PCS AVOCAT
Droit des affaires & Nouvelles Technologies

Safebear

Procédure de protection des données personnelles

A jour du 1er mai 2023

Préambule

Contexte réglementaire

Le 25 mai 2018 est entré en application le Règlement Général sur la Protection des Données (RGPD). Tous les organismes privés et publics sont désormais soumis à un ensemble d'obligations, qui pour certaines, préexistaient sous l'égide de la Directive 95/46/ CE et la loi dite « Informatique et Libertés ».

Dans ce contexte, Safebear s'engage à respecter toutes les obligations lui incombant résultant de la réglementation applicable au traitement de données à caractère personnel, spécialement :

- Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après, « le règlement européen sur la protection des données » ou « RGPD »).

- La directive (ue) 2016/680 du parlement européen et du conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil

- La Loi Informatique et Libertés n°78-17 du 6 janvier 1978 modifiée ;

- Les règles spécifiques à ses activités notamment en matière de secret professionnel ;

- Et toutes recommandations de toute autorité de contrôle compétente notamment la CNIL, AMF, DGCCRF, etc.

Principes essentiels

Cette procédure a pour objectif de fixer le cadre et les principes de base pour la protection et le traitement des données personnelles au sein de Safebear (ci-après la « Société »).

En tant qu'employeur, salarié, partenaire, client et fournisseur, chaque membre de la Société collecte et utilise des données personnelles concernant ses employés, se contacts d'affaires, ses clients, prospects, etc. Le traitement des données personnelles étant indispensable à ses activités, la Société considère que la protection des droits personnelles et de la sphère privée de chaque individue est la base de toute relation de confiance.

Il apparait essentiel à Safebear d'être en conformité avec les obligations pour la Protection des Données Personnelles dans les pays où ses affaires sont conduites et où les personnes concernées résident.

Tous les membres de la Société doivent se conformer aux règles en vigueur localement et relatifs au contrôle et au traitement des données personnelles. Cette Procédure doit être portée à la connaissance de tous les employés de la Société devant se conformer avec la Procédure et ses exigences.

D'autre part, la procédure s'applique également aux tiers ayant à faire aux membres de la Société et qui ont ou pourraient avoir accès aux Données Personnelles. Ces tiers sont censés avoir lu et compris la présente procédure et doivent être en conformité avec elle.

N.B : Faute d'activité impliquant le transfert de données à l'extérieur de l'Union européenne dans le cadre du lancement de l'activités, les dispositions réglementaires applicables en matière de données personnelles se concentrent sur les textes français et communautaires.

Ces dernières seront toutefois pleinement applicables en cas de collecte et/ou transfert de données personnelles en dehors de la zone couverte par les dispositions énoncées.

PCS AVOCAT
Droit des affaires & Nouvelles Technologies

Définitions

Sauf indication contraire, les mots et expressions définies dans la présente procédure sont identiques et ont exactement les mêmes significations que celles proposées et définies par la Commission Nationale Informatique et Liberté ainsi que dans l'ensemble des documents se rattachant à la conformité de Safebear à la réglementation en matière de protection des données.

Accountability : Désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

Analyse d'impact : Etude à l'initiative du responsable de traitement menée lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Base légale : Aussi appelé fondement juridique ou base juridique, origine légale motivant et autorisant légalement mise en œuvre d'un traitement de données personnelle, ce qui donne le droit à un organisme de collecter ou d'utiliser des données personnelles.

Biométrie : Ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales.

Bring your own device (BYOD) : Pratique consistant à utiliser ses équipements personnels (téléphone, ordinateur portable, tablette électronique) dans un contexte professionnel.

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

Contrôleur des données : Personne naturelle ou légale, autorité publique, agence ou tout autre organisme, qui seul ou ensemble avec des tiers, détermine le but et les moyens mis en place pour le traitement des données personnelles.

Cookies : Fichier informatique stocké par un serveur dans le terminal (ordinateur, téléphone, etc.) d'un utilisateur et associé à un domaine web (c'est à dire dans la majorité des cas à l'ensemble des pages d'un même site web). Ce fichier est automatiquement renvoyé lors de contacts ultérieurs avec le même domaine.

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.

Donnée personnelle : Toute information se rapportant à une personne physique identifiée ou pouvant être identifiée directement ou indirectement par un élément d'identification tel qu'un nom, un numéro de téléphone, une adresse postale, une adresse e-mail, un numéro d'identification, des données de localisation, etc.

