Annexe sur la protection des données personnelles

Avertissement

L'ensemble des textes régissant la protection des données personnelles étant soumis à une évolution régulière, la présente annexe sera mise à jour au fur et à mesure de la publication des nouvelles dispositions légales et règlementaires.

A - Définitions

« Données » désigne toutes informations relatives à une personne physique vivante identifiée ou identifiable ; une personne physique vivante identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par rapport à un numéro d'identification ou à un ou plusieurs éléments propres à son identité physique, physiologique, mentale, économique, culturelle ou sociale.

« Données à caractère sensible » désigne toutes données de santé, biométriques, génétiques, données liées à la sexualité ou données sur l'appartenance ethnique ou religieuse.

« Lois relatives à la Protection des Données » désigne le RGPD (Règlement Général sur la Protection des Données) et les lois applicables en matière de protection des données en France, incluant toute nouvelle promulgation ou modification du RGPD et des lois précitées et tous règlements ou ordonnances adoptés en vertu de ce qui précède.

« Traitement » fait référence à toutes les actions qui peuvent être effectuées sur des données personnelles. Cela peut inclure des opérations automatisées ou non automatisées, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la consultation, l'utilisation, la transmission, la diffusion, la mise à disposition, le rapprochement, l'interconnexion, le verrouillage, l'effacement ou la destruction de données personnelles. C'est-à-dire le traitement des données à caractère personnel fait référence à toutes les actions effectuées sur ces données, qu'elles soient automatisées ou non, et qui peuvent être liées à la collecte, à la gestion, à la transmission, à l'utilisation ou à la suppression de ces données contenues dans des fichiers.

« Responsable de traitement » : Le Directeur Général de l'APST-BTP-RP est désigné en tant que Responsable de traitement.

« Délégué à la Protection des Données (DPO) » : Le DPO travaille en étroite collaboration avec le Responsable de traitement pour garantir que l'APST-BTP-RP respecte toutes ses obligations légales et règlementaires en matière de protection des données.

B - Obligations respectives de l'APST-BTP-RP et de ses adhérents

Responsable de traitement

Le Directeur Général de l'APST-BTP-RP agit en tant que Responsable de traitement des données. En cette qualité, il est chargé de superviser l'ensemble des politiques et des procédures de protection des données mises en œuvre par l'APST-BTP-RP. Il coordonne également les évaluations d'impact sur la protection des données et assure la gestion des réponses de l'organisation en cas de violation de données. Il veille à ce que l'APST-BTP-RP respecte toutes ses obligations légales en matière de protection des données.

Dans le cadre de la relation avec les entreprises adhérentes, le Responsable de traitement supervise la collecte, le traitement et le partage des données, garantissant la conformité avec toutes les obligations règlementaires et légales.

Le Responsable de traitement est également responsable de la formation des employés en matière de protection des données et de la réalisation d'audits réguliers pour garantir la conformité de l'organisation.

Délégué à la Protection des Données (DPO)

Le DPO de l'APST-BTP-RP joue un rôle essentiel pour garantir la conformité de l'organisation en matière de protection des données. Il travaille en étroite collaboration avec le Responsable de traitement pour superviser la mise en œuvre des politiques de protection des données et s'assure que les principes de protection des données sont respectés dans toutes les opérations de traitement de données.

En cas de questions ou de demandes concernant la protection des données, le DPO est le point de contact principal, tant pour les employés que pour l'extérieur de l'organisation, y compris les autorités de contrôle de la protection des données.

Dans le cadre des relations avec les entreprises adhérentes, le DPO travaille en étroite collaboration avec le Responsable de traitement pour s'assurer que toutes les données partagées sont traitées de manière conforme et sécurisée.

