Politique de confidentialité Générale UE

Groupe Bondioli & Pavesi

1. AVANT-PROPOS

Le Groupe Bondioli & Pavesi attribue une grande importance au respect de la protection de la vie privée et des normes sur la protection des données à caractère personnel pour le bon développement de ses activités, de son commerce et de son image sur le marché. La protection des données personnelles que chaque entreprise du groupe collecte et stocke, avec des systèmes électroniques ou traditionnels, représente une valeur pertinente et stratégique pour le groupe et pour le développement des activités.

Dans cette optique, le règlement (UE) 2016/679 (ci-après également dénommé "**RGPD**") représente le cœur de la nouvelle législation européenne en matière de protection des données personnelles et constitue la base principale des activités impliquant des données personnelles au sein de l'UE.

Pour cette raison, il est essentiel d'adopter une politique commune de protection de la vie privée (ci-après "**Politique**") pour les entreprises situées dans l'UE indiquées au point 3 (ci-après dénommées comme "**Entreprise**" et, collectivement, le "**Groupe UE**") et d'informer tous les employés et ceux qui travaillent au nom et pour le compte des différentes Entreprises des principes et des règles que le Groupe UE entend suivre afin de garantir un niveau uniforme et élevé de protection des informations à caractère personnel.

Compte tenu de la complexité des règlements, d'une part, et des processus d'entreprise impliquant des données à caractère personnel, d'autre part, il est d'abord nécessaire d'adopter une structure de gouvernance de la vie privée au sein des Entreprises du Groupe UE, définissant la structure des rôles, responsabilités et tâches relatifs à la protection des données à caractère personnel.

2. BUT

Cette Politique est destinée à décrire :

(i). les principes et procédures que chaque Entreprise doit suivre dans le traitement des données à caractère personnel,
(ii). l'organisation de protection de la vie privée pour gérer la gouvernance de la matière, et
(iii). l'attribution des tâches et des responsabilités des différents niveaux opérationnels.

Pour cette raison, la Politique doit être portée à l'attention de toutes les personnes qui traitent des données personnelles dans les Entreprises.

3. SECTEUR D'APPLICATION

Cette politique doit être respectée par les Entreprises suivantes :

- toutes les entreprises italiennes appartenant au groupe Bondioli & Pavesi ;
- Bondioli & Pavesi GMBH ;
- Bondioli & Pavesi France SA ;
- Bondioli & Pavesi Iberica SA ;
- Bondioli & Pavesi Sp. Zo.o. ;
- OM Protivin AS.

Chacune d'elles, en plus de respecter la politique suivante, doit évidemment se conformer au RGPD et aux réglementations locales supplémentaires sur la protection de la vie privée et des données personnelles.

4. DÉFINITIONS

Aux fins de cette politique, les définitions suivantes, dérivées du RGPD, sont fournies par ordre de pertinence :

- **données à caractère personnel** : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «**Personne Concernée**»); est réputée être une personne physique identifiable, une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
  En outre, en cas d'activités de marketing non demandées par le destinataire (par exemple, envoi spontané de matériel publicitaire, vente directe, étude de marché ou communication commerciale), également toute information relative à une personne morale - y compris les organismes ou associations -.
  Par exemple : données personnelles, adresses postales, téléphoniques, télématiques, codes d'identification, commandes, chiffre d'affaires, image, voix, curriculum, habitudes d'achat, journaux d'accès au système et, plus généralement, de tout ce qui est enregistré sur papier ou sur ordinateur et qui peut être associé à une personne identifiée ou identifiable.

- **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, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.
  Par exemple : la gestion des salaires et des présences des employés, la gestion des contrats, l'envoi de communications marketing, le profilage, la vidéosurveillance, etc.

- **Catégories spéciales de données à caractère personnel :** données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, ou l'appartenance syndicale, ainsi que les données génétiques, les données biométriques destinées à identifier de manière unique une personne physique, les données concernant la santé ou la vie sexuelle ou l'orientation sexuelle de la personne. Il s'agit d'un sous-ensemble de données à caractère personnel.
  Par exemple : les certificats de maladie, les adhésions à un syndicat, les congés syndicaux, les handicaps, les blessures, l'appartenance à un parti, l'état de santé, etc.