Données sensibles : Catégorie de données personnelles regroupant les informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Registre de traitement : Le registre des activités de traitement permet de recenser vos traitements de données et de disposer d'une vue d'ensemble de ce que le responsable de traitement fait avec les données personnelles.

Responsable du traitement : Personne physique ou morale, publique ou privée ou le service, qui détermine seul ou avec d'autres les finalités et les moyens du traitement.

Sous-traitant : Personne physique ou morale, publique ou privé, ou le service qui traite des données personnelles pour le compte du responsable de traitement.

Traitement de données personnelles : Toute opération réalisée sur des données personnelles telle que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la consultation, l'utilisation, l'interconnexion, la limitation, l'effacement, la destruction, etc.

Transfert de données : Toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne.

Personne concernée : Signifie toute personne vivante concernée par les donnes personnelles détenues par la Société.

Pseudonymisation : Traitement de données à caractère personnel effectué de telle façon que les données ne peuvent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires.

Violation de données à caractère personnel : Toute action impliquant une violation de la sécurité physique, technique ou informatique 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.

Périmètre et organisation

Le présent document encadre les procédures applicables à l'ensemble des effectifs de Safebear. Il recouvre notamment la politique générale de Safebear en matière de protection des données personnelles et les procédures relatives à toute demande de personnes pour faire valeurs leurs droits voire notifier ou dénoncer d'éventuelles violations ou infractions constatées.

Plusieurs annexes reprenant les documents essentiels liés à la protection des données personnelles au sens des dispositions règlementaires du RGPD sont associées notamment les références documentaires dont le guide de conformité et le registre des traitements de la Société, le planning de conservation des données ou encore les références légales.

PCS AVOCAT
Droit des affaires & Nouvelles Technologies

Référents

Responsable de traitement

Safebear est une société par actions simplifiée au capital de 2 330.16 €, enregistré au RCS de Paris sous le numéro 913 424 362 et dont le siège social se trouve 35 rue du General Foy, 75008 Paris, représenté par son président **Christian Guillon**, agissant en tant que responsable des traitements pour le compte de la société.

Le responsable de traitement est la personne morale (entreprise, commune, etc.), incarnée par son représentant légal qui détermine les finalités et les moyens d'un traitement de données personnelles.

Délégué à la protection des données

Le délégué à la protection des données de Safebear est le cabinet **PCS Avocat**, dont le siège est situé 26 avenue George V, 75008 Paris, px@chomiacdesas.com, en cours de déclaration à la CNIL.

Dans le cadre du respect des dispositions règlementaires applicables en matière de protection des données, Safebear a désigné un Délégué à la Protection des données, chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.

Responsable technique de la sécurité des systèmes d'information

Cette mission a été confié à **Jérémy Guillon**, directeur général de la Société.

Afin de préserver la sécurité des données personnelles collectées et de son système informatique, SafeBear a désigné un prestataire technique en charge de la sécurité des infrastructures numériques. Il veille notamment à la sécurité des données, à leurs confidentialités par des accès et habilitations restrictifs et sensibilise les collaborateurs sur l'importance de cette protection.

Interlocuteurs internes

Assistant les responsables de traitements et délégué à la protection des données dans la mise en place de la conformité au RGPD de l'entreprise, Safebear a mandaté plusieurs interlocuteurs internes afin d'optimiser les missions et respect des obligations réglementaires.

PCS AVOCAT
Droit des affaires & Nouvelles Technologies

Plan détaillé

Section 1. Collecte et traitement des données par la Société

Collecte & licéité des traitements de données

Safebear garantit que les données personnelles issus de ses traitements sont collectées et traitées de façon juste et en conformité avec la loi. Nous prenons toutes les mesures nécessaires afin de tenir les données à jour et exactes et les conserverons uniquement pour une durée définie au préalable.

Pour rappel, Safebear justifie les traitements présentés au regard de fondements légitimes envisagées par la réglementation notamment :

i. Traitements fondés sur le consentement ;
ii. Traitements fondés sur l'exécution d'un contrat entre la personne concernée et un autre organisme ;
iii. Traitements fondés sur une obligation légale ;
iv. Traitement fondé sur l'intérêt légitime de Safebear.
v. Le cas échéant, traitements fondés sur une mission d'intérêt public ;

La présentation des données personnelles collectées et traitées est présentée et détaillé au sein du Registre de Traitement, conformément aux obligations légales et règlementaires.