Prévention et santé au travail et obligation des employeurs

D'une part, les missions et responsabilités des Services de Prévention et de Santé au Travail sont définies par plusieurs textes de lois :

- La loi n° 2011-867 du 20 juillet 2011,
- La loi n° 2016-1088 du 8 août 2016,
- Le décret n°2016-1908 du 27 décembre 2016 qui définissent les quatre missions essentielles des Services de Santé au Travail, assurées par une équipe pluridisciplinaire, animée et coordonnée par le médecin du travail : action en entreprise, conseil, surveillance de l'état de santé, traçabilité et veille sanitaire,
- Le décret n° 2022-1749 du 30 décembre 2022 relatif au financement des services de prévention et de santé au travail interentreprises,
- Le décret n° 2022-653 du 25 avril 2022 relatif à l'approbation de la liste et des modalités de l'ensemble socle des services de prévention et de santé au travail,
- D'autre part, l'adhésion à un service de santé au travail est une obligation faite à tout employeur dès l'embauche du premier salarié quelles que soient la nature et la durée du contrat de travail (Art. L.4622-1 et L4622-6 du Code du travail).

Relations entre l'APST-BTP-RP et ses entreprises adhérentes

Les relations entre un employeur adhérent et un Service de Prévention et de Santé au Travail sont régies par les textes réglementaires (lois, code du travail, code de la santé publique...) et par les dispositions des statuts de l'APST-BTP-RP et du règlement intérieur du Service de Santé au Travail (Art. D.4622-22 du Code du travail).

En particulier, l'adhérent a une obligation envers le Service de Prévention et de Santé au Travail de :

- Demander les visites pour ses salariés dans les délais et en garder la preuve,
- Informer le médecin du travail des arrêts pour les accidents du travail de moins de 30 jours,
- S'assurer du suivi des avis d'aptitude, de la réalisation des visites médicales et des visites d'information et de prévention,
- Envoyer une déclaration préalable précisant le nombre et la catégorie des salariés à suivre et les risques professionnels auxquels ils sont exposés,
- Transmettre chaque année une déclaration des effectifs en distinguant notamment les salariés soumis à un suivi individuel renforcé,
- Inviter au Comité Social et Economique le médecin du travail pour les questions relevant de sa compétence,
- Transmettre les fiches de postes au médecin du travail afin que les avis d'aptitude soient circonstanciés,
- Transmettre les fiches de données de sécurité des produits chimiques utilisés à l'équipe santé travail,
- Communiquer les éléments de compréhension du fonctionnement de l'entreprise et de ses risques professionnels.

Modalités d'échange entre l'APST-BTP-RP et ses adhérents

Afin d'assurer leurs obligations respectives, l'APST-BTP-RP et ses adhérents doivent échanger des données personnelles qui permettront à l'APST-BTP-RP d'organiser le suivi individuel de l'état de santé de chaque salarié des adhérents mais également d'assurer le suivi administratif de chaque adhérent. Ces données sont échangées par tous moyens disponibles : électronique, papier ou communication orale.
Il est précisé qu'il n'existe aucun échange entre l'APST-BTP-RP et ses adhérents portant sur les données personnelles à caractère sensible ou médicale.

Le présent document a pour objectif de préciser les engagements de l'APST-BTP-RP dans le recueil, le traitement, la protection et la conservation de ces données personnelles afin d'assurer le respect de l'ensemble des dispositions légales et règlementaires relatives à la protection des données.

Consentement et droit d'information des salariés de l'adhérent

Il est précisé que l'adhérent, préalablement à tout transfert de données personnelles concernant ses salariés, a fait son affaire des obligations d'information des salariés concernés et s'est conformé à toute obligation de notification et/ou d'enregistrement précisée par les Lois relatives à la Protection des Données. L'adhérent doit informer ses salariés de la nature des données collectées, des finalités du traitement, des destinataires des données, ainsi que de leurs droits en matière de protection des données.

C - Traitement des données

Données collectées à des fins de gestion de la relation avec l'entreprise

Dans le cadre des services rendus à ses entreprises adhérentes, l'APST-BTP-RP collecte des données à caractère personnel des salariés de celles-ci (contrat d'adhésion, déclaration d'effectifs...) qui font l'objet de traitements automatisés à des fins de gestion administrative de la relation avec l'entreprise (facturation, assistance, gestion commerciale, téléphonie, amélioration de la qualité, de la sécurité et de la performance des services, recouvrement, etc...).
Les données concernées sont essentiellement les noms, prénoms, numéros de téléphones, adresses mail des dirigeants et salariés de l'entreprise en charge de la relation avec l'APST-BTP-RP.

