- Une prise de décision automatisée ;
- Une surveillance systématique de personnes (ex : vidéosurveillance) ;
- Un Traitement de données sensibles (ex : santé, biométrie…) ;
- Un Traitement de données de personnes vulnérables (ex : personnes âgées, mineurs) ;
- Le Traitement à grande échelle de Données Personnelles ;
- Le croisement d'ensembles de données ;
- Des usages innovants ou l'application de nouvelles technologies (ex : objet connecté, SmartGrids) ;
- L'exclusion du bénéfice d'un droit, d'un service ou contrat.

2.13. Encadrer les relations avec les tiers

En cas de sous-traitance d'un Traitement ou d'un Fichier comportant des Données Personnelles, IDEX doit :

- Faire appel uniquement à des Sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le Traitement réponde aux exigences du RGPD et garantisse la protection des droits de la Personne Concernée ;
- Veiller à ce que sa relation avec le Sous-traitant soit encadrée par un contrat écrit.
- Imposer, à minima, le même niveau de protection des Données pratiqué par IDEX ;

L'application par le Sous-traitant d'un code de conduite approuvé ou d'un mécanisme de certification approuvé peut démontrer l'existence des garanties suffisantes.

Les critères pour sélectionner son sous-traitant

IDEX doit définir ses besoins et ses exigences de base, c'est-à-dire un socle en deçà duquel le Sous-traitant candidat n'offre pas les garanties suffisantes.

Ce socle doit porter sur :

- Les opérations de Traitement confiées au prestataire : bien que les sous-traitants se voient directement imposer des obligations en matière de sécurité, IDEX demeure garant de la sécurité, la confidentialité et l'intégrité des données. Le sous-traitant doit ainsi :
  - Être doté d'un programme de sécurité fondé sur un ensemble de normes reconnues
  - Être doté d'un mécanisme de gestion des risques, permettant d'identifier et d'évaluer les risques pour le système d'information
  - Avoir documenté la sécurité de son système d'information, si possible au moyen d'audit par des tiers experts et indépendants
  - Faire continuellement évoluer son système d'information, afin de prendre en compte les nouvelles menaces et l'évolution des technologique
- La sécurité technique des services, et par conséquent, des données
- La maturité du prestataire sur la question de la protection des Données Personnelles :
  - Le prestataire a défini et mis en œuvre une politique de protection des données à caractère personnel.
  - Il a sensibilisé ses salariés à cette problématique et forme régulièrement les équipes ayant vocation à traiter les données pour le compte de ses clients
  - Il dispose, à minima, d'un collaborateur en charge de la protection des données et a fortiori lorsque la désignation d'un DPO est exigée par le RGPD.

Il convient impérativement de négocier le contrat de sous-traitance adapté, qui doit prévoir un régime de responsabilité propres et des annexes spécifiques.

L'établissement de clauses contractuelles

Ce contrat reprend les obligations prévues à l'article 28.8 du RGPD. Par conséquent, les clauses de sous-traitance de Données Personnelles validées par la CNIL sont intégrées dans les contrats dès qu'ils portent sur le Traitement de Données Personnelles.

Le contrat doit prévoir un mécanisme de contrôle du changement, afin de pouvoir faire évoluer la relation contractuelle au regard des évolutions de la sous-traitance.

Le Délégué à la Protection des Données (DPO) est informé de tout contrat impliquant la sous-traitance de Données Personnelles.

La mise en place d'une revue annuelle de la sous-traitance

IDEX doit mettre en place une revue annuelle afin d'assurer la légalité continue du Traitement ainsi que l'adéquation des instructions et mesures techniques et organisationnelles, au regard de la sous-traitant effectuée par le prestataire :

- Un audit sur pièce au moins annuellement
- Un audit sur site au moins tous les 2 ans

2.14. Encadrer les transferts de Données hors de l'Union Européenne

En cas de recours à des Sous-traitants hors de l'Espace Economique Européen (EEE) ou de transfert de Données Personnelles, IDEX doit s'assurer que le transfert est réalisé dans le respect des conditions[29] prévues par le RGPD.