Conservation des données et règles de suppression

Pour rappel, l'article 5.1 du RGPD envisage les six principes fondateurs qui gouvernent tout traitement de données à caractère personnel, et qui englobent notamment le principe dit de minimisation de la durée de conservation des données.

Safebear œuvre à distinguer de manière claire au sein de sa documentation réglementaire notamment le Registre de traitement la distinction des données selon leur « cycle de vie » :

- les données issues de la base courante sont conservées à partir de leur collecte jusqu'à la fin de leur utilisation courante. Pendant cette période, le responsable de traitement doit mettre en place des mesures de sécurité standards ;
- les données d'archives intermédiaires ayant une utilité administrative notamment en cas de contentieux bénéficient d'un accès restreint ;
- les données d'archives définitives, à défaut d'être définitivement supprimés ; peuvent être anonymisées et conservées de manière illimitée.

La Société organise la mise en place de planning de conservation. Les délais de conservation sont basés sur les obligations locales légales pour les différents types de catégories des données personnelles.

Certaines données personnelles sont susceptibles d'être conservées pour une durée supérieure à la simple finalité de traitement envisagée par la Société. Ce peut être notamment le fait d'obligations légales ou de demandes émanant d'autorités compétentes et habilitées au regard notamment de problématiques d'ordre judicaire, fiscal ou comptable.

Dans tous les cas, toutes les données personnelles seront conservées pour une durée minimale permettant à la Société de procéder à la finalité du traitement envisagée ou de se conformer aux obligations légales mentionnées.

Un plan de purge des données personnelles est en préparation veillant à structurer les modalités de suppression des données : identification, mode et lieu de suppression, log des opérations, etc.

Registre de traitement et documentation associée

La Procédure intègre la création et mise à jour trimestrielle du registre de traitement (ci-après le « Registre ») par le Délégué à la protection des données avec l'aide et l'assistance des autres Référents. Ce document a vocation à retracer toute manipulation de données personnelles, ou traitement, par son inscription associée au renseignement d'information complémentaires.

Outre la conformité aux dispositions réglementaires notamment de l'article 30 du RGPD, le Registre garantit l'homogénéité des analyses et méthodologie d'identification des données personnelles, ces dernières ayant été mises en place de manière adaptée et adéquates aux spécificités des activités de Safebear.

Il permet notamment de vérifier la cohérence des flux de données et leur intérêt afin de garantir la sécurité des données et l'identification de l'ensemble des traitements.

Le Registre comporte un ensemble d'informations relevant des caractéristiques des collectes et traitements de données personnelles notamment leur finalité, le département/service concerné, les activités liées et associées, la source de la collecte et son fondement légal, les catégories de personnes et de données, les spécificités liées aux données potentiellement sensibles, la présentation de transferts internes ou externes des données notamment hors UE, les conditions de stockage et de conservation ainsi que les règles de sécurité et modalité d'exercice de droit.

PCS AVOCAT
Droit des affaires & Nouvelles Technologies

Section 2. Gouvernance des données personnelles

Organisation interne

Pour rappel, la Société a créé pour plusieurs référents relatifs à la procédure dont le Responsable de Traitement, le Délégué à la protection des données, le Responsable technique de la sécurité de systèmes d'information ainsi que les interlocuteurs internes dont les coordonnées ont été rappelées en préambule et sont régulièrement mises à jour (ci-après le(s) « Référent(s) »).

Le Délégué à la Protection des données, nommé par la Société, participe à l'application de l'ensemble des obligations inhérentes aux dispositions règlementaires relatives à la protection des données personnelles. Il assure notamment la gestion des droits des personnes, l'accompagnement et validation des analyses d'impact sur la vie privée, la création et mise à jour de la documentation notamment le registre des traitements, la formation des membres de la Société, le pilotage des plans d'action de mise en conformité de la Société, la prise en compte des règles de privacy by design et by default.

Il est également l'interlocuteur privilégié avec l'autorité de contrôle et autre entités judiciaires en matière de données personnelles.

Les Référents, membres de la Société ou prestataire externe ont vocation à assister ou participer à l'ensemble des activités liées à la protection des données personnelles au sein de Safebear, apportant leur expertise dans les différents domaines pouvant impliquer la collecte, traitement de données personnelles ou leurs conditions de stockage et de sécurité : direction marketing, direction client, direction juridique, direction des systèmes d'information, direction des ressources humaines, direction du contrôle interne, direction de la communication, direction financière. Ensemble, les Référents ont notamment vocation à :

- Anticiper la protection des données dès la conception d'un traitement et la sécurité par défaut (Privacy by design / default) ;
- Sensibiliser les membres de l'entreprise et les parties prenantes ;
- Traiter les demandes des personnes souhaitant exercer leurs droits.