Données collectées à des fins de gestion du suivi individuel de l'état de santé des salariés

Afin de respecter ses obligations de suivi individuel de l'état de santé des salariés de ses entreprises adhérentes, l'APST-BTP-RP collecte les données à caractère personnel auprès de l'entreprise. Ces données, recueillies au moment de l'adhésion de l'entreprise, lors de l'embauche de nouveaux collaborateurs et mis à jour régulièrement, concernent exclusivement l'identification des salariés (nom, prénom, sexe, date de naissance, poste, ancienneté ...). Ces données font l'objet de traitements qui ont pour objectif unique la gestion administrative de la relation entre l'APST-BTP-RP et le salarié concerné (organisation des visites médicales et entretiens de suivi).

Les données sont conservées pour la durée nécessaire à l'exécution des objectifs mentionnés ci-dessus. Après cela, elles sont soit supprimées, soit anonymisées et conservées à des fins statistiques.

Secret professionnel et confidentialité des données

D'une part, l'ensemble du personnel de l'APST-BTP-RP est soumis au secret professionnel (par l'article 226-13 du code pénal, l'article 1110-4 du code de santé publique et le code de déontologie médicale).

D'autre part, la relation contractuelle entre l'APST-BTP-RP, son éditeur de progiciel et son hébergeur de données, étend à ceux-ci les obligations de secret professionnel.

Dans ces conditions, l'APST-BTP-RP s'engage à ne pas utiliser les données ainsi collectées à d'autres fins que celles susmentionnées dans les deux paragraphes ci-dessus et à n'en faire communication à aucun tiers, et à faire respecter ces dispositions par ses salariés et ceux de ses sous-traitants ou fournisseurs intervenant dans la gestion des données personnelles concernées.

Une exception à cet engagement est possible : la fourniture de données aux autorités judiciaires et / ou administratives, notamment dans le cadre de réquisitions.

Dans ce cas, et sauf disposition légale l'en empêchant, l'APST-BTP-RP s'engage à en informer l'adhérent et à limiter la communication de données à celles expressément requises par lesdites autorités.

Une autre exception à cet engagement pourrait survenir si l'APST-BTP-RP est impliqué dans une fusion, acquisition, réorganisation ou autre forme de transaction. Dans ce cas, nous nous engageons à garantir la confidentialité des données personnelles et à informer les adhérents avant que leurs données personnelles ne soient transférées ou soumises à des règles de protection des données différentes.

Hébergement des données et sécurité des données

L'ensemble des données concernées par les traitements susmentionnés sont hébergées exclusivement sur le territoire français, par la société SI2S d'une part et ADDEO d'autre part. Ces sociétés fournissent à l'APST-BTP-RP un service de haute disponibilité (backup en continu des données, plan de reprise d'activité) et d'un haut niveau. Pour les données de santé, SI2S et ADDEO travaillent avec des hébergeurs disposant de l'agrément « hébergeur de données de santé » délivré par l'Agence des Systèmes d'Information Partagés (ASIP) et sont donc conformes à l'ensemble des référentiels en vigueur dans le domaine de la protection des données de santé et des données personnelles.

Ainsi l'APST-BTP-RP est en mesure, conformément à l'article 34 de la loi Informatique et Libertés modifiée et au Règlement Général sur la Protection des Données (RGPD), d'assurer à ses adhérents que toutes les précautions utiles pour préserver la sécurité et la confidentialité des données à caractère personnel, et notamment empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès, ont été prises.

En particulier, en conformité avec son contrat d'hébergement avec l'APST-BTP-RP, les hébergeurs ont mis en place :

- Des mesures de sécurité physique visant à empêcher l'accès aux Infrastructures sur lesquelles sont stockées les données de l'APST-BTP-RP par des personnes non autorisées,
- Des contrôles d'identité et d'accès via un système d'authentification ainsi qu'une politique de mots de passe,
- Un système de gestion des habilitations permettant de limiter l'accès aux locaux aux seules personnes ayant besoin d'y accéder dans le cadre de leurs fonctions et de leur périmètre d'activité,
- Un personnel de sécurité et des dispositifs de vidéosurveillance chargés de veiller à la sécurité physique des locaux,
- Un système d'isolation physique et logique des clients entre eux,
- Des processus d'authentification des utilisateurs et administrateurs, ainsi que des mesures de protection des fonctions d'administration,
- Dans le cadre d'opérations de support et de maintenance, un système de gestion des habilitations mettant en œuvre les principes du moindre privilège et du besoin d'en connaître,
- Des processus et dispositifs permettant de tracer l'ensemble des actions réalisées sur son système d'information, et d'effectuer conformément à la réglementation en vigueur, des actions de reporting en cas d'incident impactant les données de l'APST-BTP-RP.

