Politique générale de protection des données à caractère personnel

Version 1.0

Groupe BSL

Politique générale de protection des Données à caractère personnel.

Date d'application	1er janvier 2023
Auteur	Patrick de La Guéronnière – SECCOM Consulting
Direction émettrice	DPO externe
Valideur	Richard TRANCHE

Signataire	
Nom et Prénom	ALLOUCH Marc
Fonction	Directeur juridique du Groupe BSL

Diffusion		
☐ Confidentiel	☒ Interne	☐ Public

Destinataires	
Pour action	FSP, BSL Paris, BSL Lyon, BSL Marseille, BSL Tunis
Pour information	Conseil d'Administration

Suivi des mises à jour				
Date	Référence	Auteur	Objet	État
2/01/2023	V.X	XXX	XXX	Validé/Diffusé

Documents de références

1. Objectifs et champ d'application de la Politique

Les termes commençant par une majuscule et utilisés dans la présente Politique générale de protection des Données à caractère personnel (ci-après la « Politique ») sont définis dans l'Annexe « Définitions ».

1.1 Objectifs de la Politique

En tant que Responsable de Traitement, les entités du Groupe BSL s'engage à **garantir la protection des Données à caractère personnel** 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 et Données à caractère personnel sensibles.

Cette Politique a pour objectifs de :

- définir les engagements du Groupe BSL au sujet des principes imposés par la Législation applicable, et notamment le Règlement (UE) 2016/679 relatif à la protection des Données à caractère personnel, en date du 27 avril 2016, applicable depuis le 25 mai 2018 ;
- définir les rôles et responsabilités des principaux contributeurs ; et
- assurer la mise en place de méthodes et procédures adéquates ainsi que des structures de gouvernance et de contrôle appropriées pour garantir le respect des engagements et de la Législation applicable.

Les engagements du Groupe BSL sont résumés dans les encarts de règle REG. La conformité du Groupe BSL avec ces règles sera auditée dans les conditions définies à la Section « Contrôle de la conformité ».

Cette Politique est complétée par les politiques et procédures suivantes :

- Procédure de gestion des droits des Personnes concernées
- Procédure de gestion des Violations de Données à caractère personnel
- Procédure de gestion d'un contrôle CNIL
- Politique de confidentialité du site web
- Politique des cookies

1.2 Champ d'application de la Politique

La Politique a vocation à s'appliquer à l'ensemble des entités du Groupe BSL

En cas de conflits entre la présente Politique et la Législation applicable, les règles suivantes s'appliqueront :

- Si la Politique est plus protectrice, elle a vocation à primer sur la Législation applicable.
- Si la Législation applicable est plus protectrice, elle s'appliquera sur les points concernés en lieu et place de la Politique.

Si un doute subsiste, le collaborateur de l'entité concernée sollicitera les conseils du DPO.

1.3 Révision de la Politique

La Politique est mise à jour par le DPO du Groupe BSL en cas de :

- Changements significatifs du contexte métier ou de la stratégie de protection des Données à caractère personnel de du Groupe BSL ;
- Changements significatifs de l'exposition aux risques (par exemple, nouvelles menaces, nouvelles tendances…) ;
- Évolution significative de la Législation applicable.

Ces modifications sont soumises à la validation de la Direction Générale. Une communication adéquate sera effectuée aux collaborateurs du Groupe BSL en cas de modifications.

2. Organisation et gouvernance de la protection des Données à caractère personnel

Chaque personne au sein du Groupe BSL est responsable de la protection des Données à caractère personnel. Cette protection doit être une préoccupation constante, reflétée dans les politiques, procédures et pratiques opérationnelles.

Les contributeurs clés identifiés dans cette section adoptent les rôles et responsabilités qui leur incombent afin de s'assurer que cette Politique soit mise en œuvre de manière cohérente et coordonnée au sein du Groupe BSL.

2.1 Contributeurs clés

2.1.1 La Direction générale

La Direction générale garantit un engagement fort du Groupe BSL en faveur de la protection des Données à caractère personnel en tant qu'actif stratégique de l'entreprise. À ce titre, la Direction générale doit :

- S'assurer de la mise en place d'une gouvernance de la protection des Données à caractère personnel appropriée, définissant les rôles et responsabilités au sein du Groupe BSL et permettant au DPO d'être associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des Données ;
- Communiquer auprès de l'ensemble des collaborateurs sur la nomination d'un DPO, ses missions et les moyens de le contacter ;

- Veiller à ce que le DPO :
    - Dispose des ressources et moyens nécessaires à l'exercice de ses missions ;
    - Ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions ;
    - Reçoive la formation adaptée ;
    - Soit en mesure de faire directement rapport à la Direction générale.

2.1.2 Les Directions métiers

Chaque responsable d'une Direction métier en charge de la mise en œuvre d'un ou plusieurs Traitements doit :

- Veiller au respect des principes et règles édictés dans la présente Politique et les procédures et politiques complémentaires ;
- Associer le DPO dès la phase de conception dans tous les nouveaux projets impliquant un Traitement de Données à caractère personnel ;
- Réaliser si nécessaire une Analyse d'impact relative à la protection des Données, avec l'assistance du DPO et de tout autre expert technique ;
- Documenter et justifier par écrit les raisons pour lesquelles l'avis du DPO n'a pas été suivi le cas échéant ;
- Répondre à toute demande d'information du DPO sur tous les sujets ayant un impact sur la vie privée des personnes ;
- Fournir toute documentation relative aux Traitements dans leur périmètre d'intervention ;
- Inscrire tout nouveau Traitement dans le registre des Traitements du Groupe BSL.

2.1.3 Le Délégué à la protection des Données (« DPO »)

Le Groupe BSL a désigné un Délégué à la protection des Données (DPO) pour garantir la conformité du Groupe BSL à la Législation applicable et le respect des engagements pris aux termes de la présente Politique.

