Politique générale de protection des données personnelles

Table des matières

1) Objet et champ d'application de la politique

1.1 Objectifs

Scan-Match s'engage à assurer la protection des données obtenues dans le cadre de son activité, ainsi qu'à se conformer aux lois et réglementations applicables en matière de Traitement de Données à Caractère Personnel.

Cette politique a pour objectif d'assurer la mise en place par Scan-Match des principes imposés par le Règlement Européen n°2016/679 relatif à la protection des Données à Caractère Personnel, en date du 27 avril 2016, applicable depuis le 25 mai 2018 (ci-après RGPD).

1.2 Champ d'application

La Politique s'applique à l'ensemble des collaborateurs de Scan-Match.

Elle s'applique à toutes les Données à Caractère Personnel recueillies, traitées, partagées par Scan-Match en ligne et hors ligne, y compris :

- les sites internet opérés au sein de l'UE ;
- les pages officielles opérées sur les réseaux sociaux ;
- les emails échangés au sein de la société ;
- les conversations ou correspondances ;
- les documents papiers.

Une communication adéquate sur la Politique doit être réalisée par Scan-Match conformément à l'article 7 « Sensibilisation et Formation ».

La Politique est rendue obligatoire et exécutoire auprès de tous les collaborateurs Scan-Match. Scan-Match peut prendre des mesures disciplinaires à l'égard de ses collaborateurs, notamment en cas de non-respect des dispositions établies dans la Politique.

1.3 Application de la politique aux tiers

Sous réserve de dispositions législatives ou réglementaires contraires, la présente politique doit être appliquée aux Tiers qui ont accès ou à qui sont transmises les Données Personnelles des clients/collaborateurs de Scan-Match.

Scan-Match doit s'assurer que les contrats avec les Tiers ayant un accès aux Données Personnelles contiennent au minimum des dispositions sur :

- le périmètre de responsabilité ;
- la propriété des Données Personnelles ;
- les transferts internationaux des Données Personnelles, s'il y en a ;
- le respect des instructions et le recours à d'autres Sous-traitants ;

- la procédure de réponses aux requêtes et demandes des Personnes Concernées ;
- le sort des données à l'expiration du contrat ;
- l'obligation de sécurité et de confidentialité des Données Personnelles ;
- la possibilité pour le Responsable de Traitement de réaliser un audit auprès du Tiers ;
- la procédure en cas de violations des Données Personnelles (failles de sécurité).

2) Définitions

Dans le cadre de la présente Politique, les termes employés avec une majuscule auront le sens qui leur est donné par la présente section :

« **Données à Caractère Personnel/Données Personnelles** » désigne toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, N° de carte d'identité, salaire/rémunération, dossiers de santé, informations de compte bancaire, habitudes de conduite ou de consommation, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

« **Personne Concernée »** désigne l'individu sur lequel porte les « Données à Caractère Personnel » et qui peut être identifié ou distingué des autres, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à ses caractéristiques physique, physiologique, mentale, économique, comportementale, culturelle ou sociale. Cela inclut les étudiants, salariés, professeurs, prospects etc.

« Responsable de Traitement » désigne une personne qui, seule, individuellement ou conjointement, décide quelles Données à Caractère Personnel sont collectées, pourquoi et comment elles sont collectées et traitées. Dans la plupart des cas, ce serait la personne ou la société qui « possède » les données. Être le Responsable de Traitement ne signifie pas qu'il a la propriété des données et qu'il puisse les divulguer ou les utiliser comme il l'entend.
Au sens du Règlement Européen sur la protection des données à caractère Personnel, le Responsable de Traitement sera entendu au sens général comme le Dirigeant de l'entité, et par délégation de pouvoir expresse et écrite, les Responsables de Direction ou de métiers.

« Sous-Traitant » désigne toute personne ou société, non employée du Responsable de Traitement, qui traite des Données à Caractère Personnel au nom du Responsable de Traitement et selon ses instructions (par exemple des prestataires ou fournisseurs). Les Responsables de Traitement doivent assurer le maintien de la même obligation de diligence lorsqu'un Sous-Traitant traite des Données à Caractère Personnel en leur nom.

« Tiers » désigne toute personne physique ou morale, autorité publique, agence ou tout autre organisme autre que la Personne Concernée, le Responsable du Traitement, le Sous-Traitant et les personnes qui, sous l'autorité directe du Responsable du Traitement ou du Sous-

Traitant, sont habilitées ou autorisées à traiter les données (distributeurs, représentants désignés et Sous-Traitants, Réseau non propre, Clients Gestionnaires de Flotte etc….). Les partenaires commerciaux sont des Tiers au sens de la présente politique.