- **Données à caractère personnel relatives aux condamnations pénales et aux infractions :** (ci-après "**Données judiciaires**") les données à caractère personnel relatives aux condamnations et infractions pénales ou aux mesures de sûreté qui y sont liées. Il s'agit d'un sous-ensemble de données à caractère personnel.

- **Responsable du traitement** : la personne physique ou morale, l'autorité publique, le service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel.
  Par exemple, si le site est entièrement géré par Bondioli & Pavesi S.p.A., le traitement des données qui y sont relatives sera effectué en qualité de Responsable.
  Chaque entreprise sera responsable du choix en autonomie de la manière dont elle effectuera le traitement. Par exemple, le traitement des données relatives aux employés implique que chaque entreprise soit responsable du traitement.

- **Sous-traitant** : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement conformément à l'art. 8 du RGPD.

- **Personne Autorisée au traitement :** (également appelé Personne chargée du traitement) la personne physique qui traite les données à caractère personnel sous l'autorité directe du responsable ou du sous-traitant ;

- **Personne Concernée**. La personne physique identifiée ou identifiable à laquelle se réfèrent les données à caractère personnel. En outre, dans l'hypothèse d'activités de marketing non demandées par le destinataire (par exemple, envoi spontané de matériel publicitaire, vente directe, étude de marché ou communication commerciale), la partie intéressée est également la personne morale - y compris les organismes ou associations - comme le prévoit la directive (UE) "Vie privée et communications électroniques" 2002/58, et ses ajouts et modifications ultérieures.
  Ce sont, par exemple : les clients, y compris les clients potentiels, les employés, les candidats à l'emploi, les consultants, les fournisseurs, les visiteurs, les utilisateurs des sites web du Responsable, etc.

5. MODÈLE D'ORGANISATION DU GROUPE UE EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE

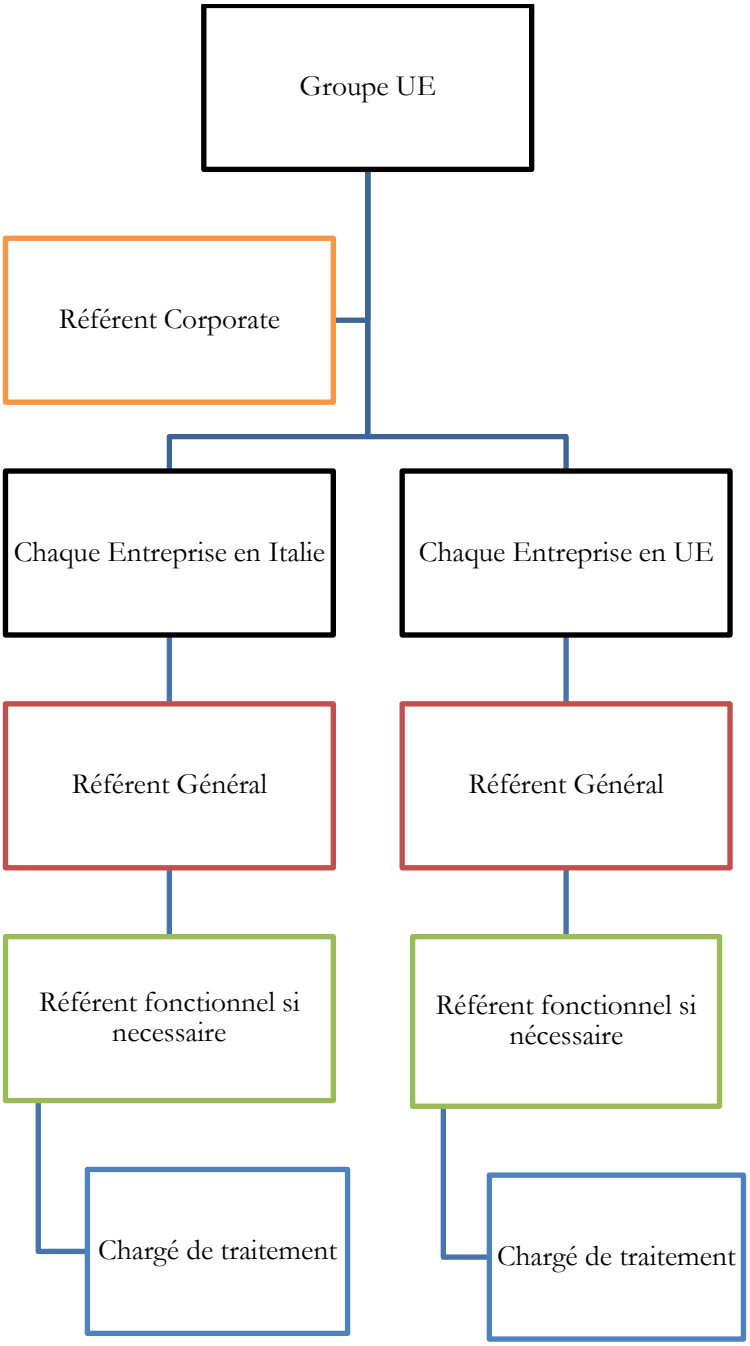
Afin de rendre ses activités de protection des données personnelles homogènes, le Groupe UE a décidé d'adopter le modèle organisationnel suivant :