Les décisions d'adéquations

IDEX peut transférer des Données vers les pays reconnus comme offrant un niveau de protection des Données adéquat (pays dotés d'une législation assurant une protection suffisante des Données) par la Commission Européenne[30] tels que :

- La Suisse,
- Le Canada,
- L'Andore,
- L'Argentine,
- Les îles Guernesey,
- L'île de Man,
- Les îles Féroé,
- Jersey,
- Israël,
- La Nouvelle-Zélande
- L'Uruguay.
- L'Islande,
- Le Liechtenstein,
- la Norvège.

Les garanties appropriées

[29] Art. 44 du RGPD

[30] Art.45 du RGPD

En l'absence d'une telle décision, IDEX peut effectuer des Transferts sous réserve qu'il existe des garanties appropriées parmi celles qui figurent dans la liste suivante :

- Outils de transferts sans autorisation de la CNIL
    - Des clauses contractuelles types[31] de protection des données adoptées par la Commission européenne ;
    - Des clauses contractuelles types[32] adoptées par les autorités de contrôle et approuvées par la Commission européenne ;
    - Des règles d'entreprise contraignantes[33] "binding corporate rules" ou "BCR" (politique de protection des Données intra-groupe, juridiquement contraignantes et respectées par les entités signataires du groupe);
    - Un code de conduite[34] approuvé par une autorité de contrôle (comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées) ;
    - Un mécanisme de certification[35] approuvé par une autorité de contrôle ou un organisme de certification agréé (comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées).

- Outils de transferts soumis à l'autorisation de la CNIL
    - Des clauses contractuelles spécifiques[36] entre IDEX et un Sous-traitant.

Les dérogations

En l'absence de décision d'adéquation ou de garanties appropriées, le RGPD prévoit certaines dérogations[37] pour l'encadrement des Transferts vers des pays tiers.

- La Personne Concernée a donné son consentement explicite au transfert envisagé ;
- Le Transfert est nécessaire :
    - à l'exécution d'un contrat demandé par la Personne,
    - à l'exécution d'un contrat auquel la Personne Concernée et IDEX sont parties,
    - à l'exécution d'un contrat conclu dans l'intérêt de la Personne Concernée,

[31] Art.46.2.c du RGPD

[32] Art. 46.2. d du RGPD

[33] Art. 47 du RGPD

[34] Art. 40 et 46.2.e du RGPD

[35] Art. 42 et 46.2.f du RGPD

[36] Art. 46.3. a du RGPD

[37] Art. 49.1 du RGPD

Ces exceptions ne couvrent pas les Transferts répétitifs ou massifs de Données.

2.15. Respecter les droits des Personnes

Le RGPD s'assure que la Personne Concernée dispose[38] des droits sur ses Données Personnelles, dont elle est la seule propriétaire.

IDEX s'engage à répondre dans les meilleurs délais aux demandes des Personnes Concernées, et en tout état de cause, dans un délai d'un mois à compter de la réception de la demande.

Au besoin, ce délai pourra être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes adressées à IDEX. Dans ce cas, les Personnes Concernées seront informées dans un délai d'un mois à compter de la réception de la demande de cette prolongation et des motifs du report.

Si la demande est présentée sous format électronique, les informations seront également fournies par voie électronique lorsque cela est possible, à moins qu'il en soit demandé expressément autrement.

Si IDEX ne donne pas suite à la demande, elle en informera la Personne Concernée des motifs et elle disposera de la possibilité d'introduire une réclamation auprès de l'autorité de contrôle et/ou de former un recours juridictionnel.

Dans le cas où IDEX s'est appuyée sur des tiers pour traiter les Données, ces derniers doivent coopérer pour répondre à la demande.