Gestion des demandes

Toute question ou interrogation concernant cette Procédure et ses annexes peut être envoyée au Délégué à la Protection des Données ou tout Référent.

Les personnes concernées par une réclamation relative au traitement de leurs Données Personnelles doivent transmettre leur demande par écrit à la Société ou au Délégué à la Protection des Données. Chaque enquête sur les réclamations sera effectuée de façon appropriée au cas spécifique. Le Délégué à la Protection des données ou à défaut l'un des Référents informera la personne concernée sur les suites données à la réclamation dans un délai de temps raisonnable.

Formalisme et contrôle

Afin de faciliter les demandes d'exercice du droit d'accès et de copie de toute personne concernée par un des traitements mis en œuvre par l'établissement, Safebear a organisé par le biais des Référents notamment le Délégué à la Protection des Données la gestion des droits d'accès afin de conserver le niveau de confidentialité adéquat pour la gestion de telles demandes.

La Procédure comprend l'identification de l'auteur d'une demande d'exercice de droit – conformation, accès, actualisation, rectification, effacement, limitation, portabilité – pouvant impliquer des informations complémentaires. En effet, conformément à la législation sur la protection des données à caractère personnel, les personnes sont informées qu'il s'agit d'un droit individuel qui ne peut être exercé que par la personne concernée relativement à ses propres informations : pour des raisons de sécurité, les Référents seront amenés à vérifier l'identité de l'auteur de la démarche afin d'éviter toute communication d'informations confidentielles à des tiers ou l'exercice de procédures abusives et/ou illicites.

Par ailleurs, les Référents sont susceptibles d'analyser, confirmer ou infirmer le bienfondé de leur(s) demande(s). A titre d'exemple, le droit à l'effacement ne sera pas applicable dans les cas où le traitement est mis en œuvre pour répondre une obligation légale. Les personnes pourront demander l'effacement de leurs données dans les cas limitatifs suivants :

- les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
- lorsque la personne concernée retire le consentement sur lequel est fondé le traitement et qu'il n'existe pas d'autre fondement juridique au traitement ;
- la personne concernée s'oppose à un traitement nécessaire aux fins des intérêts légitimes poursuivis par Safebear et qu'il n'existe pas de motif légitime impérieux pour le traitement ;
- la personne concernée s'oppose à un traitement de ses données à caractère personnel à des fins de prospection, y compris au profilage ;
- les données à caractère personnel ont fait l'objet d'un traitement illicite.

Traitement et suivi des réclamations

Des procédures de gestion des demandes d'accès mises en place par la Société distinguent selon l'origine de la demande et les liens auprès de la société – salarié, anciens salariés, personnes en processus de recrutement, clients, partenaires fournisseurs, etc.

Assurant son obligation de transparence, la Procédure de gestion des demandes est accompagnée d'une information exhaustive précisant notamment le rappel du droit exercé, ses modalités d'exercice, le contact compétent et les coordonnées de l'interlocuteur privilégié pour l'appliquer, les informations relatives au droit de copies de données ainsi que, le cas échéant, un rappel de la prohibition de l'exercice de ce droit de façon abusive.

Si, malgré les réponses apportées par le Délégué à la Protection des données, la réclamation ou litige relevant d'un traitement de données personnelles de la Société perdure, la personne concernée peut, au choix, avoir recours à un médiateur, à un processus d'arbitrage exécutoire, à un contentieux ou à une réclamation déposée auprès de l'autorité de la Protection des Données en charge dans la juridiction concernée.

Section 3. Sécurité des données personnelles

Violation des données

Organisation et sécurité

Pour rappel, une violation des données personnelles est une violation de la sécurité entraînant une destruction, perte, altération ou transmission non autorisée, ou accès non autorisé à, des Données Personnelles transmises, stockées ou autrement traitées. De tels incidents pourraient se produire techniquement ou physiquement.

Conformément aux articles 33 et 34 du RGPD en cas de violation de données personnelles, le responsable de traitement notifie cette violation à l'autorité compétente dans les délais prévus. Si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement le communique à la personne concernée dans les meilleurs délais.