- **Référent corporate** : brièvement, il a pour tâche de coordonner la question au niveau de l'ensemble du Groupe UE et de fournir des orientations fonctionnelles à tous les référents pour la protection de la vie privée nommés au sein du Groupe UE. Une liste détaillée des responsabilités et des taches est reportée dans le document PRCY011 disponible sur l'intranet de l'entreprise;

- **Référent général :** brièvement, il a pour tâche de coordonner le sujet au niveau de l'Entreprise qui l'a nommé, considérée dans son ensemble, et de fournir une orientation fonctionnelle à tous les Référents fonctionnels qui peuvent être nommés au sein de la même Entreprise. Une liste détaillée des responsabilités et des taches est reportée dans le document PRCY014 disponible sur l'intranet de l'entreprise;
- **Référent fonctionnel :** brièvement, il a pour tâche de coordonner la matière au niveau du service qui lui est attribué au sein de l'Entreprise qui l'a nommé. Une liste détaillée des responsabilités et des taches est reportée dans le document PRCY015 disponible sur l'intranet de l'entreprise. Ce Référent est nommé seulement si le Référent général le juge nécessaire.
- **Personne autorisée / chargée du traitement** : c'est la personne physique qui effectue matériellement les opérations de traitement des données, à l'aide d'outils informatiques et/ou au moyen de supports papier au sein du service de l'entreprise auquel elle est affectée. Chaque Entreprise doit désigner comme Personne chargée du traitement chacun de ses employés qui traite des données à caractère personnel durant l'exécution de ses fonctions. Le document pour la nomination de Personne chargée du traitement avec la définition de l'étendue du traitement autorisé, les instructions données et les tâches confiées est reportée dans le document PRCY016 disponible sur l'intranet de l'entreprise.

6. SCHÉMA ORGANISATIONNEL PRIVACY UE

Compte tenu de ce qui précède, le schéma organisationnel de la protection de la vie privée est le suivant :



7. AUTRES SUJETS INTÉRESSÉS

D'autres parties peuvent être impliquées dans la gestion des données à caractère personnel, notamment :

- **Sous-traitant du traitement :** comme nous l'avons déjà vu, il s'agit de la partie externe qui effectue le traitement des données à caractère personnel au nom du responsable du traitement. Ce traitement doit avoir lieu sur la base d'un contrat écrit stipulant la matière réglementée, la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel, les catégories de personnes concernées, les obligations et les droits du responsable du traitement.

Dans le contexte de l'UE, un tel contrat doit également contenir les éléments essentiels prescrits par l'article 28, paragraphe 3, du RGPD.
Les services qui peuvent généralement être externalisés aux sous-traitants sont, par exemple, la gestion des salaires, la gestion de site web, la gestion du support informatique, etc.

- **DPO** : le Délégué à la Protection des Données ou Data Protection Officer, est un rôle prévu par le RGPD aux art. 37 et suivants, qu'une société doit désigner quand :
  - les activités principales du responsable du traitement ou du sous-traitant consistent en des traitements qui, en raison de leur nature, de leur champ d'application et/ou de leurs finalités, nécessitent un suivi régulier et systématique des personnes concernées sur une grande échelle ; ou
  - les activités principales du responsable du traitement ou du sous-traitant consistent à traiter, à grande échelle, des catégories particulières de données à caractère personnel visées à l'article 9 du RGPD ou des données relatives aux condamnations pénales et aux infractions visées à l'article 10 du RGPD.