Droit d'accès

Ce droit[39], permet aux personnes dont les Données sont traitées, d'obtenir d'IDEX la confirmation que des Données Personnelles les concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites Données ainsi que les informations suivantes :

- Les finalités d'utilisation des Données ;
- Les catégories des Données collectées ;
- Les destinataires ou catégories de destinataires qui ont pu accéder à ces Données ;
- La durée de conservation des Données ou les critères qui déterminent cette durée ;
- L'existence des autres droits (droit de rectification, d'effacement, de limitation, d'opposition) ;
- La possibilité de saisir la CNIL ;

[38] Art. 12 du RGPD

[39] Art.15 du RGPD

- Toute information relative à la source des données collectées si celles-ci n'ont pas directement été récoltées auprès de vous,
- L'existence d'une prise de décision automatisée, y compris en cas de profilage, et la logique sous-jacente, l'importance et les conséquences pour vous d'une telle décision,
- L'éventuel transfert de vos données vers un pays tiers (non-membre de l'UE) ou vers une organisation internationale.

Droit de rectification

Ce droit[40] permet aux Personnes dont les Données sont traitées, d'obtenir d'IDEX, dans les meilleurs délais, la rectification ou la mise à jour des Données Personnelles les concernant qui sont inexactes, incomplètes ou expirées.

Le droit de rectification complète le droit d'accès. Il permet d'éviter de traiter ou de diffuser de fausses informations (ex : un changement de nom à la suite d'un mariage ou d'un divorce, un changement d'adresse mail ou d'adresse postale.)

Droit à l'effacement ou droit à l'oubli

Ce droit[41] permet aux Personnes Concernées de demander l'effacement de leurs Données dans les cas suivants:

- Les Données ne sont plus nécessaires au regard des finalités établies ;
- La Personne Concernée retire le consentement sur lequel est fondé le Traitement ;
- La Personne Concernée s'oppose au Traitement et il n'existe pas de motifs légitimes impérieux pour le Traitement ;
- Les Données ont fait l'objet d'un Traitement illicite ;
- Les Données doivent être effacées pour respecter une obligation légale.

Ce droit ne peut être exercé si IDEX justifie qu'une conservation est légitime et nécessaire à des fins de preuve ou pour respecter une obligation légale à laquelle il est soumis (ex : factures, contrats).

Droit à la limitation du Traitement

Le RGPD prévoit un droit de limitation[42] temporaire des Traitements dans 4 cas spécifiques :

[40] Art.16 du RGPD

[41] Art. 17 du RGPD

[42] Art.33 du RGPD

- Lorsque la Personne Concernée conteste l'exactitude d'une donnée, le temps que le responsable du Traitement puisse contrôler cette exactitude.
- Si le Traitement est illicite et que la Personne Concernée s'oppose à l'effacement (ex. constituant un élément de preuve dans le cadre d'une action en justice).
- Lorsqu'il n'est plus nécessaire à l'organisation mais que la Personne Concernée a besoin de ses données pour la constatation, l'exercice ou la défense de ses droits en justice.
- Le temps nécessaire à l'appréciation du caractère fondé d'une demande d'opposition sur le point d'être effacées, les données « sont encore nécessaires à la Personne Concernée pour la constatation, l'exercice ou la défense de droits en justice ».

Ce droit est généralement exercé lorsque les Personnes Concernées souhaitent vérifier l'intérêt légitime servant de base juridique au Traitement ou faire valoir leur droit en justice suite à une défaillance supposée ou avérée d'IDEX.

La limitation doit entrainer le gel temporaire du Traitement des données qui ne peuvent plus faire l'objet que d'une conservation sauf si :

- La Personne Concernée donne son consentement à une autre forme de Traitement
- Leur Traitement est nécessaire à « la constatation, l'exercice ou la défense de droits en justice (…), la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public de l'Union ou d'un État membre ».

Le choix technique pour limiter le Traitement est à la charge d'IDEX et peut inclure :

- Un déplacement temporaire des données vers un autre système ;
- Un verrouillage des données les rendant inaccessibles ;
- Un retrait temporaire de données publiées sur un site internet.