Le DPO a plusieurs missions au sein du Groupe BSL :

- Informer et sensibiliser les collaborateurs aux règles à respecter en matière de protection des Données à caractère personnel ;
- Veiller au respect de la Législation applicable ainsi que des engagements pris aux termes de la présente Politique ;
- Conseiller les Directions métiers sur l'application concrète des principes aux projets de Traitement ;
- Informer et responsabiliser, voire alerter si besoin, la Direction générale du Groupe des risques que les initiatives des opérationnels ou le non-respect de ses recommandations feraient courir à l'organisme ;
- Établir si une Analyse d'impact relative à la protection des Données doit être réalisée et conseiller la Direction métier dans la réalisation de l'AIPD ;
- Assister en cas de Violation de Données à caractère personnel pour évaluer le risque de la Violation et agir en point de contact en cas de notification à l'Autorité de contrôle compétente et/ou les Personnes concernées ;

- Analyser, investiguer, auditer et contrôler le degré de conformité du Groupe BSL et accompagner les Directions métiers dans la définition et la mise en œuvre d'un plan de remédiation le cas échéant ;
- Établir et maintenir une documentation au titre de l'« *accountability* » ;
- Garantir la gestion adéquate des droits des Personnes concernées telle que définie dans la procédure afférente ;
- Présenter un rapport annuel à la Direction générale ;
- Interagir avec l'Autorité de contrôle.

Le DPO a la possibilité de nommer un ou plusieurs suppléants au sein des collaborateurs du Groupe BSL. Une communication adéquate est effectuée par le DPO sur cette nomination.

2.1.4 La Direction juridique

La Direction juridique apporte son soutien et son expertise sur les sujets suivants :

- Compréhension et mise en œuvre des exigences de la Législation applicable ;
- Conseils sur les impacts juridiques potentiels ;
- Assistance sur les aspects juridiques de l'AIPD ;
- Rédaction de la documentation juridique appropriée (par exemple, notice d'information, BCR, etc.)
- Rédaction et négociation de contrats avec des parties externes (Contrats, NDA, LOI, accords commerciaux, accords de Transfert de Données, etc.)

2.1.5 La Direction des systèmes d'information/le RSSI

Pour chaque projet, la DSI/le RSSI apporte son soutien et son expertise sur les sujets suivants :

- Évaluation du contexte et de la criticité du projet ;
- Analyse des risques, notamment dans le cadre de l'évaluation préalable à l'Analyse d'impact relative à la protection des Données ;
- Conseil sur les mesures de sécurité pour réduire, éviter ou transférer les risques :
- Évaluation du niveau de sécurité des Tiers intervenants et négociation avec ces derniers pour intégrer les exigences du Groupe BSL en la matière dans le contrat ;
- Coordination de la surveillance, détection et gestion des incidents de sécurité, avec les conseils du DPO en cas de Violation de Données.

2.2 Rapport annuel du DPO

Le DPO établit et publie un rapport annuel sur les activités liées à la protection de la vie privée au sein du Groupe BSL. À cette fin, le DPO définit, recueille et publie des indicateurs qui mettent en évidence le niveau de conformité aux politiques et procédures internes en la matière ainsi qu'à la Législation applicable.

3. Les principes à respecter en matière de Traitement des Données à caractère personnel

Conformément à la Législation applicable, le Groupe BSL s'engage à respecter les principes établis ci-après lors de la collecte et du Traitement de Données à caractère personnel.

3.1 Licéité, loyauté et transparence

Les Données à caractère personnel doivent être collectées et traitées de manière **licite, loyale et transparente.**

A ce titre, le Groupe BSL garantit que tout Traitement repose une **base légale reconnue** par la Législation applicable telles que :

- La Personne concernée a donné son Consentement au Traitement de ses Données à caractère personnel pour une ou plusieurs finalités spécifiques (sous réserve du respect des exigences supplémentaires détaillées à la section « Consentement ») ;
- Le Traitement est nécessaire à l'exécution d'un contrat auquel la Personne concernée est partie ou pour prendre les mesures appropriées à la demande de la Personne concernée avant de conclure un contrat ;
- Le Traitement est nécessaire au respect des obligations légales auxquelles le Groupe BSL est soumis ;
- Le Traitement est nécessaire aux fins d'intérêts légitimes poursuivis par le Groupe BSL ;
- Le Traitement est nécessaire afin de protéger les intérêts vitaux de la Personne concernée ;
- Le Traitement est nécessaire pour l'exécution d'une mission d'intérêt public.

Lorsqu'un Traitement est basé sur l'intérêt légitime, le Groupe BSL procède à une analyse pour déterminer si cet intérêt légitime prime ou non sur les intérêts ou les droits et libertés fondamentaux des Personnes concernées. Cette évaluation et ses résultats doivent être documentés et consignés à des fins probatoires (*accountability*).

Exceptionnellement, le Groupe BSL peut traiter des Données à caractère personnel sensibles, auquel cas le Groupe BSL veille à respecter les exigences de la Section « Traitement des Données à caractère personnel sensibles » de la présente Politique.

REG1 Tout Traitement repose sur une base légale clairement identifiée et documentée dans le registre.