« **Traitement de Données à Caractère Personnel** » désigne 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 telles que la collecte, l'accès, l'enregistrement, la copie, la reproduction, le transfert, la recherche, le tri, la conservation, le stockage, la séparation, le croisement, la fusion, la modification, la structuration, l'adaptation, la mise à disposition, l'utilisation, la divulgation, la diffusion, la communication, l'extraction, l'enregistrement, l'organisation, l'adaptation, la divulgation par transmission ou toute autre forme de mise à disposition, la dissimulation, le déplacement, le rapprochement, l'interconnexion, la limitation, l'effacement, la destruction ainsi que la mise en œuvre d'autres actions sur les données, que ce soit de manière automatique, semi-automatique ou autre. Cette liste n'étant pas exhaustive.

« Destinataire » désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers.

« Consentement » de la personne concernée désigne toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

« Violation de données à caractère personnel » désigne une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ;

«Transfert de données » désigne toute communication, toute copie ou déplacement de données par l'intermédiaire d'un réseau, ou toute communication, toute copie ou déplacement de ces données d'un support à un autre, quel que soit ce support, dans la mesure où ces données ont vocation à faire l'objet d'un traitement dans le pays destinataire (exemple : Transfert à un fournisseur de services pour informatiser la collecte des données, call center étrangers, plateforme informatique internationale, maintenance IT internationale).

« Finalités de traitement » désigne l'objectif poursuivi par le traitement de Données à caractère personnel ou l'objectif principal d'une application informatique de données personnelles. Exemples de finalité : gestion des recrutements, gestion des clients, enquête de satisfaction, surveillance des locaux, etc.

3) Standards et exigences minimum

3.1 La transparence

Toutes les Données Personnelles collectées doivent être collectées et traitées de manière licite, loyale, et transparente au regard de la personne concernée.

3.1.1 Quelles informations fournir aux Personnes Concernées ?

Les informations suivantes doivent être systématiquement fournies aux utilisateurs du site internet de Scan-Match :

- l'identité et les coordonnées de Scan-Match en tant que Responsable de traitement,
- toutes les finalités du traitement ;
- les coordonnées du DPO ;
- la base juridique du traitement, le cas échéant, les intérêts légitimes poursuivis ;
- la durée de conservation ou les critères de détermination de cette durée ;
- le cas échéant, les destinataires ou catégories de destinataires ;
- les droits des personnes concernées ;
- le cas échéant, l'existence d'un transfert de données hors Union Européenne ainsi que informations et garanties qui s'y rattachent ;
- le cas échéant, le fait que la fourniture des données dépend d'une exigence à caractère réglementaire ou contractuel ;
- le cas échéant, le fait que la fourniture des données conditionne la conclusion d'un contrat ;
- l'existence d'une obligation pour la personne concernée de fournir ses données ;
- les conséquences de la non fourniture des données ;
- le cas échéant, le droit de retirer son consentement pour les traitements basés sur le consentement ;
- le cas échéant, l'existence d'une décision automatisée et les informations qui s'y rattachent ;
- le cas échéant, l'existence d'un traitement ultérieur pour une autre finalité et les informations qui s'y rattachent.

3.1.2 Quand informer les Personnes Concernées ?

Les informations doivent être communiquées au plus tard au moment de la collecte des Données à Caractère Personnel, de façon concise, transparente, compréhensible, aisément accessible et en des termes clairs et simples.

3.1.3 Par quels moyens informer les Personnes Concernées ?

Ces informations doivent être fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique. Lorsque la Personne Concernée en fait la demande, les informations peuvent être fournies oralement, à condition que l'identité de la Personne Concernée soit démontrée par d'autres moyens.

3.2 La minimisation et l'adéquation

Les Données à caractère personnel collectées pour toute finalité doivent être pertinentes et non excessives par rapport au but poursuivi par le Traitement. En d'autres termes, seules les Données strictement nécessaires aux finalités doivent être collectées.

Afin d'accomplir cette obligation, le Responsable de Traitement doit réaliser un test de proportionnalité ou d'adéquation avant la mise en place du projet ou du traitement. Ce test de proportionnalité passera nécessairement par la réalisation d'une analyse d'impact sur la vie privée conformément à la procédure mise en place par Scan-Match en la matière.