Si IDEX vient à lever la limitation, il doit préalablement informer la Personne Concernée de cette action.

Droit à la portabilité

Les Personnes Concernées doivent pouvoir exercer une demande de récupération de leurs Données[43] pour :

- Leur usage personnel, à charge de ne lui fournir que des données la concernant issus de Traitements effectués à l'aide de procédés automatisés (dossiers papiers non concernés)
- La facilitation de ses relations avec des tiers, même concurrent, transmettre à un autre responsable de Traitement si cette demande est techniquement possible.

[43] Art. 20 du RGPD

Le droit à la portabilité n'est applicable qu'aux Traitements suivants :

- Traitement automatisé se fondant sur le consentement de la Personne Concernée ou
- Traitement automatisé se fondant sur un contrat (à l'exclusion des Traitements fondés sur l'intérêt public ou intérêt légitime),

Les données concernées à restituer sont :

- Données déclarées sciemment et activement par la Personne Concernées (ex : données fournies pour créer un compte en ligne tels que l'adresse électronique, l'adresse postale, etc.)
- Données générées par son activité et données observées (ex : l'historique des achats, l'historique des recherches faites sur internet, les courriels envoyés ou reçus, telles que des données transactionnelles et le suivi de commande).

Droit d'opposition

Ce droit[44] permet aux Personnes Concernées de demander à IDEX d'arrêter le Traitement de leurs Données (ex : opposition à la réception de newsletters, à l'utilisation des cookies, etc.). Les Données ne sont pas supprimées mais ne sont plus utilisées pour les finalités auxquelles la Personne s'est opposée.

Ce droit peut être utilisé dans les cas suivants :

- Lorsqu'un Traitement de Données est fondé sur l'intérêt légitime d'IDEX ou l'intérêt public. Dans ce cas, IDEX peut refuser la demande si elle démontre que son intérêt légitime l'emporte sur les droits et libertés des Personnes Concernées ou qu'elle a besoin des Données pour l'établissement, l'exercice ou la défense d'une plainte ;
- Lorsque les Données Personnelles sont traitées à des fins de prospection commerciale ce qui inclut le profilage effectué à cette fin ;
- Lorsque les Données Personnelles sont traitées à des fins de recherche scientifique ou historique ainsi qu'à des fins statistiques à moins que le Traitement soit mis en œuvre dans l'intérêt public.

Droit de ne pas être soumis à des décisions fondées uniquement sur le Traitement automatisé

Les Personnes Concernées ont le droit de ne pas être soumis à une décision lorsqu'elle est uniquement basée sur un Traitement automatisé[45], y compris le profilage (en utilisant un algorithme où il n'y a pas d'intervention humaine).

[44] Art.21 du RGPD

[45] Art.22 du RGPD

En général, les décisions importantes concernant les Personnes Concernées, effectuées sur la base de leurs Données Personnelles, doivent avoir une contribution humaine et ne doivent pas être générées automatiquement par un ordinateur, sauf :

1. Si la prise de décision automatisée est nécessaire pour l'exécution d'un contrat entre IDEX et la Personne Concernée car elle permet à IDEX de :
    - Réduire :
        - Le risque d'erreur humaine, de discrimination ou d'abus de position ;
        - Le risque d'impayés ;
        - Les délais de prise de décision ;
    - Optimiser :
        - L'efficacité des processus.
2. Si la Personne Concernée a explicitement consenti aux Traitements automatisés ;
3. Si la prise de décision automatisée est autorisée par les lois en vigueur.

Dans tous les cas, d'IDEX doit informer les Personnes Concernées de :

- La prise de décision automatisée les concernant et s'ils doivent fournir de nouvelles Données Personnelles ;
- La méthodologie de Traitement ;
- Les conséquences potentielles du Traitement.