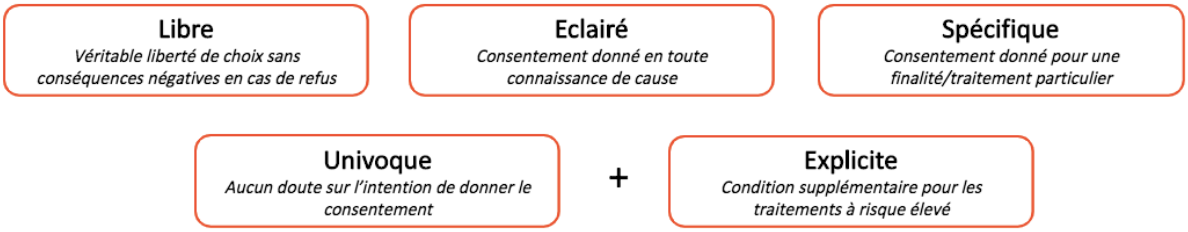
De plus, le Groupe BSL s'assure que les activités de Traitement des Données à caractère personnel sont effectuées de manière **apparente et transparente**. À cette fin, le Groupe BSL fournit des informations accessibles et intelligibles aux Personnes concernées sur la façon dont leurs Données à caractère personnel sont utilisées, conformément aux termes et exigences de la procédure de gestion des droits des Personnes concernées (cf. Section « Relations avec les Personnes concernées » de cette Politique).

3.2 Consentement

Lorsque le Traitement est fondé sur le Consentement de la Personne concernée, le Groupe BSL s'assure que ce Consentement a été obtenu légalement (voir Section sur les « Conditions de validité du Consentement ») et est correctement géré pendant toute la durée du Traitement (voir Section « Gestion du Consentement »).

3.2.1 Les conditions de validité du Consentement (caractéristiques et modalités de collecte)

Le Groupe BSL s'assure que le Consentement obtenu de la part de la Personne concernée répond aux critères suivants :



En outre, le Groupe BSL doit le cas échéant s'assurer du respect des lois locales sur les conditions de validité du Consentement.

Ce Consentement doit être obtenu avant la collecte des Données et, *a minima*, concomitamment à la collecte des Données. La demande de Consentement doit être distinguée de tout autre demande/sujet, sous une forme intelligible et facilement accessible, dans un langage clair et simple.

REG2 Lorsque la base légale est le Consentement, le Consentement obtenu répond aux conditions de validité de fond (caractéristiques) et de forme (collecte).

3.2.2 La gestion du Consentement (durée, preuve)

Le Groupe BSL veille à la **durée de validité du Consentement** : lorsque les modalités de Traitement changent ou évoluent, le Consentement original n'est plus valide. Un nouveau Consentement doit alors être obtenu.

Le Groupe BSL assure le **suivi**, dans la mesure du possible, **des déclarations de Consentement reçues**, c'est-à-dire quelle Personne concernée a donné son Consentement, comment et quand le Consentement a été obtenu, ainsi qu'une copie des informations fournies à la Personne concernée à l'époque.

REG3 Les Consentements sont renouvelés en cas de modification significative des modalités de Traitement.

REG4 Un suivi des déclarations de Consentement est mis en place.

3.2.3 Le retrait du Consentement

La Personne concernée doit être en mesure de **retirer son Consentement à tout moment**. Le Groupe BSL doit donner à la Personne concernée les moyens de retirer son Consentement aussi facilement qu'il a été donné, dans la mesure du possible par une méthode équivalente à celle utilisée pour obtenir le Consentement.

Une fois le Consentement révoqué, Le Groupe BSl doit s'assurer que le **retrait est enregistré dans ses systèmes** et bases de Données dès que possible, de telle sorte que les Données à caractère personnel ne soient plus traitées pour la finalité en question (par exemple, un client qui révoque son Consentement pour recevoir une publicité ne devrait plus en recevoir). En outre, ce changement de statut doit être **relayé chez tous les Tiers intervenants**, en particulier les Sous-traitants, de sorte qu'aucun d'entre eux ne traite plus les Données à caractère personnel concernées pour la finalité en question.

Une fois le Consentement révoqué, le Groupe BSL ne peut plus se fonder sur le Consentement comme base légale pour le Traitement. Toutefois, le retrait du Consentement :

- n'affecte pas la licéité du Traitement fondé sur le Consentement avant son retrait, et ;
- n'exige pas nécessairement la suppression des Données à caractère personnel concernées dans la mesure où elles peuvent encore être utiles pour un autre Traitement et/ou présenter un intérêt administratif.

REG5 La Personne concernée a la possibilité de retirer son Consentement à tout moment aussi facilement qu'il a été donné.

REG6 Le retrait du Consentement est pris en compte de façon effective dans les outils de Traitement.

3.3 Limitation des finalités

Avant toute collecte de Données à caractère personnel, le Groupe BSL définit de façon claire la ou les finalités poursuivies par la collecte, lesquelles doivent être **déterminées, explicites et légitimes**. Le Groupe BSL s'assure également que la ou les finalités ainsi définies sont compatibles avec ses activités.

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. À ce titre, le Groupe BSL effectue un **test de compatibilité** pour vérifier si la finalité ultérieure est compatible avec la finalité initiale. Ce test prend en compte :

- L'existence d'un lien entre les deux finalités ;

- Le contexte dans lequel les Données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les Personnes concernées et les entités du Groupe BSL ;
- La nature des Données à caractère personnel, en particulier si des Données à caractère personnel sensibles sont traitées ;
- Les conséquences possibles du Traitement ultérieur envisagé pour les Personnes concernées ;
- L'existence de garanties appropriées.

Lorsque la finalité ultérieure est incompatible avec la finalité initiale, le Groupe BSL s'assure de recueillir le Consentement de la Personne concernée, conformément aux exigences de la Législation applicable (Article 6 (4) du RGPD).

REG7 Les Données à caractère personnel ne sont collectées qu'à des fins spécifiques, explicites et légitimes, et ne doivent pas être traitées ultérieurement d'une manière incompatible avec cette ou ces finalités.

3.4 Minimisation et exactitude

Les Données à caractère personnel collectées doivent être **adéquates, pertinentes et non excessives** par rapport à la finalité poursuivie par le Traitement. En d'autres termes, les entités du Groupe BSL s'assurent que la collecte porte uniquement sur les Données **strictement nécessaires** pour atteindre la finalité.