Fort de situations antérieures vécues par Safebear, des procédures d'investigation de reporting relatives aux éventuelles violations ont été préparées avec les différents acteurs techniques, juridiques de manière à garantir la meilleure réactivité et efficacité en cas d'identification d'une violation de données.

En complément, la Société garde un registre des violations, dans lequel elle conserve les informations sur les faits relatifs à toute violation de données personnelles, les effets des violations et les actions mises en place pour y remédier.

Procédure de gestion des violations de données

Dans le cas de la survenance d'une violation de données constatées, Safebear organise des procédures visant à proposer une réponse efficace dans le meilleur délai possible, au plus tard 72 heures après qu'il en ai pris connaissance. Il implique notamment (i) la remontée de l'information concernant la violation aux Référents, (ii) l'analyse du risque sur la vie privée, (iii) la détermination de concert des mesures de rémédiation, (iv) la notification à a la CNIL et/ou aux personnes concernées ainsi qu'aux autres autorités pertinentes, (v) le cas échéant le lancement de procédures judiciaires notamment pénales contre les auteurs de la violation notamment en cas d'attaque informatique, (vi) la consignation des informations dans le registre de violation des données.

Conformément aux obligations réglementaires précisées notamment aux articles 33 et 34 du RGPD, le registre de violations des données, conservé par le Délégué à la Protection des données comprend les informations suivantes :

- Nature et date de la violation de données ;
- Catégories et nombre approximatif de personnes et de données concernées ;
- Mesures de remédiation ;
- Date de notification ou justification d'absence de notification.

Pour information, la dernière procédure engagée par Safebear en la matière a inclus la mise en place des actions suivantes :

- Identifier et corriger la faille dans un premier temps afin de limiter au maximum ses conséquences sur les données à caractère personnel visées ;
- Constituer un dossier de preuve technique, notamment par la création d'un document comportant une description de la faille identifiée, de ses conséquences réelles ou supposées sur les données et des mesures prises pour la corriger ;
- S'interroger sur la qualification juridique éventuellement susceptible de s'appliquer ;
- Le cas échéant et selon les résultats de cette analyse, déposer une plainte pénale ;
- Notifier à la CNIL la violation de sécurité, si possible dans les 72 heures après avoir pris connaissance des faits ;
- Si la faille de sécurité emporte des conséquences sur des données à caractère personnel, communiquer aux personnes concernées à propos de celle-ci conformément aux dispositions de l'article 34 précité ;
- Prendre attache avec sa compagnie d'assurance, étant précisé qu'il existe des polices d'assurance couvrant spécifiquement les risques afférents à la protection des données à caractère personnel.

Procédures de réclamation

Comme évoqué, toute question ou interrogation concernant cette Procédure et ses annexes peut être envoyée à tout Référent de la Société tel que présenté en préambule de la Procédure de Protection des Données.

Les personnes concernées par une réclamation relative au traitement de leurs Données Personnelles doivent transmettre leur demande par écrit au Responsable de Traitement ou au Délégué à la Protection des Données. Chaque enquête sur les réclamations sera effectuée de façon appropriée au cas spécifique. L'interlocuteur de la Société informera la personne concernée sur les suites données à la réclamation dans un délai de temps raisonnable.

Si le problème ne peut être résolu par une consultation entre la personne concernée et le Référent de la Société, la personne concernée peut, au choix, avoir recours à un médiateur, à un processus d'arbitrage exécutoire, à un contentieux ou à une réclamation déposée auprès de l'autorité de la Protection des Données en charge dans la juridiction concernée.

Personnes habilitées

Conformément aux dispositions réglementaires applicables, seul un nombre limité de personnes sont susceptibles d'avoir accès aux données personnelles faisant l'objet d'une collecte ou traitement par la Société. Ces derniers sont identifiés selon leur rôle au sein de la société, leurs fonctions et missions et plus généralement l'opportunité de connaitre les données concernées au regard notamment de la finalité du traitement.

Dans ces conditions, selon les données et le traitement en cause et sauf disposition législative, règlementaire ou décision de justice contraire, les destinataires des données concernées peuvent être des salariés internes de la société, d'éventuels sous-traitants (prestataires informatiques, hébergeurs, experts comptable, conseil juridique, etc.), des partenaires et clients de la société voire des organismes et autorités publiques). Le détail de ces informations est présenté dans le Registre de traitement et est régulièrement mis à jour par les Référents de la Société.