Dans les deux derniers cas, IDEX doit s'assurer de la mise en œuvre de mesures appropriées pour permettre aux Personnes Concernées d'obtenir une intervention humaine, d'exprimer leur point de vue, d'obtenir une explication de la décision prise post- évaluation et de contester la décision.

Droit de porter plainte

IDEX doit toujours porter à la connaissance des Personnes Concernées qu'elles ont la faculté de saisir le Service des plaintes de la Commission Nationale de l'Informatique et des Libertés par courrier postale pour faire valoir leurs droits, notamment en cas de difficultés, de réponse insatisfaisante ou d'absence de réponse.

3. CADRE ORGANISATIONNEL DE TRAITEMENT DES DONNEES

La protection des Données utilisées par IDEX doit être prise en compte, dès la phase de conception d'un Traitement de Données Personnelles.

3.1. Structure organisationnelle

Le Délégué à la protection des données (DPO)

Le Délégué à la protection des données est l'interlocuteur principal pour toutes les questions concernant les Données Personnelles. Pour IDEX, il exerce le rôle référent principal sur les sujets de Données, et pour l'autorité de contrôle, celui de représentant principal d'IDEX.

Le Délégué à la protection des données a pour mission de :

- Conseiller IDEX, ainsi que l'ensemble des salariés sur les obligations qui incombent à IDEX en vertu du RGPD et d'autres dispositions en matière de protection des Données Personnelles ;
- Informer IDEX des manquements constatés, conseiller sur les actions correctives à mettre en place pour y remédier, soumettre les arbitrages nécessaires ;
- Veiller à la bonne application du principe de protection des données dès la conception et par défaut dans tous les projets impliquant un Traitement de Données Personnelles ;
- Tenir le Registre des Traitements et documenter les Traitements mis en œuvre au sein d'IDEX en tenant compte du risque associé à chacun d'entre eux compte tenu de sa nature, sa portée, du contexte et de sa finalité et assurer son accessibilité à la CNIL ;
- Mener des actions de sensibilisation et de communication à destination des salariés afin de les sensibiliser aux enjeux de la protection des Données Personnelles ;
- Assurer la bonne gestion des demandes d'exercice de droits, de réclamations et de requêtes formulées par les Personnes Concernées par les Traitements et s'assurer de leur transmission aux services concernés et apporter à ces derniers des conseils dans la réponse à fournir aux demandeurs ;
- Dispenser des conseils concernant la réalisation d'analyse d'impact sur la vie privée, vérifier son exécution et assurer sa pertinence au regard du RGPD ;
- Mettre IDEX en position de notifier d'éventuelles violations de données auprès de la CNIL et porter conseil, notamment concernant les éventuelles communications aux Personnes Concernées et les mesures à apporter ;
- Veiller, en toute indépendance, au respect du cadre réglementaire en matière de protection des Données Personnelles au sein d'IDEX ;

- Veiller à la mise en œuvre de mesures appropriées pour permettre à IDEX de démontrer que les Traitements sont effectués conformément au RGPD, et si besoin, réexaminer et actualiser ces mesures ;
- Piloter la production et la mise en œuvre de politiques, de procédures et de règles de contrôle pour une protection efficace des Données Personnelles et de la vie privée des Personnes Concernées ;
- Être l'interlocuteur privilégié de la CNIL, coopérer avec elle et solliciter son avis sur les opérations de Traitement si nécessaire.

Le Délégué à la protection des données est joignable via l'adresse mail : ***dpo@idex.fr***

Comité de gouvernance des Données à Caractère Personnel

Le Comité de Gouvernance des Données Personnelles est composé du :

- Délégué à la protection des données (DPO) ;
- Secrétaire Général ;
- Directeur Juridique ;
- Directeur des Systèmes d'Information ;
- Directeur des Ressources Humaines ;
- Directeur Outils, Performance et Innovation ;
- Responsable du Contrôle Interne.