En outre, le Groupe BSL s'assure que les Données à caractère personnel sont **exactes et, le cas échéant, mises à jour**. A cette fin et compte tenu de la finalité pour laquelle elles sont traitées et de la nécessité qui en résulte de disposer de Données exactes, le Groupe BSL prend des **mesures raisonnables** pour effacer ou rectifier sans délai toute Donnée à caractère personnel inexacte.

REG8 Les Données à caractère personnel sont adéquates, pertinentes et non excessives au regard de la finalité poursuivie par le Traitement. Elles sont exactes, complètes et mises à jour si nécessaire.

3.5 Conservation limitée

Le Groupe BSL s'assure que les Données à caractère personnel traitées ne sont **pas conservées plus longtemps que nécessaire** au regard des finalités pour lesquelles elles sont collectées.

Les Données à caractère personnel peuvent être conservées :

1) Sous une forme permettant l'identification des Personnes concernées pendant une **durée n'excédant pas celle nécessaire au regard des finalités** pour lesquelles elles sont traitées par

les entités du Groupe BSL. Une fois la finalité atteinte, les Données doivent donc **être supprimées**.

2) Au-delà de la durée nécessaire à la finalité du Traitement, lorsqu'elles présentent encore un **intérêt administratif**. La durée de conservation des Données peut alors être prolongée au-delà du délai jugé pertinent pour la finalité de collecte initiale. Ce prolongement doit être dûment **justifié et documenté**.

   Les Données peuvent encore être conservées en vue de respecter des **durées légales de prescription**, des **durées de conservation particulières** (conservation des documents comptables et pièces justificatives, archivage des contrats électroniques, etc.), essentiellement à **des fins probatoires**, ou encore afin d'être en capacité de **répondre aux demandes de communication** susceptibles d'être adressées par certains Tiers légalement habilités (l'administration fiscale, les organismes sociaux, etc.).

3) Pour des **durées plus longues** dans la mesure où les Données à caractère personnel seront traitées exclusivement par le Groupe BSL à des **fins d'archivage** dans l'intérêt public, à des **fins de recherche scientifique** ou **historique,** pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées afin de garantir les droits et libertés de la Personne concernée, telles que **l'anonymisation** ou la **pseudonymisation**.

Afin d'assurer le respect de ce principe, le Groupe BSL définit les durées de conservations applicables à chaque Traitement. Les éléments suivants doivent être pris en compte pour la détermination de la durée de conservation de chaque catégorie de Données collectées :

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

Ces durées sont **revues et mises à jour autant que de besoin** pour refléter les évolutions de la Législation applicable et/ou des pratiques au sein du Groupe BSL.

Au terme de cette durée, les Données sont **supprimées sans délai indu**. Cette suppression peut être opérée par destruction des Données ou anonymisation. En cas de suppression par destruction, le Groupe BSL s'assure que les Données sont effectivement détruites des systèmes, y compris les systèmes des Tiers le cas échéant.

Les exigences et modalités de mise en œuvre du principe de conservation limitée des Données à caractère personnel sont détaillées dans la « Politique de conservation/suppression des Données à caractère personnel » du Groupe BSL.

REG9 Des durées de conservation sont définies et implémentées.

3.6 Sécurité des Données à caractère personnel

Le Groupe BSL prend des **mesures techniques et organisationnelles** dans le but d'assurer **la sécurité, la confidentialité et l'intégrité** des Données à caractère personnel pendant toute la durée du Traitement. Sont pris en compte dans la détermination de ces mesures :

- la gravité et la probabilité du préjudice éventuel pouvant résulter de la perte, de l'altération et/ou de l'accès non autorisé aux Données ;
- les éléments caractéristiques du Traitement concerné ;
- le cas échéant, les résultats de l'Analyse d'impact relative à la protection des Données menée ;
- l'état de l'art ;
- les coûts d'implémentation.

Le Groupe BSL a établi une politique de sécurité du système d'information (PSSI) détaillant l'ensemble des mesures de sécurité techniques et organisationnelles mises en œuvre. Cette PSSI est régulièrement revue et mise à jour.

Le groupe BSL s'engage à réviser de façon régulière les mesures de sécurité afin de **tester, évaluer et mesurer leur efficacité et entreprendre toute amélioration nécessaire**.

Le Groupe BSL s'assure également que toute Violation des Données est gérée correctement conformément à la Section « Gestion des Violations de Données » de la présente Politique.

REG10 Des mesures techniques et organisationnelles appropriées sont mises en œuvre afin d'assurer la sécurité, l'intégrité et la confidentialité des Données à caractère personnel.

3.7 Transfert des Données à caractère personnel en dehors de l'Union européenne

Les Transferts de Données à caractère personnel exigent une attention et des garanties supplémentaires. Le Groupe BSL s'assure que tout Transfert de Données à caractère personnel est **sécurisé de façon adéquate** et **encadré juridiquement** conformément aux exigences de la Législation applicable.

A ce titre, le Groupe BSl veille à :

- **Identifier tout Transfert de Données** à caractère personnel, y compris, dans la mesure du possible, les Transferts ultérieurs opérés par les Sous-traitants (de 1er rang) ;
- **Encadrer dans le contrat** avec le prestataire les Transferts de Données ainsi que, le cas échéant, le lieu d'hébergement des Données (lequel doit être par principe sur le territoire de l'Union européenne). Le prestataire doit ainsi garantir l'application de mesures permettant d'assurer un niveau de protection des Données à caractère personnel équivalent à celui fourni par le RGPD ;
- **Sécuriser tout Transfert** par des mesures techniques et organisationnelles adaptées ;

- Lorsque le Transfert n'est pas à destination d'un pays reconnu comme d'adéquat (en vertu d'une décision d'adéquation de la Commission européenne), encadrer juridiquement le Transfert par un **mécanisme approprié** (clauses contractuelles types, *binding corporate rules*, etc.).