Sécurité du traitement

La Société s'engage à maintenir un niveau de sécurité adéquat compte tenu des usages et pratiques pour la sécurité de ses systèmes informatiques. Il inclue des mesures physiques, techniques et organisationnelles afin de garantir la sécurité des données personnelles ainsi que des mesures de prévention contre la perte ou l'endommagement, altération non autorisée,

accès ou traitement, et d'autres risques qui pourraient survenir par action humaine ou l'environnement physique ou naturel.

La Société emploie ses meilleurs efforts pour veiller notamment à ce que l'accès aux données personnelles traitées intègrent une protection par login et mot de passe avec les exigences posées par la Société, la conservation sur un support informatique crypté et pouvant être supprimé efficacement selon les procédures de réclamation validées et tout autre méthode jugée pertinente ou utile par la Société et ses Référents.

Les données personnelles seront détruites ou éliminées uniquement en conformité avec le planning de conservation.

La Société doit s'assure que les Données Personnelles ne sont pas rendues accessibles à des tiers, y compris membres de la famille, amies, autorités gouvernementales sauf si requis par la loi. Chaque demande de fournir des données pour une de ces raisons doit être accompagnée par des documents appropriés et doit être autorisée par le Responsable de traitement et le Délégué à la Protection des données.

La Société s'assure que l'ensemble de ses membres adhèrent à cette Procédure et autres documents encadrant leurs conditions de travail. D'autre part, la Société s'engage à ce que ses employés participent à la sécurité et protection des données dans l'exécution de la Procédure.

Sensibilisation des effectifs de la Société

Formation continue

Safebear s'engage à informer l'ensemble de ses salariés ayant accès aux Données Personnelles, de leurs responsabilités relatives à cette Procédure, et ceci comme partie intégrante de la formation d'intégration du personnel, avec le cas échéant notamment pour les Référents internes de l'entreprise, un accompagnement régulier concernant le respect des procédures, organisée par le Délégué à la Protection des Données ou le cas échéant tout organisme compétent en la matière notamment la CNIL, l'agence nationale de la sécurité des systèmes d'information (ANSSI).

Le Responsable de la Protection des Données est en charge d'organiser les formations appropriées à l'ensemble des membres de la société.

Les salariés de la société Safebear sont formés aux risques et aux enjeux que représentent la collecte de données personnelles.

Présentation des formations

Les formations des membres de la société ont et auront pour vocation notamment :

- ✓ D'intégrer les obligations de l'employeur en matière de protection des données ;
- ✓ Décrypter les nouvelles références législatives et règlementaires ;
- ✓ Décrire le rôle de la CNIL ;
- ✓ Sécuriser les pratiques internes.

Le format de ces formations peut varier en fonction du type d'audience, le nombre de salariés à former et des objectifs de la formation et d'autres facteurs. Les derniers supports de formation sont partagés avec chaque nouvel arrivant.

Parmi les différents thèmes abordés au sein des formations, à la demande du Responsable de traitement ou le cas échéant d'un ou plusieurs salariés, peuvent porter notamment sur :

a. La réglementation de protection des données personnelles :

- Renforcement de la protection depuis le règlement européen de décembre 2015
- Réforme de la loi informatique et libertés
- Les délais de mises en conformité
- Les principes applicables aux traitements des données des salariés
- Quizz sur le RGPD

b. La maitrise des obligations des organes de direction

- Les conditions d'utilisation des informations personnelles : quelles informations peuvent être collectées ?
- Utilisation et exploitation des données dans le cadre de la gestion du personnel :
  - Gestion RH : évaluation, mobilité, recrutement... ;
  - Dispositifs de vidéosurveillance, badgeuses, vote électronique ;
  - Coordonnées des dirigeants, rémunérations, informations sur l'état de santé des salariés ;
  - Biométrie ;
- Règles d'utilisation et de conservation des données ;
- Types de traitement interdits ;
- Comprendre les droits des personnes, des salariés ;
- Quelles obligations en cas de modification et/ou d'enrichissement des informations, fichiers et traitements? ;
- Transferts de données personnelles hors Union européenne ;
- Quid du droit à l'oubli ? ;
- Les autres obligations de l'employeur en sa qualité de responsable de traitement, telles qu'issues notamment du règlement européen de décembre 2015 (accountability, privacy by design, etc.) ;
- Mini cas pratiques à résoudre en sous-groupe sur les obligations de l'employeur.