Par ailleurs, les Données à Caractère Personnel collectées doivent être exactes, complètes et, si nécessaire, mises à jour.

Exemple de questions à se poser pour assurer la minimisation :

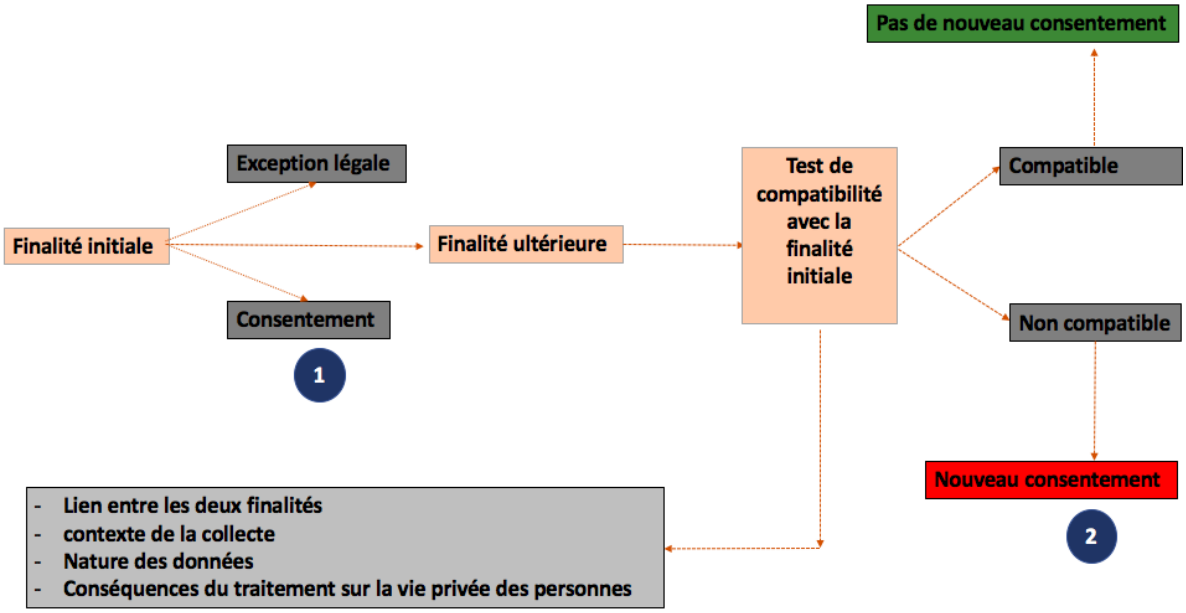
- Pourquoi ai-je besoin de collecter ces données ?
- Quelles sont les données indispensables pour atteindre mon objectif ?
- Les données obligatoires ont-elles été marquées par un astérisque non obligatoire ?

3.3 Le respect des finalités de traitement

Avant toute collecte des Données Personnelles, le Responsable de Traitement doit définir de façon claire tous les objectifs poursuivis par la collecte.

Les Données à Caractère Personnel ne doivent pas être traitées pour une finalité ultérieure incompatible avec la finalité initiale pour laquelle les données ont été collectées.

Pour pouvoir effectuer tout traitement ultérieur dont la finalité est incompatible avec la finalité initiale, le Responsable de Traitement doit s'assurer qu'il a reçu le consentement de la Personne Concernée pour cette nouvelle finalité et dans le cas contraire recueillir le consentement de la Personne Concernée ou répondre à une autre condition de licéité (exécution d'un contrat, respect d'une obligation légale, etc.)



3.4 Le consentement

Lorsque le traitement de Données Personnelles repose sur le Consentement de la Personne Concernée, Scan-Match démontre que le consentement a bien été donné, qu'il a été enregistré et tracé dans un système informatique.

Les traitements concernés sont :

- utilisation de photographies et vidéo des participants aux évènements à des fins d'informations et de communication ;
- utilisation des photographies des collaborateurs de Scan-Match sur le site internet.

Afin d'obtenir le consentement des personnes concernées, Scan-Match respecte les exigences suivantes :

- lorsque la demande de Consentement est faite par écrit et qu'elle concerne également d'autres questions, la demande doit être présentée de façon distincte par rapport à ces autres questions ;
- la demande de Consentement faite par écrit est établie sous une forme compréhensible, aisément accessible, formulée en des termes clairs et simples ;
- la demande de Consentement n'est pas formulée de manière contraignante pour la Personne Concernée ;
- Scan-Match s'assure que le Consentement est donné librement, notamment lorsque l'exécution d'un contrat est subordonnée au consentement de la Personne Concernée au traitement de ses Données à caractère personnel, alors qu'un tel traitement ne serait pas nécessaire à l'exécution de ce contrat.