Dans la mesure du possible, les Données à caractère personnel ne doivent pas être transférées dans un pays situé hors de l'Union Européenne de manière automatique sans l'autorisation du DPO de du Groupe BSL.

REG11 Tout Transfert de Données à caractère personnel est sécurisé de façon adéquate et encadré juridiquement conformément aux exigences de la Législation applicable.

3.8 Traitement de Données à caractère personnel sensibles

En plus de la base légale générique (voir section « Licéité, loyauté et transparence »), les Données à caractère personnel sensibles ne peuvent être collectées QUE SI l'une des **conditions spéciales** suivantes s'applique :

- La Personne concernée a donné son Consentement explicite ;
- Le Traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propre au Groupe BSL ou à la Personne concernée en matière de droit du travail, sécurité sociale et protection sociale ;
- Le Traitement est nécessaire à la sauvegarde des intérêts vitaux de la Personne concernée ;
- Le Traitement porte sur des Données à caractère personnel qui sont manifestement rendues publiques par la Personne concernée ;
- Le Traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- Le Traitement est nécessaire pour des motifs d'intérêt public importants, sur la base du droit de l'Union européenne ou d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des Données à caractère personnel et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la Personne concernée ;
- Le Traitement est nécessaire aux fins de la médecine préventive, ou de médecine du travail, de l'appréciation de la capacité de travail du travailleur, des diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et services de soins de santé ;
- Une condition spécifique prévue par une loi locale s'applique.

Le Groupe BSL doit prévoir des **mesures de sécurité particulières** pour ces Données au regard du risque qu'elles peuvent représenter pour la Personne concernée.

Les Données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes ne doivent pas, par principe, être recueillies, sauf dans des cas très exceptionnels et avec la validation du DPO (par exemple, la collecte du casier judiciaire pour vérifier les

informations concernant un candidat à un emploi en raison de la nature spécifique de l'offre d'emploi).

En tout état de cause, ce type de Données à caractère personnel sensibles ne peut pas être traité (par exemple, la copie du casier judiciaire, si elle peut être collectée, ne peut être conservée).

REG12 Le Traitement de Données sensibles est par principe interdit. Toute exception doit être réalisée dans les conditions requises par la Législation applicable et validée par le DPO.

4. Documentation et gestions des risques

Toutes les preuves du respect de la règlementation doivent être conservées afin de pouvoir démontrer la conformité du Groupe BSL à l'Autorité de contrôle.

4.1 Protection des Données dès la conception et par défaut (« *Privacy by Design/by Default* »)

Pour tout nouveau projet impliquant le Traitement de Données à caractère personnel, le Groupe BSL met en place des mesures visant à protéger les Données à caractère personnel dès la conception du Traitement, mais aussi tout au long du projet et du cycle de vie de la Donnée à caractère personnel, c'est-à-dire de la collecte à la destruction.

A cette fin, tout collaborateur du Groupe BSL pilotant un projet devra suivre les étapes suivantes :

Etape 1. Vérifier que les principes définis en Section 3 de la présente Politique sont bien respectés.
Etape 2. Liste les mesures techniques et organisationnelles existantes et envisagées permettant d'assurer la sécurité, l'intégrité et la confidentialité des Données à caractère personnel.
Etape 3. Réaliser l'évaluation préalable à l'Analyse d'impact relative à la protection des Données.
Etape 4. Réaliser si nécessaire l'Analyse d'impact relative à la protection des Données.
Etape 5. Implémenter les mesures de sécurité adaptées au niveau de risque.

Le processus à suivre est détaillé dans le « Guide *Privacy by design* » du Groupe BSL.

Lorsque le projet implique de confier tout ou partie du Traitement à un Sous-traitant, le Groupe BSL s'assure que les exigences de la section « Gestion des Tiers intervenants » sont respectées.

REG13 Tout projet prend en compte la protection des Données à caractère personnel dès la conception et par défaut.

4.2 L'Analyse d'impact relative à la protection des Données (AIPD)

Lorsqu'un Traitement est susceptible d'engendrer un **risque élevé** pour les droits et libertés des Personnes concernées, le groupe BSl effectue une **Analyse d'impact relative à la protection des Données** (AIPD) sur le Traitement, **en amont de la mise en place du Traitement**.

Aussi, le groupe BSL s'assure qu'une **évaluation préalable** est réalisée pour tout nouveau Traitement afin de déterminer le niveau de risque du Traitement et, partant, si une AIPD doit être conduite. Cette évaluation préalable prend en compte :

- Les cas obligatoires définis dans le RGPD et l'Autorité de contrôle ;
- Les critères établis par le Comité européen de la protection des Données ;
- Les hypothèses d'exemption prévues par le RGPD et l'Autorité de contrôle.

L'AIPD doit être **documentée** et doit *à minima* :

- décrire la nature, la portée, le contexte et les finalités du Traitement ;
- évaluer la nécessité, la proportionnalité et les mesures de conformité ;
- déterminer et évaluer les risques pour les Personnes concernées ;
- déterminer toute mesure supplémentaire visant à atténuer ces risques.

Pour plus de renseignements : Fiche pratique de la CNIL sur l'AIPD

REG14 La nécessité d'effectuer une Analyse d'impact relative à la protection des Données est identifiée pour chaque nouveau projet et une AIPD est effectuée si nécessaire, avant le début du Traitement.

L'AIPD est un **processus continu** et devra être **revue régulièrement** pour assurer que le niveau de **risque reste acceptable** tout au long de la vie du Traitement, dans la mesure où l'environnement, technique notamment, sera amené à évoluer, ce qui nécessitera d'adapter les mesures mises en œuvre.

De même, si un Traitement ne nécessite pas une AIPD dans un premier temps mais que les opérations de Traitement évoluent, une AIPD pourra devoir être effectuée dans un second temps.