  Ses principales missions sont de veiller au respect du RGPD, de conseiller l'entreprise, de surveiller les opérations, de former et de sensibiliser à ce sujet, etc.

  La désignation d'un DPO a été jugée non nécessaire pour les Entreprises car, compte tenu de l'activité des Entreprises, qui, par nature, ne comporte aucun risque dans le domaine de la protection des données à caractère personnel, compte tenu du traitement minimal des données à caractère personnel des personnes concernées, certainement pas à grande échelle, et compte tenu du fait que le traitement de catégories particulières de données dans le cadre de la relation de travail ne constitue pas une activité principale mais une activité auxiliaire (voir WP29, Lignes directrices DPO, 2.1.2., p. 9), il ne semble pas que les conditions susmentionnées existent.
  Si les directives ou réglementations locales exigent la nomination d'un DPO dans l'une des Entreprises (autres que celles situées en Italie), la circonstance doit être signalée à l'avance au Référent corporate.

- **Autres sujets potentiels :** les réglementations locales peuvent exiger l'identification d'autres sujets pertinents pour la protection des données à caractère personnel. Chaque Entreprise a l'obligation d'évaluer s'il existe une législation locale imposant de telles obligations.
  En Italie, par exemple, un rôle d'Administrateur Système est prévu qui c'est à dire les personnes physiques chargées de la gestion technique de l'ensemble du système de communication ou même d'une seule de ses composantes ou des activités connexes. Ces personnes doivent recevoir une désignation spécifique d'Administrateur Système et des instructions spécifiques.

8. PRINCIPES GÉNÉRAUX

En ce qui concerne le traitement des données à caractère personnel, le Groupe UE entend adopter toutes les mesures technologiques, organisationnelles et logistiques les plus appropriées pour garantir le respect effectif des garanties de protection des données à caractère personnel.

Dans ce but, les processus d'entreprise et les opérations de traitement des données effectués par les employés, les sujets chargés du traitement, doivent respecter les principes suivants.

8.1. **Licéité, équité et transparence**

Le traitement des données à caractère personnel ne doit être effectué que si une des conditions prévues par la loi est remplie, que si la personne concernée en a connaissance et qu'il correspond à ce qui lui a été déclaré.

8.2. **Limitation des finalités**

Les données à caractère personnel ne doivent être traitées qu'aux fins déclarées à la personne concernée et ne doivent pas être incompatibles avec ces fins.

8.3. **Minimisation**

L'utilisation des données à caractère personnel doit être réduite au minimum et donc si les finalités peuvent être atteintes sans l'utilisation de données à caractère personnel, le traitement doit être effectué avec des données anonymes. Les données anonymes sont des données qui ne peuvent en aucun cas permettre d'être associées avec une personne concernée identifiée ou identifiable. En particulier, les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

8.4. **Exactitude**

Les données traitées doivent être exactes et mises à jour et la personne concernée doit pouvoir les vérifier et les rectifier.

8.5. **Limitation de la conservation**

Les données à caractère personnel traitées ne doivent pas être conservées pour une durée indéterminée. Elles doivent être supprimées une fois l'objectif atteint et chaque Entreprise doit donc déterminer des durées de conservation compatibles avec l'objectif et conformes à la réglementation locale.

8.6. **Intégrité et confidentialité**

Chaque Entreprise doit traiter les données à caractère personnel de manière à assurer sécurité et confidentialité adéquates, notamment en empêchant l'accès non autorisé aux données à caractère personnel ou leur utilisation, ainsi qu'aux équipements utilisés pour le traitement.

8.7. **Responsabilité**

Chaque entreprise doit veiller au respect des principes ci-dessus et doit être en mesure de le démontrer.

9. RÈGLES DE FONCTIONNEMENT

En application des principes décrits ci-dessus et des autres normes envisagées par le RGPD, chaque société doit opérer dans le respect des règles opérationnelles suivantes.

9.1. **Registres des activités de traitement.**

Chaque Entreprise, par l'intermédiaire de ses Référents, doit conserver les preuves du traitement, tant informatisé que manuel, effectué en interne par les différents services de l'entreprise. Chaque Entreprise doit remplir cette obligation en compilant les registres des activités de traitement visés à l'article 30 du RGPD, en respectant les indications fournies à cet égard dans chaque pays par les autorités de contrôle locales.