Le Comité détient la responsabilité du projet de mise en conformité au RGPD, suit régulièrement son application, veille au maintien en conformité et prend les décisions sur les sujets afférents aux Données Personnelles. Le Comité se réunit tous les 6 mois afin de suivre l'évolution des Traitements entrepris par IDEX et les jurisprudences RGPD.

Sensibilisation des salariés d'IDEX

Les salariés doivent être sensibilisés aux enjeux de la protection des Données Personnelles. Pour cela, IDEX doit disposer d'outils de sensibilisation, dont :

- La Charte RGPD, annexée au Règlement Intérieur et signée par chaque salarié à son arrivée, et comportant des mentions sur la protection des Données Personnelles ;
- Les guides des salariés qui explicitent les règles d'or et bonnes pratiques à adopter au quotidien ;
- Les supports de sensibilisation à la protection des Données.

3.2. Privacy by design

Lorsqu'un nouveau Traitement de Données Personnelles est défini pour IDEX, le Responsable de Traitement doit s'assurer qu'il est conforme aux principes et aux droits de protection de la vie privée précités dans ce document :

- Seules les Données Personnelles nécessaires sont collectées ;
- La durée de rétention de ces Données doit être définie au strict minimum : les Données ne doivent pas être conservées plus longtemps que nécessaire pour la finalité du Traitement ;
- L'exercice des droits des Personnes Concernées doit être pensé dès la conception du Traitement, ceci afin de faciliter leur mise en œuvre.

3.3. Evaluation d'impact sur la vie privée (EIVP)

L'utilisation de nouvelles technologies et de nouveaux processus peut induire des risques. Afin d'être en mesure de qualifier le niveau de risque d'atteinte à la vie privée ainsi que des moyens de les atténuer, une Etude d'Impact peut être nécessaire comme indiqué ci-dessus.

Cette évaluation vise à identifier et à mesurer les risques avant la mise en œuvre d'un nouveau Traitement.

A la suite de cette analyse d'impact, les mesures de sécurité organisationnelles et techniques adaptées au Traitement sont définies et doivent être mises en œuvre.

3.4. Registre des Traitements

Un Registre des Traitements doit être mis en place et maintenu pour cartographier l'ensemble des Traitements de Données Personnelles réalisés par IDEX. Ce Registre contient les informations essentielles pour chaque Traitement, telles que définies ci-dessus.

Ce registre précise, pour chaque activité de Traitement, entre autres :

- Le métier ou la fonction support responsable du Traitement ;
- L'éventuel co-responsable ou Sous-traitant ;
- La finalité du Traitement ;
- Le fondement juridique du Traitement ;
- Les Personnes Concernées ;
- Les Données traitées ;
- Les droits des Personnes Concernées applicables au Traitement.

3.5. Registre des violations des Données Personnelles

IDEX doit maintenir un Registre des violations de Données Personnelles. Ce registre permettra à IDEX de suivre l'évolution de chaque incident, et de fournir preuves à l'autorité de régulation en cas d'audit. Le registre contient, entre autres :

- La date, l'heure du début et de la fin de la violation ;
- Les critères de sécurité affectés (disponibilité, intégrité, confidentialité) ;
- La nature des Données concernées ;
- Le nombre et la catégorie des Personnes Concernées ;
- Les éventuels sous-traitants concernés ;
- Les conséquences potentielles de la violation ;
- Les mesures de protection déployées en amont de la violation et prévues pour éviter ce type d'incidents ;
- Les mesures de sécurisations prises immédiatement après la détection de l'incident ;
- Le résultat de l'évaluation de la gravité de la violation et de la nécessité d'une communication ;
- Les dates et contenus des communications faites aux Personnes Concernées.

Dans le cadre de la gestion des violations de Données Personnelles, IDEX doit disposer d'une procédure formalisée. Elle définit les actions à effectuer suite à une violation de Données et, le cas échéant, les organismes à prévenir et les modalités d'envoi de notifications aux Personnes Concernées.