REG15 La nécessité de mettre à jour une AIPD existante ou d'effectuer une AIPD est prise en compte pour chaque changement majeur dans une opération de Traitement.

Après approbation de la Direction générale, le DPO **consulte l'Autorité de contrôle** si l'AIPD indique que le Traitement entraînerait un risque élevé pour les droits et libertés des Personnes concernées, c'est-à-dire si le **risque résiduel est encore élevé** une fois que le plan de remédiation des risques a été défini et implémenté.

REG16 Lorsque l'AIPD montre qu'un risque résiduel élevé persiste, la CNIL est consultée.

4.3 Le registre des Traitements

En qualité de Responsable de Traitement, le Groupe BSL tient à jour un **registre des Traitements** conforme aux exigences de la Législation applicable.

A cette fin, le Groupe BSL détermine les acteurs clés de la tenue et mise à jour du registre, leurs rôles et responsabilités.

REG17 Un registre des Traitements mis en œuvre est tenu à jour.

5. Formation et sensibilisation du personnel

Le Groupe BSL s'assure que l'intégralité de ses collaborateurs est **sensibilisée à la problématique de la protection des Données à caractère personnel** et comprend l'intention et la portée de la Législation applicable ainsi que les risques en cas de non-conformité.

Dans la mesure du possible, le Groupe BSL assure également une **formation spécifique** des collaborateurs qui ont vocation à traiter des Données à caractère personnel au quotidien.

Les collaborateurs sont régulièrement informés et/ou formés des évolutions législatives ou jurisprudentielles en matière de protection des Données à caractère personnel ainsi que des mises à jour des règles internes applicables.

Tout nouveau collaborateur suit une sensibilisation/formation appropriée eu égard à ses missions et à son niveau de connaissance.

REG18 L'ensemble des collaborateurs sont sensibilisés aux principes et enjeux de la protection des Données à caractère personnel. Une formation plus approfondie est dispensée aux collaborateurs traitant des Données à caractère personnel au quotidien.

6. Relations avec les Personnes concernées

Le Groupe BSL s'engage à garantir l'**exercice effectif** des droits des Personnes concernées qui leur sont accordés par la Législation applicable. La Législation applicable accorde aux Personnes concernées les droits suivants :

1. **Droit à l'information** : le droit d'avoir une information claire, précise et complète sur l'utilisation des Données à caractère personnel par les entités du Groupe BSL.
2. **Droit d'accès** : le droit d'obtenir une copie des Données à caractère personnel que le Responsable de Traitement détient sur le demandeur.
3. **Droit de rectification** : le droit de faire rectifier les Données à caractère personnel si elles sont inexactes ou obsolètes et/ou de les compléter si elles sont incomplètes.

4. **Droit à l'effacement / droit à l'oubli** : le droit, dans certaines conditions, de faire effacer ou supprimer les Données, à moins que le Groupe BSL ait un intérêt légitime à les conserver.
5. **Droit d'opposition** : le droit de s'opposer au Traitement des Données à caractère personnel par le Groupe BSL pour des raisons tenant à la situation particulière du demandeur (sous conditions).
6. **Droit de retirer son Consentement** : le droit à tout moment de retirer le Consentement lorsque le Traitement est fondé sur le Consentement.
7. **Droit à la limitation du Traitement** : le droit, dans certaines conditions, de demander que le Traitement des Données à caractère personnel soit momentanément suspendu.
8. **Droit à la portabilité des Données** : le droit de demander que les Données à caractère personnel soient transmises dans un format réexploitable permettant de les utiliser dans une autre base de Données.
9. **Droit de ne pas faire l'objet d'une décision automatisée** : le droit pour le demandeur de refuser la prise de décision entièrement autorisée et/ou d'exercer les garanties supplémentaires offertes en la matière.
10. **Droit de définir des directives post-mortem** : le droit pour le demandeur de définir des directives relatives au sort des Données à caractère personnel après sa mort.

Des droits additionnels peuvent être octroyés par la réglementation locale aux Personnes concernées.

A cette fin, le Groupe BSL définit et met en œuvre une **procédure de gestion des droits des Personnes concernées** conformes aux exigences de la Législation applicable. Cette procédure établit :

- Les standards à respecter pour assurer l'information transparente des personnes ;
- Les exigences légales qui doivent être respectées ;
- Les moyens autorisés pour présenter une demande pour chaque droit, selon la catégorie de Personnes concernées ;
- Les processus opérationnels pour traiter ces demandes conformément aux exigences susmentionnées ;
- Les parties impliquées dans ces processus, leurs rôles et responsabilités.

Les demandes soumises par les Personnes concernées en application de leurs droits sont **consignées dans un registre** à des fins de preuve de la conformité. La procédure de gestion des droits des Personnes concernées susmentionnée définit le contenu et les modalités de tenue de ce registre.

REG19 Une procédure relative à la gestion des droits des Personnes concernées est établie et appliquée, les demandes éligibles étant enregistrées dans un registre dédié.

7. Gestion des Violations de Données à caractère personnel

Conformément à son obligation de sécurité, le Groupe BSL définit, documente et met en œuvre un **processus pour détecter, qualifier et répondre aux Violations de Données à caractère personnel**. La procédure documentée doit comprendre :

- une matrice d'évaluation des risques pour les droits et libertés des Personnes concernées, en tenant compte des critères définis par l'Autorité de contrôle et le Comité européen de protection des Données ;
- une répartition des rôles et des responsabilités entre toutes les parties concernées par le plan de réponse, y compris celles des Sous-traitants du Groupe BSL ;
- les conditions, modalités et délais concernant la notification d'une Violation de Données à l'Autorité de contrôle compétente et/ou aux Personnes concernées.