La responsabilité de s'assurer que chaque Entreprise dispose des enregistrements prescrits par le RGPD et qu'ils sont constamment mis à jour incombe au Référent général qui, à cette fin, doit définir une procédure de gestion spécifique, en identifiant les responsabilités et les tâches au sein de l'Entreprise et, si elle est présente, en impliquant les Référents fonctionnels.

Dans tous les cas, la mise à jour des registres doit être effectuée au moins une fois par an.

9.2. **Communication et collecte de données (transparence et loyauté).**

En règle générale, les données à caractère personnel sont fournies directement par les personnes concernées dans le cadre des contacts professionnels normaux et dans l'exécution des activités opérationnelles de l'Entreprise, ou par le biais du site web, mais elles peuvent également être acquises auprès de tiers. Les employés qui collectent des données à caractère personnel auprès d'une personne concernée doivent s'assurer, lors de la collecte des données, que la personne concernée est correctement informée des finalités pour lesquelles les données sont collectées et traitées ultérieurement.

À cette fin, ils doivent fournir le document "communication" approprié préparé par la société.

La communication est toujours requise, même lorsqu'il n'est pas nécessaire de demander à la personne concernée son consentement au traitement de ses données.

Les opérations pour lesquelles aucune communication n'a été émise, ou qui ne sont pas décrites dans la communication elle-même, sont illégales et ne peuvent donc pas être réalisées.

La communication fournie est "ponctuelle" et doit précéder la première collecte de données d'une personne concernée.

Une nouvelle communication est effectuée en cas de modification de l'un des éléments indiqués dans la communication précédente.

9.3. **Conditions de licéité du traitement**

Pour chaque finalité énumérée dans la communication, il faut identifier au moins une base juridique qui rend son traitement licite.

Les bases juridiques sont celles indiquées à l'article 6 du RGPD pour les données personnelles "communes", qui consistent, en résumé, dans les alternatives suivantes :

- Consentement
- Exécution du contrat
- Exécution d'une obligation légale
- Sauvegarde des intérêts vitaux
- Tâche d'intérêt public
- Intérêt légitime (qui ne prévaut pas sur les droits de la personne concernée)

En ce qui concerne le traitement de catégories spéciales de données, les bases juridiques sont énoncées à l'article 9 du RGPD, et à l'article 10 pour les données judiciaires, et sont plus restrictives que celles des données ordinaires.

9.4. **Consentement de la Personne Concernée (licéité).**

Parmi les bases juridiques de la licéité, le consentement de la personne concernée est mentionné. Le consentement ne doit pas être recueilli si le traitement est fondé sur l'une des autres conditions de licéité (comme indiqué au point précédent). Toutefois, certains traitements requièrent nécessairement un consentement comme condition de licéité. Les opérations de traitement doivent être conformes à ce consentement donné par la personne concernée en réponse à la communication. Le consentement doit être donné librement par la personne concernée, ne doit être recueilli qu'après une communication adéquate ait été fournie et doit être démontrable et sans équivoque.

Lorsque le consentement est nécessaire pour effectuer le traitement, celui-ci ne peut pas être effectué s'il n'a pas été obtenu.

9.5. **Accessibilité des données et activités autorisées pour le personnel.**

L'accès aux données à caractère personnel et l'exécution des activités de traitement ne sont autorisés qu'aux personnes dûment autorisées et ayant reçu des instructions en bonne et due forme. Ces personnes chargées du traitement pourront accéder aux données aux données qu'ils ont besoin de connaître sur la base d'un critère de 'need to know'. Les données ne doivent être utilisées qu'aux fins de l'exécution de la tâche et des fonctions qui leur sont à chaque fois confiées.

Comme indiqué ci-dessus, nous insistons sur le fait que :

- les opérations pour lesquelles aucune communication n'a été émise, ou qui ne sont pas explicitement mentionnées dans ladite communication, ne peuvent être effectuées ;
- il est interdit d'effectuer les traitements pour lesquels le consentement n'a pas été obtenu lorsque nécessaire.