Scan-Match met en place une procédure interne relative à la gestion des consentements (suivi, retrait des consentements). La Personne Concernée doit être mise en mesure de retirer son Consentement à tout moment et Scan-Match l'informe des moyens permettant de retirer son consentement notamment à travers les mentions d'information fournies au moment de la collecte des Données. Ces moyens doivent permettre à la personne concernée de retirer son consentement aussi simplement qu'il a été donné (ex. lien de désinscription aux newsletters).

La procédure interne de gestion des consentements permet de répercuter les consentements et les retraits de consentement dans les applications utilisées et le système d'information.

3.5 Durée de conservation

Scan-Match ne conserve pas les Données à Caractère Personnel plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont collectées.

Dans ce cadre, Scan-Match met en œuvre une politique documentée de conservation des Données à Caractère Personnel qui précise la durée de conservation, les conditions de conservation ainsi que leur format de stockage.

De manière générale, la durée maximale de conservation des données doit être déterminée en fonction de la finalité de chaque Traitement en prenant en compte :

- les obligations légales ;
- les recommandations de la CNIL ;
- les meilleures pratiques dans chaque domaine concerné ;
- les besoins opérationnels.

Par ailleurs, les Données à Caractère Personnel sont détruites dès lors qu'elles ne sont plus nécessaires aux finalités pour lesquelles elles ont été obtenues ou enregistrées. Avant leur effacement, elles sont stockées d'une manière permettant l'exercice du droit d'accès des Personnes Concernées. Elles peuvent être conservées pendant une durée résultant de relations ou obligations juridiques, de l'exécution d'un contrat ou de l'application de mesures précontractuelles demandées par la personne concernée.

Chaque année, Scan-Match procède à une revue des données. En dehors des cas dans lesquels il existe une obligation d'archivage, les Données Personnelles qui ne présentent plus d'intérêt sont supprimées sans délai. Lors des procédures de suppression automatique, Scan-Match s'assure que les données sont effectivement supprimées par l'établissement d'un certificat de destruction.

3.6 Droit des Personnes Concernées

De manière générale, le Règlement européen sur la Protection des Données accorde aux Personnes Concernées les droits :

- d’être informées lorsque les Données à Caractère Personnel sont enregistrées pour la première fois par Scan-Match pour ses besoins propres ;
- de demander des informations sur les données enregistrées les concernant, y compris des informations concernant la source des données ;
- de demander les destinataires auxquels les données sont transférées ;
- de demander la finalité de l'enregistrement des données ;
- de demander l’accès aux données les concernant, y compris sous forme de liste fournie par écrit ou par voie électronique ;
- de demander la rectification des données, quand elles sont inexactes ;
- de demander la suppression de données si cela est légalement possible ;
- d’obtenir la limitation du traitement de leurs Données à caractère personnel lorsque cela est légalement possible ;
- de s’opposer au traitement de leurs Données à caractère personnel par Scan-Match ;
- de demander la portabilité de leurs Données à caractère personnel ;
- d’obtenir toute autre information qui serait exigée par la loi.

Lorsqu’une Personne Concernée fait valoir ses droits soit par voie écrite (y compris par voie électronique) soit par voie orale, Scan-Match répond à la Personne Concernée dans un délai de 30 jours. Si la demande est complexe ou si la Personne Csoncernée effectue un trop gros volume de demande, le délai est alors porté à 60 jours. Dans cette hypothèse, la Personne Concernée devra être notifiée de la prolongation du délai de réponse. Les éléments communiqués doivent être aisément compréhensibles

Scan-Match met en place une organisation interne spécifique afin de traiter les demandes des Personnes Concernées. Les modalités de cette organisation sont détaillées dans une procédure de gestion des demandes.

3.7 Sécurité des données

Des mesures de contrôle et procédures appropriées sont mises en œuvre par Scan-Match, afin d’assurer la sécurité des Données à Caractère Personnel et de prévenir tout accès ou divulgation non autorisés.