Des moyens techniques et organisationnels adéquats sont mis en œuvre pour détecter, enquêter et signaler les Violations de Données à caractère personnel. De plus, afin de mieux détecter et gérer les Violations, les employés des entités du Groupe BSL sont sensibilisés et formés à la procédure à suivre en cas de Violation avérée ou suspectée.

REG20 Une procédure de gestion des Violations de Données à caractère personnel est définie et mise en œuvre.

De plus, le Groupe BSL établit un registre des Violations de Données à caractère personnel à des fins d'*accountability*, pour notifier l'ensemble des Violations, qu'une notification soit requise ou non.

REG21 Un registre des Violations est tenu à jour.

8. Gestion des Tiers intervenants

Conformément à la Législation applicable, le Groupe BSL s'engage à choisir des prestataires qui présentent des **garanties suffisantes** quant à la mise en œuvre de mesures techniques et organisationnelles appropriées.

A ce titre, le Groupe BSL vérifie **en amont les garanties** présentées par tout prestataire Tiers envisagé, au moyen notamment de questionnaires et/ou analyse de documentation. Cette vérification doit permettre d'**évaluer les conditions de mise en œuvre du Traitement chez le prestataire** : modalités de réalisation des opérations de Traitement confiées, sécurité et confidentialité des Données à caractère personnel, maturité du prestataire Tiers sur la question de la protection des Données à caractère personnel.

REG22 Un contrôle des garanties offertes par chaque prestataire Tiers est réalisé préalablement à la mise en œuvre des activités de Traitement.

Le Groupe BSL s'assure que le Tiers intervenant est **correctement qualifié** (Responsable de Traitement distinct, co-Responsable ou Sous-traitant) et s'assure qu'un **contrat écrit définit clairement les rôles et responsabilités** de chacune des parties. Ce contrat intègre au minimum les clauses requises par la Législation applicable (notamment le RGPD).

Lorsque le Tiers intervient en qualité de Sous-traitant, le contrat signé détaille le ou les Traitements confiés au Sous-traitant en déterminant :

- l'objet et la durée du Traitement ;
- la nature et la finalité du Traitement ;
- la ou les catégories de Données à caractère personnel ;
- la ou les catégories de Personnes concernées ;
- les instructions relatives aux opérations de Traitement.

REG23 Un contrat écrit est signé avec chaque Tiers impliqué dans le Traitement des Données. Cet accord comprend des clauses contractuelles adéquates, conformes à la Législation applicable.

Les Sous-traitants sont **audités régulièrement** pour vérifier leur conformité continue aux obligations contractuelles et réglementaires, selon une récurrence et des modalités définies en fonction de la nature et sensibilité des opérations de Traitement confiées, des coûts nécessaires et des ressources disponibles.

REG24 Les Sous-traitants sont audités régulièrement pour vérifier leur conformité continue aux obligations contractuelles et réglementaires.

9. Relations avec l'Autorité de contrôle

Le Groupe BSL coopère **pleinement avec toute Autorité de contrôle** lorsque cela est requis et fournit toutes les preuves de sa conformité avec la Législation applicable.

Le Délégué à la protection des Données du Groupe BSL agit en **qualité de point de contact** de l'Autorité de contrôle et pilote à ce titre :

- La consultation de l'Autorité de contrôle concernée dans le cas où un Traitement de Données à caractère personnel implique un risque résiduel élevé pour la vie privée ;
- Le signalement d'une Violation de Données à l'Autorité de contrôle lorsque cela est requis ;
- Le Traitement de toutes demandes (telles que les demandes d'accès aux registres de Traitements, les demandes d'information, etc.)

Le Groupe BSL définit une **procédure en cas d'audit** par une Autorité de contrôle, laquelle définit les rôles et responsabilités des acteurs clés dans le cadre de ces contrôles.

REG25 Le Groupe BSL coopère avec l'Autorité de contrôle compétente et définit une procédure en cas de contrôle.

10. Contrôle de la conformité

Le Groupe BSL garantit respect de la présente Politique ainsi que des procédures de mises en œuvre et des politiques supplémentaires relatives à la protection des Données à caractère personnel.

A cette fin, un **contrôle annuel de conformité** est réalisé sur le **respect des règles** édictées et la **concordance des activités de Traitement** mises en œuvre avec le registre des Traitements. Ce dispositif de contrôle est porté par le DPO et toutes les parties prenantes concernées.

Lorsque des manquements sont identifiés, un **plan de remédiation** est défini par le DPO et toutes les parties prenantes concernées afin de remédier aux déficiences détectées, en tenant compte des risques encourus, des coûts de mise en œuvre, des contraintes opérationnelles existantes et prévisibles et des ressources humaines disponibles. Les mesures correctives du plan de remédiation sont mises en œuvre **sans retard injustifié** par les parties prenantes concernées, sous la supervision du DPO.

REG26 Un dispositif de contrôle de la conformité est mis en place.

REG27 Un plan de remédiation est défini et mis en œuvre pour corriger toute non-conformité détectée.

11. Engagements du Groupe BSL en qualité de Sous-traitant

11.1 Le registre des Traitements Sous-traitant

Conformément à la Législation applicable, le Groupe BSL s'engage à tenir à jour un **registre des activités de Traitement mis en œuvre pour le compte de Tiers Responsables de Traitement**. Ce registre doit comporter les informations suivantes :

- Le nom et les coordonnées du Sous-traitant, ainsi que du Responsable de Traitement pour le compte duquel il traite des Données à caractère personnel, ainsi que les coordonnées du DPO ;
- La ou les catégories de Traitements effectués pour le compte de chaque Responsable de Traitement ;
- Le cas échéant, les Transferts de Données à caractère personnel vers un pays Tiers ou de cette organisation internationale ainsi que les documents attestant de l'existence de garanties appropriées ;
- Une description générale des mesures de sécurités techniques et organisationnelles mises en œuvre.

Ce registre de Traitement doit être actualisé autant que de besoin pour être **exact et exhaustif**.