9.6. **Accessibilité aux catégories particulières de données et aux données juridique et activités autorisées au personnel.**

Ces données ne doivent être traitées que par les personnes chargées du traitement qui en ont strictement besoin, qui sont indispensables à l'exercice de leurs fonctions et qui sont spécifiquement autorisés.

Outre les contraintes, décrites ci-dessus, concernant la nécessité de communication et le consentement éventuel, il convient de noter que les opérations de traitement de ces données doivent également respecter les conditions et limites fixées par les réglementations locales.

Par exemple, en Italie, les conditions et les limites sont définies dans les Autorisations Générales délivrées par le Garante della Privacy, qui peuvent être consultées sur le site web du Garant (www.garanteprivacy.it).

Il n'est donc pas autorisé à effectuer des traitements qui ne sont pas conformes aux réglementations locales.

9.7. **Mesures de sécurité.**

Toutes les personnes chargées du traitement sont tenues de respecter rigoureusement les règles de sécurité élaborées par l'Entreprise, dont le non-respect peut entraîner des conséquences juridiques importantes, parfois même de nature pénale. Le respect de certaines mesures de sécurité dépend uniquement du comportement des personnes chargées du traitement.

9.8. **Circulation des données et communication des données à des tiers.**

Les données à caractère personnel peuvent circuler légalement au sein des sociétés du Groupe UE parmi les personnes qui ont besoin de les connaître à des fins professionnelles (*need to know*) et qui ont reçu des instructions à cet effet. Elles ne doivent pas être transmises - ou en tout cas rendues accessibles - à des tiers extérieurs au Groupe UE, sauf dans l'un des cas suivants :

- la transmission au tiers est nécessaire pour se conformer à une obligation légale ou à un ordre d'une autorité publique ;
- la transmission au tiers est nécessaire à l'exécution des obligations découlant d'un contrat signé avec la personne concernée auquel les données à caractère personnel sont attribuables ;
- si le tiers a été désigné comme sous-traitant des données, conformément à l'article 28 du RGPD, et que les données sont nécessaires à l'exécution du service externalisé ;
- la personne à laquelle les données peuvent être rattachées a explicitement donné son consentement à la transmission des données en question à ce tiers.

Toute nécessité de transmettre des données à un tiers pour des raisons autres que celles énumérées ci-dessus doit faire l'objet d'une autorisation écrite de la personne du Référent Général en charge dans l'entreprise.

En tout état de cause, le Groupe UE n'a pas pour politique de procéder, pour quelque raison ou à quelque fin que ce soit, au transfert de listes, de répertoires ou d'adresses sous forme de commercialisation de données à caractère personnel.

9.9. **Nouveaux traitements et traitements à haut risque.**

Sans autorisation préalable, aucun nouveau traitement présentant un risque élevé ne peut être mis en œuvre, tel que défini et réglementé dans la politique de l'entreprise concernant l'évaluation de l'impact du traitement prévu sur la protection des données à caractère personnel (analyse d'impact ou **AIPD**). Les principaux éléments à évaluer, qui peuvent comporter des risques élevés pour les personnes concernées, sont les suivants :

- Évaluation, notation ou profilage
- Processus décisionnel automatisé ayant des effets juridiques ou affectant de manière significative les personnes physiques de façon similaire
- Surveillance systématique
- Traitement de catégories particulières de données
- Traitement de données à grande échelle
- Créer des correspondances ou combiner des ensembles de données
- Traitement des données relatives aux personnes vulnérables
- Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles

- Traitement qui, en soi, "empêche la personne concernée d'exercer un droit ou de bénéficier d'un service ou d'un contrat".

En plus de ces éléments, les réglementations locales peuvent prévoir des cas à risques supplémentaires ou des cas où l'AIPD est obligatoire. En Italie, le Garant de la vie privée a imposé que l'AIPD soit obligatoire dans un certain nombre de cas dont, par exemple, le traitement non occasionnel des données relatives aux personnes vulnérables, le traitement systématique des données biométriques, etc.

9.10. **Violation de données (Data Breach)**

Une violation des données personnelles est définie comme « violation de la sécurité entraînant la destruction accidentelle ou illégale, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé aux données personnelles transmises, stockées ou traitées » (ci-après également dénommé "**Data Breach**").

En cas de Data Breach, il est obligatoire d'informer l'Autorité de contrôle (le garant local) dans les 72 heures suivant la prise de connaissance de la violation.