L'APST-BTP-RP met en place des procédures robustes pour agir en cas de violation de données. L'APST-BTP-RP a des protocoles pour informer règlementairement les autorités de contrôle et les individus dont les données pourraient être affectées par une telle violation.

Pour garantir la confidentialité et l'intégrité des données, l'APST-BTP-RP utilise des techniques de chiffrement pour sécuriser les données pendant leur transmission et leur stockage.

De plus, l'APST-BTP-RP réalise régulièrement des audits et des révisions de sa sécurité pour s'assurer que ses mesures sont à jour et qu'elles répondent aux meilleures pratiques de l'industrie. Les procédures de contrôle et d'audit de sécurité sont effectuées au moins une fois par an ou à chaque fois que des changements significatifs sont apportés à ses systèmes d'information.

Exercice des droits relatifs aux données personnelles

Conformément au Règlement Général sur la Protection des Données (RGPD) et à la loi "Informatique et Libertés" du 6 janvier 1978, l'adhérent et le salarié suivi bénéficient des droits suivants relatifs à leurs données personnelles :

Droit d'accès : Les individus ont le droit de savoir si leurs données sont traitées, quelles sont ces données, pourquoi elles sont traitées, et à qui elles peuvent être divulguées.

Droit de rectification : Les individus ont le droit de faire rectifier ou compléter des informations inexactes ou incomplètes les concernant.

Droit à l'effacement ("droit à l'oubli") : Dans certains cas, les individus ont le droit de demander la suppression de leurs données.

Droit à la limitation du traitement : Les individus ont le droit de demander la limitation du traitement de leurs données dans certaines circonstances.

Droit à la portabilité des données : Les individus ont le droit de recevoir leurs données dans un format structuré, couramment utilisé et lisible par machine, et de transmettre ces données à un autre contrôleur de données.

Droit d'opposition : Les individus ont le droit de s'opposer au traitement de leurs données pour des raisons liées à leur situation particulière.

Ces droits peuvent être exercés en envoyant un courrier postal à l'adresse : APST-BTP-RP - Service adhérents, 110 avenue du Général Leclerc BP 1, 92340 BOURG-LA-REINE, en justifiant de son identité. Il est également possible de contacter le Délégué à la Protection des Données (DPO) de l'APST-BTP-RP à l'adresse électronique suivante : dpo@apst.fr pour toute question relative à la protection des données personnelles.

Concernant les données administratives, il y sera répondu dans un délai d'un mois suivant réception, sauf en cas de complexité ou du nombre élevé de demandes, où ce délai peut être prolongé de deux mois supplémentaires.
Concernant spécifiquement les demandes d'accès aux données de santé, en vertu de l'article L.1111-7 du code de la santé publique, il sera répondu dans un délai maximum de 8 jours à partir de la réception de la demande. En cas de données de santé datant de plus de 5 ans, ce délai peut être prolongé jusqu'à 2 mois.

En cas de non-réponse ou de réponse insatisfaisante, l'individu a le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente, en France, la Commission Nationale de l'Informatique et des Libertés (CNIL).

Coordonnées des personnes à contacter pour toute question relative à vos données :

Traitement des données

Monsieur le Directeur Général
Responsable du traitement des données
APST-BTP-RP
Direction Générale
110 avenue du Général Leclerc - BP 1
92340 BOURG-LA-REINE

Protection des données

Monsieur le Délégué à la Protection des Données
APST-BTP-RP
110 avenue du Général Leclerc - BP 1
92340 BOURG-LA-REINE

Fait à Bourg-la-Reine, le jeudi 25 avril 2024

Le Président de l'APST-BTP-RP

Christian GONNET

Association de Prévention et de Santé au Travail du Bâtiment et des Travaux Publics de la Région Parisienne
APST-BTP-RP
110, av. du Général Leclerc
92340 BOURG-LA-REINE