3.6. Registre des demandes des Personnes Concernées

Les Personnes dont les Données sont traitées peuvent exercer leurs différents droits garantis par la législation. IDEX doit maintenir un Registre de toutes les demandes d'exercice de droit qu'il reçoit. Ce Registre permet de suivre chaque demande, jusqu'à sa clôture, et peut servir en cas d'audit.

Il contient, pour chaque demande, entre autres, les éléments suivants :

- La date et de réception de la demande ;
- Le nom et prénom de la Personne Concernée ayant effectué la demande ;
- Le droit exercé ;
- La Donnée concernée par la demande ;
- L'éventuelle modification proposée (s'il s'agit d'une demande de modification) ;
- Le Traitement concerné ;
- Le support de la Donnée ;
- Le membre d'IDEX en charge du Traitement ;

- Les actions effectuées pour répondre à la demande ;
- Le contenu des réponses envoyées à la Personne Concernée ;
- La date de clôture de la demande.

Afin de faciliter les réponses aux demandes, IDEX doit également disposer d'une procédure claire pour y répondre. Cette procédure doit décrire les actions à mener selon chaque type de demande, les supports de Données Personnelles concernées par les différents types de demandes et les délais et modèles de réponse.

3.7. Registre des consentements

Certains Traitements nécessitent le consentement des Personnes Concernées comme fondement juridique. Les consentements des différentes Personnes Concernées doivent être recensés dans un registre des consentements.

Ce registre contient donc :

- L'identité de la Personne Concernée ;
- Le Traitement concerné par son consentement ;
- Les Données concernées et éventuellement ;
- La date de retrait de son consentement.

3.8. Gestion des Sous-traitants

Lorsque des sous-traitants réalisent un Traitement de Données Personnelles au nom et pour le compte d'IDEX, IDEX demeure Responsable du Traitement. Il est donc important pour IDEX de s'assurer que ses sous-traitants proposent des mesures conformes au RGPD et de les documenter.

La conformité des sous-traitants avec les exigences d'IDEX et du RGPD nécessite des accords contractuels, sous la forme de clauses ou d'accords sur le niveau de sécurité des Données, et un contrôle de la conformité effectué par IDEX.

4. CADRE TECHNIQUE DE TRAITEMENT DES DONNEES

La Politique de Sécurité du Système d'Information (PSSI) du groupe IDEX définit les exigences de sécurité et procédures à appliquer pour atteindre les objectifs suivants :

- Prévenir tout risque d'appropriation illégale de biens financiers, matériels ou informationnels ;
- Prévenir tout risque de dommage ou destruction de biens matériels ou informationnels ;
- Prévenir tout risque d'accès non autorisé aux biens informationnels, de divulgation ou de modification non autorisée ;
- Respecter les obligations légales ;
- Assurer la continuité des activités.

Le respect de l'ensemble de ces règles permet de préserver les Données en assurant :

- Leur Confidentialité ;
- Leur Disponibilité ;
- Leur Intégrité ;
- Leur Résilience.

4.1. Gestion de l'exploitation

IDEX a pour objectif d'assurer une gestion sécurisée et fluide des procédures d'exploitation de ses systèmes d'information. Pour cela, elle :

- Effectue régulièrement des sauvegardes, pour limiter l'impact d'une perte ou d'un vol de données ;
- Met en place des dispositifs de protection contre les codes malveillants ;
- Garantit la disponibilité et l'intégrité des données sur une durée définie en procédant à de l'archivage ;
- Prévoit les conditions de restitution et de destruction des Données Personnelles ;
- Détruit les archives obsolètes de manière sécurisée.

4.2. Contrôle des accès

IDEX veille à ce que les utilisateurs, salariés ou prestataires, n'aient accès qu'aux données dont ils ont besoin, en définissant notamment des profils d'habilitation. Aussi, une revue régulière des habilitations et une maîtrise des mouvements de personnel permettent de couvrir les risques liés à continuité de service, la perte et la fuite d'informations ou d'actifs.