Scan-Match prend des mesures raisonnables pour mettre en place des systèmes organisationnels efficaces et des mesures organisationnelles, physiques et techniques. Ces mesures concernent spécifiquement, la collecte, l’utilisation, le traitement, la transmission, le transfert, le stockage et la destruction des Données à Caractère Personnel.

Elles visent ainsi à :

- empêcher les personnes non autorisées d'avoir accès aux systèmes de traitement des données d’information pour traiter ou utiliser des Données à Caractère Personnel (contrôle d'accès) ;
- s’assurer que seules les personnes habilitées à accéder aux données peuvent y avoir accès dans la limite de la finalité pour laquelle les données sont traitées. Ces personnes

doivent garantir la confidentialité des Données à Caractère Personnel auxquelles elles ont accès ;

- s'assurer que les personnes autorisées à utiliser un système de traitement des données n'ont accès qu'aux seules données auxquelles elles sont autorisées à accéder, et que les Données à Caractère Personnel ne peuvent pas être lues, copiées, altérées ou supprimées sans autorisation pendant le Traitement, l'utilisation et après l'enregistrement (contrôle d'accès, principe du besoin d'en connaître) ;
- s'assurer que les Données à Caractère Personnel ne peuvent pas être lues, copiées, modifiées ou supprimées sans autorisation pendant le transport, le transfert électronique ou l'enregistrement sur des supports de stockage, et qu'il est possible de vérifier et de contrôler les personnes qui transfèrent des Données à Caractère Personnel à l'aide de moyens de transferts de données (contrôle de divulgation) ;
- s'assurer qu'il est possible de contrôler et de vérifier si les Données à Caractère Personnel ont été ajoutées, modifiées ou supprimées des systèmes de traitement de données et si tel est le cas, par qui (contrôle d'entrée) ;
- s'assurer que les Données à Caractère Personnel traitées pour le compte d'autrui sont en stricte conformité avec les instructions du Responsable de Traitement (contrôle des tâches) ;
- s'assurer que les Données à Caractère Personnel sont protégées contre la destruction accidentelle ou la perte (contrôle de disponibilité) ;
- s'assurer que les Données à Caractère Personnel collectées pour des finalités différentes peuvent être traitées séparément ;
- s'assurer que l'anonymisation des Données à Caractère Personnel est effective lorsqu'elle est requise par une loi pour mettre en œuvre le traitement.

Scan-Match identifie les risques qui pèsent sur la vie privée des personnes engendrés par son Traitement en menant des analyses d'impact sur la vie privée avant de déterminer les mesures de sécurité adéquates pour réduire ces risques, le niveau des mesures de sécurité nécessaires pour la protection des données dépendant de la sensibilité des données.

Les Données à Caractère Personnel détenues par Scan-Match peuvent notamment contenir des mesures telles que la pseudonymisation, le cryptage ou l'anonymisation en fonction des risques.

Par ailleurs, un plan de reprise d'activité est mis en place afin de restaurer la disponibilité et l'accès aux données personnelles en temps opportun en cas d'incident physique ou technique.

Enfin, ces mesures peuvent prendre la forme d'un processus pour tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles afin d'en assurer le traitement.

3.8 Privacy by design et privacy by default

Pour tout nouveau projet impliquant le traitement de données personnelles, Scan-Match prend en compte le Privacy By Design et le Privacy By Default.

A cet effet, Scan-Match met en place des mesures visant à protéger les données personnelles dès la conception du projet, mais aussi tout au long du projet et du cycle de vie de la donnée (de la collecte à la destruction).

Seules les Données Personnelles strictement nécessaires au regard de la finalité du Traitement doivent être collectées. Scan-Match s'engage à paramétrer le service proposé de façon à ce que, par défaut, la vie privée des personnes soient respectées au plus haut degré possible, sans toutefois empêcher le Traitement d'atteindre sa finalité.

3.9 Relations avec les sous-traitants

Avant tout recours à un prestataire devant traiter les Données Personnelles, Scan-Match vérifie que celui-ci présente toutes les garanties en matière de protection des Données Personnelles.

Exemples de question à poser pour s'assurer du niveau de conformité des Sous-Traitants :

- Avez-vous une politique de protection des données ?
- Avez-vous nommé un délégué à la protection des données
- Avez-vous une politique de sécurité permettant d'éviter toute divulgation non autorisée, une perte ou altération des données ?
- Avez-vous une politique pour la gestion des droits des personnes ?
- Avez-vous des procédures pour assurer la suppression des données ?
- Les membres de votre personnel sont-ils sensibilisés à la protection des données ?
- Les données seront-elles hébergées au sein de l'Union Européenne ?