REG28 Un registre des activités de Traitement mis en œuvre en qualité de Sous-traitant est tenu à jour.

11.2 Obligations additionnelles du Groupe BSL en qualité de Sous-traitant

Dans le cadre de ses activités, le Groupe BSL intervient en qualité de Sous-traitant de Tiers Responsables de Traitement. A ce titre, des **obligations spécifiques** s'imposent au Groupe BSL en application desquelles le Groupe BSL s'assure de :

- **Tenir à jour un registre des activités de Traitement** mis en œuvre au nom et pour le compte des Responsables de Traitement (cf. Section précédente) ;
- **Agir dans le cadre des instructions licites** du Responsable de Traitement ;
- **Établir un contrat** avec le Responsable de Traitement conforme aux dispositions de la Législation applicable ;
- **Veiller à l'application des principes de protection des Données à caractère personnel dès la conception et par défaut** ;
- Soumettre les collaborateurs en charge des activités de Traitement à une **obligation de confidentialité** ;
- Respecter les **obligations contractuelles** concernant le recrutement d'un **Sous-traitant ultérieur ;**
- Intégrer à la procédure de gestion des Violations de Données les mesures nécessaires pour **notifier toute Violation de Données au(x) Responsable(s)** de Traitement concerné(s) ;
- Prendre les **mesures techniques et organisationnelles adéquates pour garantir un niveau de sécurité adapté aux risques** ;
- Sur les instructions du Responsable de Traitement, **supprimer ou restituer l'ensemble des Données à caractère personnel** du Responsable de Traitement, sauf obligation légale de les conserver (les Données à caractère non personnel attestant de la bonne exécution des prestations peuvent être conservées pendant la durée de la prescription des actions commerciales) ;
- **Assister, alerter et conseiller** le Responsable de Traitement en :
    - L'informant lorsqu'une instruction est susceptible de constituer une Violation de la Législation applicable ;
    - Aider le Responsable de Traitement à répondre aux demandes des Personnes concernées (une compensation financière pouvant être demandée au Responsable de Traitement) ;
    - Fournir les informations à sa disposition pour permettre au Responsable de Traitement de conduire une Analyse d'impact relative à la protection des Données et de respecter ses obligations en matière de gestion des Violations de Données (une compensation financière pouvant être demandée au Responsable de Traitement) ;
- Mettre à la disposition du Responsable de Traitement les **preuves de sa conformité** et **permettre la réalisation d'audit** (dans les termes et conditions prévues au Contrat).

REG29 Les obligations additionnelles en qualité de Sous-traitant sont mises en œuvre.

Annexe 1 Définitions

Analyse d'impact relative à la protection des Données (ou « AIPD ») : analyse à effectuer par les entités du groupe BSL pour les Traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des Personnes concernées.

Autorité de contrôle : autorité publique indépendante instituée par un État membre en vertu de l'article 51 du RGPD, chargée de surveiller l'application du RGPD, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du Traitement et de faciliter le libre flux des Données à caractère personnel au sein de l'Union européenne.

Consentement : toute manifestation de volonté, libre, spécifique, éclairée, univoque et explicite par laquelle la Personne concernée accepte, par une déclaration ou par un acte positif clair, que ses Données à caractère personnel fassent l'objet d'un Traitement.

Délégué à la protection des Données (ou « *DPO* ») : personne désignée par le Groupe BSL en charge de la protection des Données à caractère personnel au sein des entités du Groupe BSL et de la conformité de celles-ci à la Législation applicable.

Destinataire : 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.

Données à caractère personnel : toute information se rapportant à une Personne concernée notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, un numéro de carte d'identité, un salaire, des dossiers de santé, des informations de compte bancaire, des habitudes de conduite ou de consommation, des Données de localisation, un identifiant en ligne, etc. Le terme « Données à caractère personnel » inclut les Données à caractère personnel sensibles.

Données à caractère personnel sensibles : désigne les Données à caractère personnel révélant ou reposant sur :

- L'origine raciale ou ethnique, les opinions politiques, religieuses ou philosophiques ;
- L'appartenance à une organisation syndicale ;
- La santé physique ou mentale ;
- L'orientation sexuelle ou la vie sexuelle ;
- Les Données génétiques et biométriques ;
- Les Données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes.

Législation applicable : ensemble de réglementation relative à la protection des Données à caractère personnel et applicable aux Traitements de Données à caractère personnel effectués par le Groupe BSL, à l'instar du Règlement (UE) 2016/679 relatif à la protection des Données à caractère personnel (RGPD), de la Loi informatique et libertés modifiée, et de toute autre réglementation qui y serait relative, applicable au Groupe BSL.

Personne concernée : individu sur lequel porte les Données à caractère personnel et qui peut être identifié ou identifiable, directement ou indirectement, grâce à ses Données à caractère personnel. Cela inclut les clients, prospects, et collaborateurs anciens et actuels.

Responsable de Traitement : 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 d'un Traitement de Données à caractère personnel.

RGPD : acronyme du Règlement (UE) 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.

Sous-traitant : toute personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données à caractère personnel au nom du Responsable de Traitement et selon ses instructions (par exemple, des prestataires ou fournisseurs).

Tiers : 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.

Traitement : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des Données à caractère personnel telle que la collecte, l'accès, l'enregistrement, la copie, le Transfert, la conservation, le stockage, le croisement, la modification, la structuration, la mise à disposition, la communication, l'enregistrement, la destruction, que ce soit de manière automatique, semi-automatique ou autre. Cette liste n'étant pas exhaustive.

Transfert de Données : 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, de Données à caractère personnel vers un pays Tiers à l'Union européenne ou à une organisation internationale qui font ou sont destinées à faire l'objet d'un Traitement après ce Transfert.

Violation de Données à caractère personnel : 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.

Marc ALLOUC
Directeur Juridique