Le Groupe UE a adopté une politique de gestion des Data Breach qui doit être connue et comprise par tous les sujets chargés du traitement qui, lors de la manifestation de la situation décrite, doivent immédiatement la signaler à leur propre Référent fonctionnel ou, en cas d'absence, au Référent général afin de respecter les délais de notification.

9.11. **Privacy by design et Privacy By Default**

Le Groupe UE a adopté une politique de "privacy by design" et "privacy by default" qui doit être suivie lors du développement de nouvelles applications et de nouvelles opérations de traitement, et qui doit être portée à la connaissance de tous ceux qui participent à la conception et au développement de ces applications et opérations de traitement.

9.12. **Gestion des droits des personnes concernées**

Le RGPD accorde les droits suivants aux personnes concernées :

- Droit d'accès aux propres données personnelles (art. 15) ;
- Droit de rectification (art. 16) ;
- Droit à l'effacement (droit à l'oubli) (art. 17) ;
- Droit à la limitation du traitement (art. 18) ;
- Droit à la portabilité des données (art. 20) ;
- Droit d'opposition (article 21) ;
- Droit d'opposition à une décision fondée uniquement sur un traitement automatisé (article 22) ;
- Droit de révoquer, à tout moment, le consentement donné, sans compromettre la licéité du traitement fondé sur le consentement donné avant le retrait (article 7.3) ;

Le Groupe UE a adopté une politique de gestion des demandes d'exercice des droits susmentionnés, qui illustre son contenu. Cette politique doit être connue de toutes les personnes impliquées dans le processus de gestion de ces demandes. Il faut rappeler qu'en l'absence d'un

traitement approprié des demandes visées dans la politique, la personne concernée a le droit de déposer une plainte auprès du Garant ou d'engager une action en justice pour protéger ses droits.

10. FORMATION

Le RGPD exige que les personnes chargées du traitement des données soient sensibilisées aux risques liés au traitement des données personnelles. Chaque Entreprise doit donc veiller à ce que les personnes chargées du traitement des données soient sensibilisées à leurs responsabilités en leur dispensant une formation adéquate et adaptée à la tâche qui leur est confiée.
La formation ne peut être un événement ponctuel, mais doit être répétée de façon périodique, notamment en cas de changements de réglementation ou de nouvelles interprétations.
Il est également possible de mettre à disposition à des fins de formation des documents et des présentations expliquant les principaux aspects de la législation, des programmes de formation en ligne, des conférences en classe et des sessions de communication, etc.

Cette activité de formation doit être obligatoirement documentée (conformément au principe de Accountability - responsabilité). Chaque employé est tenu d'approfondir ses connaissances en la matière afin d'opérer dans le plein respect de la réglementation, de la présente politique et des instructions émises en matière de traitement des données. Tout besoin de formation complémentaire doit être signalé aux Référents fonctionnels (ou, en leur absence, au Référent général), qui assurent le suivi des demandes.

11. CONTRÔLES RÉGULIERS

Chaque société, en exécution de ses obligations au titre du RGPD, doit organiser des audits périodiques, notamment par l'intermédiaire des Référents désignées en son sein (Référent général et éventuels Référents fonctionnels), concernant le respect des dispositions du RGPD, des réglementations locales et des politiques du Groupe UE, ainsi que des instructions émises concernant le traitement des données.
Les contrôles peuvent être documentés. Les personnes chargées du traitement sont invitées à apporter leur plus grande coopération pour faciliter les vérifications.

12. SANCTIONS

La violation partielle ou totale des dispositions de la réglementation relative à la protection de la vie privée peut entraîner des sanctions pénales, civiles et administratives pour traitement illicite ou non conforme à la réglementation en question.
Dans les cas les plus graves, il est rappelé que l'amende administrative applicable en vertu de l'article 83, paragraphe 5, du RGPD peut aller jusqu'à 20 000 000 euros, ou pour les entreprises, jusqu'à 4 % du chiffre d'affaires mondial annuel total de l'année précédente, le montant le plus élevé étant retenu.

Tout comportement illégal ou non conforme à la présente politique, aux politiques du Groupe UE et aux instructions émises concernant le traitement des données à caractère personnel peut entraîner des mesures disciplinaires proportionnelles à la gravité des faits.

*** *** ***