Par ailleurs, un contrat écrit doit être signé entre Scan-Match et ses Sous-Traitants. Ce contrat doit prévoir que le prestataire :

- s'engage à mettre en œuvre et à maintenir les mesures techniques et organisationnelles de nature à garantir un niveau de sécurité, d'intégrité et de confidentialité adapté au risque du ou des traitements qui lui sont confiés ;
- n'agit que sur les instructions de Scan-Match ;
- s'interdit d'utiliser ou traiter les données à une fin autre que celle prévue par ledit contrat ;
- n'acquiert aucun droit ou propriété sur les données et ne doit les communiquer à d'autres personnes même pour leur conservation ;
- demande l'autorisation à Scan-Match pour Sous-Traiter la prestation dont il a la charge ;
- supprime les Données Personnelles à l'issu de la relation contractuelle.

3.10 Accountability

Scan-Match respecte le principe d'*accountability*. A cet effet, Scan-Match conserve toutes les preuves du respect de la réglementation en matière de protection des Données à Caractère Personnel.

Scan-Match est en mesure de démontrer par des preuves tangibles que les mesures de conformité appropriées ont été mises en œuvre.

3.11 Registre de traitements

Scan-Match tient à jour un registre des traitements qui contient les informations suivantes :

- le nom et les coordonnées du responsable de traitement et du DPO ;
- les finalités du traitement ;
- une description des catégories de Personnes concernées et des catégories de Données à caractère personnel ;
- les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées ;
- les transferts de données vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et les documents attestant de l'existence de garanties appropriées ;
- les durées de conservation prévues pour les différentes catégories de données ;
- une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre pour le traitement en question.

Le DPO est responsable de la tenue du registre de Scan-Match. Avec la contribution des collaborateurs en charge du traitement et/ou les responsables de direction il s'assure que tout nouveau Traitement est inscrit au registre avec les informations décrites ci-dessus. Le DPO valide les traitements renseignés et veillera à la mise à jour du registre.

Ce registre est tenu sous forme électronique (via le logiciel myDPO) et est mis à disposition de la CNIL sur demande.

4) Gouvernance de la protection des données

4.1 Missions et responsabilités du DPO

Afin de garantir la conformité des traitements de Données à Caractère Personnel, Scan-Match a nommé un Délégué à la Protection des Données (DPO) externalisé.

La mission principale du DPO est de faire en sorte que Scan-Match soit en conformité constante avec le cadre légal relatif aux données personnelles.

Le DPO assure les missions suivantes :

- conseil sur la conformité des nouveaux traitements ;
- conseil sur les études d'impact sur la vie privée ;
- point de contact de la CNIL et gestion des demandes de la CNIL ;
- audit annuel de conformité au RGPD ;
- sensibilisation du personnel (e-learning) ;
- bilan annuel au Responsable de Traitement ;

- veille data privacy ;
- registre des traitements du Responsable de Traitement ;
- registre des traitements du Sous-Traitant ;
- point de contact pour les personnes concernées ;
- audit annuel sur pièce et entretien de conformité au RGPD ;
- assistance en cas de contrôle de la CNIL ;
- gestion documentaire de la conformité ;
- reporting semestriel d'activité ;
- violation de données personnelles ;
- livrables documentaires.

4.2 Missions et responsabilités des collaborateurs de Scan-Match

4.2.1 Missions générales

Chaque collaborateur concerné par le traitement de Données Personnelles devra respecter les obligations suivantes vis-à-vis du DPO :

- indiquer les coordonnées du DPO sur tous les supports de collecte des Données à caractère personnel et mentions d'information (adresse postale, numéro de téléphone ou adresse électronique dédié) conformément à leur périmètre d'intervention ;
- associer le DPO dès la phase de conception dans tous outils ou produits répertoriant toutes Données à Caractère Personnel et le cas échéant documenter et justifier par écrit les raisons pour lesquelles l'avis du DPO n'a pas été suivi lorsque celui-ci a été exprimé ;
- répondre à toute demande d'information du DPO sur tous les sujets ayant un impact sur la vie privée des personnes ;
- fournir les accès à toutes les documentations relatives aux Traitements de données et aux procédures associées et mettre en place une structure documentaire permettant de faciliter cet accès.