L'ensemble des applications et serveurs n'est accessible que par un identifiant et un mot de passe personnel. Cette identification obligatoire permet la traçabilité des opérations effectuées par chaque utilisateur.

L'utilisation de mots de passe complexes (Majuscules, minuscules, chiffres et caractères spéciaux) doit être généralisée pour les bases de données et applications contenant des Données à Caractère Personnel.

4.3. Sécurité physique

L'accès aux locaux n'est possible que par la détention d'un badge ou d'un code afin de prévenir toute intrusion malveillante. Chaque visiteur doit se présenter à l'accueil et prouver son identité. Les visiteurs doivent être accompagnés tout au long de leur présence dans les locaux.

Les câbles et serveurs ne doivent pas être accessibles, le local des serveurs doit être verrouillé à clef.

IDEX prévoit des moyens de chiffrement des postes nomades et supports de stockage mobiles (ordinateurs portables, clés USB, disque dur externes,…), par exemple :

- le chiffrement du disque dur dans sa totalité lorsque le système d'exploitation le propose ;
- le chiffrement fichier par fichier ;
- la création de conteneurs chiffrés.

4.4. Sécurité des communications

IDEX met en place des mesures de sécurité permanentes et filtrantes pour lutter contre les menaces liées à l'ouverture des systèmes sur Internet, notamment en réduisant le niveau de vulnérabilité des réseaux Wi-fi, et pour garantir la sécurité des informations véhiculées et contenues dans la messagerie électronique. En tout état de cause, IDEX garantit un stockage et un échange sécurisé des fichiers et prévient les accès frauduleux.

Concernant ses sites Internet, elle prévoit de :

- Mettre en œuvre le protocole TLS (en remplacement de SSL23) sur tous les sites web, en utilisant uniquement les versions les plus récentes et en vérifiant sa bonne mise en œuvre ;
- Rendre l'utilisation de TLS obligatoire pour toutes les pages d'authentification, de formulaire ou sur lesquelles sont affichées ou transmises des données à caractère personnel non publiques ;
- Limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées. Si l'accès à un serveur web passe uniquement par HTTPS, seuls les flux réseau IP sont autorisés ;

- Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées ;
- Si des cookies non nécessaires au service sont utilisés, recueillir le consentement de l'internaute après information de celui-ci et avant le dépôt du cookie ;
- Limiter le nombre de composants mis en œuvre, en effectuer une veille et les mettre à jour.

4.5. Sécurité des réseaux

IDEX s'assure qu'aucune interface d'administration n'est accessible depuis Internet et impose un VPN pour l'accès à distance (salarié, télémaintenance,..). Elle limite les flux réseau au strict nécessaire en filtrant les flux entrants/sortants sur les équipements (pare-feu, proxy, serveurs, etc.) et les accès Internet en bloquant les services non nécessaires (VoIP, peer to peer, etc.).

L'accès aux outils et interfaces d'administration est réservé aux seules personnes habilitées et les mises à jour critiques sont installées sans délai.

4.6. Continuité d'activité

Afin d'assurer la résilience et la continuité des activités en cas de sinistre, IDEX :

- Identifie les activités critiques ;
- Identifie les ressources nécessaires à ses activités ;
- Valide l'adéquation des mesures de sécurité de ces ressources avec les exigences des activités critiques ;
- Formalise un Plan de continuité d'activité (PCA)
- Planifie des simulations.

4.7. Conformité règlementaire

Aux fins d'éviter tout manquement aux obligations légales, réglementaires et aux exigences de sécurité, Idex poursuit son projet de mise en conformité et prévoit de :

- Réaliser des audits de sécurité sur son Système d'Information ;
- Planifier une revue régulière de la PSSI et de son application au sein du Groupe ;

5. REVUE DE LA POLITIQUE

Cette politique doit être régulièrement mise à jour par IDEX en collaboration avec le Délégué à la protection des données (DPO) pour rester pertinente, en particulier lorsque les exigences commerciales ou légales subissent un changement significatif.