4.2.2 Missions relatives aux ressources humaines

Dans le cadre du Traitement des Données Personnelles relatives ressources humaines, les obligations suivantes devront être respectées :

- assurer une information complète aux collaborateurs et aux candidats ;
- garantir et suivre l'exercice des droits par les collaborateurs /candidats ;
- assurer une formation adéquate en droit des Données à caractère personnel aux opérationnels qui traitent de la Donnée et établir un registre des formations ;
- garantie le respect de la politique ressources humaines (cf. Article 5) en matière de protection des Données à caractère personnel.

4.2.3 Missions relatives aux systèmes d'information

Les collaborateurs en charge des systèmes d'information devront :

- mettre en place des procédures de tests et d'évaluation pour vérifier l'efficacité des mesures de sécurité techniques et organisationnelles ;
- assurer la purge des Données Personnelles à l'expiration de leur durée de conservation ;
- mettre en place une procédure de gestion des failles de sécurité et établir un registre ;
- être garant du respect des mesures de sécurité par le personnel (politique de sécurité du système d'information) ;
- être garant de la procédure relative à la prise en compte du respect de la protection de la vie privée pour tout nouveau Traitement.

5) Traitement des données RH

5.1 Modalités de traitement des données

La gestion des ressources humaines donne lieu à un grand nombre de traitements de Données à Caractère Personnel ; lesquels font usage des Données à caractère personnel que Scan-Match a collectées :

- directement auprès des collaborateurs à l'occasion du processus de recrutement, de la conclusion du contrat de travail ou suite à l'exécution du contrat de travail ;
- indirectement auprès d'autres employés habilités de Scan-Match, dans le cadre de la relation de travail, notamment dans le cadre de processus d'évaluation (évaluation par les managers par exemple), de formation ;
- indirectement et de manière automatisée, dans le cadre de l'utilisation des locaux, systèmes d'information et d'autres outils mis à disposition par Scan-Match (en ce compris, ordinateurs, téléphones, outils connectés, application, etc.) ;
- indirectement auprès tiers, pour les besoins de la gestion de la relation de travail à savoir :
    - vérification des diplômes et référence, après accord de la Personne Concernée ;
    - communication de résultats de test, examens, suivis dans le cadre de la formation professionnelle ;
    - certificats d'aptitudes reçus de la médecine du travail ;
    - informations collectées ou transmises par des organismes sociaux ou d'administratif.

5.2 Droit des Personnes Concernées

Les collaborateurs disposent d'un droit d'accès et de communication à leurs Données Personnelles, de celui de faire rectifier ou compléter celles qui seraient inexactes ou incomplètes, ainsi que de demander la limitation du traitement de ces Données.

Dans certains cas limitativement prévus par la loi, les collaborateurs disposent d'un droit à la portabilité leur permettant de récupérer leurs Données Personnelles dans un format

interopérable dès lors que les Données Personnelles concernées sont fournies sur la base de leur consentement ou en exécution de leur contrat. Ce droit ne s'exerce toutefois pas aux Données Personnelles traitées par Scan-Match, sur la base d'un intérêt légitime ou d'obligations légales.

Lorsque le traitement des Données Personnelles repose sur le consentement, il peut à tout moment être retiré.

Les collaborateurs peuvent également, mais uniquement pour des motifs légitimes, s'ils estiment que le traitement de leurs Données Personnelles n'est plus nécessaire au regard des finalités pour lesquelles elles ont été collectées, ou s'ils ont retiré leur consentement, demander l'effacement de leurs Données Personnelles ou demander la limitation de leur traitement. Scan-Match ne pourra s'opposer à une telle demande que pour des motifs légitimes lui imposant de conserver vos Données Personnelles.

Les collaborateurs disposent également du droit de définir des directives relatives au sort de leurs Données Personnelles après votre mort.

Les collaborateurs peuvent exercer leurs droits directement à l'adresse suivante dpo@captag.fr.

Ils peuvent également saisir la Commission Nationale de l'Informatique et des Libertés (CNIL), 3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07, Tel : 01 53 73 22 22, de toute réclamation se rapportant à la manière dont Scan-Match collecte et traite leurs Données Personnelles.

5.3 Sécurité des données

Scan-Match prend toutes les précautions, mesures techniques et organisationnelles nécessaires pour garantir la sécurité, l'intégrité et la confidentialité des Données à caractère personnel que de ses collaborateurs et en particulier, pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

À cette fin, Scan-Match a mis en place les mesures techniques et organisationnelles suivantes :

- les accès aux ordinateurs sont protégés par un mot de passe ;
- un verrouillage automatique de la session est paramétré au bout de cinq minutes ;
- l'accès au dossier informatique contenant des collaborateurs est limité aux seules personnes qui ont réellement besoin d'y accéder ;
- les collaborateurs habilités et chargés de traiter des Données à caractère personnel ont été formé/ sensibilisé à la protection de ces Données.

Ces mesures sont détaillées dans la politique de sécurité des systèmes d'information.

6) Obligations en tant que sous-traitant

Dans le cadre de son activité principale, Scan-Match intervient comme sous-traitant de Données Personnelles de ses clients.

En tant que sous-traitant, Scan-Match doit notamment offrir à ses clients des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées.

6.1 Transparence et traçabilité

Scan-Match transmet au Responsable de Traitement toutes les informations sur la manière dont sont traitées les Données Personnelles.

Les principes de transparence et de traçabilité imposent la rédaction d'un contrat entre Scan-Match et son client, qui précise les obligations des parties.

Scan-Match doit tenir informé ses clients des sous-traitants auxquels il fait appel pour fournir ses services.

Scan-Match doit choisir des Sous-Traitants qui offrent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées pour protéger les données personnelles.

6.2 Tenir un registre sous-traitant

Scan-Match tient un registre des traitements effectués pour le compte du Responsable de Traitement.

Le registre est tenu à la disposition des clients qui peuvent en demander la communication à tout moment.

6.3 Obligation de documentation

Scan-Match documente l'ensemble des actions menées pour sa mise en conformité.

La documentation obligatoire comprend notamment :

- le registre de traitement en tant que Sous-Traitant,
- le registre de l'ensemble des failles de sécurités ;
- la preuve de l'information des Personnes Concernée, et le cas échant, son consentement explicite, de manière traçable et conservé ;
- les politiques de sécurité existantes.

6.4 Conservation des instructions clients

Scan-Match recense **par écrit** les instructions reçues de clients. Pour toute instruction donnée par voie orale, le collaborateur Scan-Match doit demander une confirmation par écrit par l'intermédiaire d'un e-mail ou d'un courrier.

Par exemple, il est important de recenser toutes les demandes de suppressions et de transfert de données.

6.5 Obligation d'assistance, d'alerte et de conseil

6.5.1 Obligation d'assistance

Scan-Match en tant que Sous-Traitant a le devoir d'assister le client dans la gestion des droits des personnes. Ainsi sur instructions du client, Scan-Match pourra être acteur de la gestion des droits des personnes.

Scan-Match a également le devoir d'aider le client à respecter ses obligations de sécurité.

Enfin, Scan-Match a l'obligation d'assister le client dans l'hypothèse où une analyse d'impact sur la vie privée doit être effectuée par le Responsable de traitement. L'assistance consiste *a minima* à fournir toutes les informations relatives au traitement et particulièrement les mesures de sécurité associées au traitement.

6.5.2 Obligation d'alerter

Scan-Match est dans l'obligation d'alerter le Responsable de Traitement en cas de faille de sécurité concernant les Données Personnelles de son client, par une notification de faille.

Le détail du contenu de cette notification, ainsi que les modalités d'alerte sont contenus la procédure de gestion des failles de sécurité.

6.5.3 Obligation de conseil

Scan-Match a le devoir d'informer son client quand une instruction de ce dernier constitue une violation des règles en matière de protection des données personnelles.

6.6 Obligation de sécurité

Scan-Match doit veiller à mettre en œuvre des mesures adaptées pour garantir la sécurité des données de ses clients.

La politique de sécurité des systèmes d'information détaille ces mesures et leurs modalités de mise en œuvre.

7) Sensibilisation et formation

Le Responsable de Traitement doit s'assurer que les collaborateurs de Scan-Match sont sensibilisés et formés aux principes de la présente Politique ainsi qu'aux exigences de toutes autres lois, réglementations, règles et procédures relatives à la protection des Données à Caractère Personnel, lorsqu'ils sont impliqués dans le Traitement de Données à Caractère Personnel.

Les séances de formation ou de sensibilisation peuvent être dispensées sous les formes suivantes :

- e-learning ;
- séances en présentiel ;
- lettres d'information internes.

En particulier, les collaborateurs concernés devraient être régulièrement informés des évolutions législatives ou jurisprudentielles en matière de protection des Données à Caractère Personnel.