c. La CNIL : présentation et fonctions de régulateur du RGPD

- L'évolution du rôle de la CNIL et ses nouveaux pouvoirs ;
- Les contrôles de la CNIL ;
- Sanctions : que risque l'entreprise en cas de mauvaise utilisation de ces données numériques ? ;
- Les pouvoirs des agents et experts de la CNIL ;
- Vos recours auprès de la CNIL ;
- Atelier pratique : établir un formulaire de déclaration de demande d'autorisation auprès de la CNIL.

d. Les services RH face à la conformité RGPD

- Tendance à la dématérialisation des documents RH ;
- Vérification du traitement des données RH ;
- Comment s'assurer des bonnes déclarations à la CNIL ?
- Faire un état des lieux de la conformité
- Quid du collaborateur sur le départ ?
  - effacement des données de messagerie ;
  - droit à la portabilité des documents (bulletin de paie, évaluation, formation...) ;
- Comment gérer le transfert des données personnelles au niveau d'un groupe International ?
  - les précautions à prendre ;
  - transfert des données dans l'Union Européenne et hors UE ;
- Exercice pratique: audit de son propre service au niveau de la conformité sur ces différents aspects.

PCS AVOCAT
Droit des affaires & Nouvelles Technologies

Section 4. Contrôle des procédures

Procédures internes

Safebear dispose d'un contrôle permanent et périodique permettant de s'assurer que les dispositions de la présente procédure (ci-après la « Procédure ») sont respectées et conformes au cadre réglementaire applicable :

- Le Délégué à la Protection des données assure notamment :
  - Le respect des droits des utilisateurs notamment leurs demandes d'accès, rectification ou suppression de données dans les conditions prévues par les textes ;
  - La veille juridique de l'évolution des textes et/ou de la jurisprudence en matière de données personnelles et l'intègre aux processus de la Société ;
  - Conseille et participe à l'ensemble des activités de prévention, formation et préparation de la Société et ses membres quant aux problématiques liées aux données personnelles ;
  - Met à jour l'ensemble de la documentation liée à l'activité de collecte et traitement de données personnelles réalisées par la Société.
- Le Responsable de Traitement assure la coordination de l'ensemble des Référents notamment entre Délégué à la protection des données et le Responsable technique ;
- Des réunions périodiques sont mises en place entre les différents Référents pour évoquer l'ensemble des sujets liées au données personnelles, les actions mises en place et problématiques nécessitant leur avis ou aval.

Responsabilité & conformité de la Procédure

Conformément aux dispositions réglementaires, Safebear est seule responsable de la conformité avec la Procédure, ses obligations légales et le traitement approprié des Données Personnelles. La conformité avec les exigences de la Procédure est obligatoire pour tous les employés de la Société impliqués dans toute collecte ou traitement de données personnelles.

En cas de doute ou d'interrogation quant à une éventuelle contradiction des obligations énoncées dans cette Procédure de Protection des Données avec le cadre réglementaire imposé, le Responsable de Traitement et le Délégué à la Protection des Données doivent en être informés sans délai.

Si opportun, tout membre de la société peut proposer des règles qui, soit, complètent la procédure, soit, s'en différencient. Ces règles devront être approuvées par le Responsable de traitement et les différents Référents associés.

Contrôle & surveillance

La Société garantit à ses salariés que le fait de se conformer aux obligations de cette procédure, ou le fait d'alerter sur d'éventuelles violations déjà survenues ou à venir, ne portera aucun préjudice à l'employé concerné. Toutefois, la Société n'acceptera aucune action de ses employés qui pourrait être contraire à cette procédure.

La Société part du principe et attend de ses salariés qu'ils remontent tous les cas de violation avérés ou potentiels par tout moyen. Les détails de ces guidelines sont accessibles publiquement et disponibles sur le site de la Société.

La Société se réserve le droit de vérifier à intervalle régulier les connaissances de ses salariés sur la Protection des Données Personnelles, de réaliser des audits, d'appliquer cette Procédure et de faire une analyse de son efficacité.

Confidentialité & secret professionnel

Sous réserve de dispositions légales ou contractuelles spécifiques, les données personnelles collectées dans le cadre des activités de la Société sont couvertes par une obligation générale de confidentialité, applicable à l'ensemble des effectifs de la Société ainsi que ses partenaires, sous-traitants, clients, etc.

Toutefois, sous certaines conditions, il est permis de partager les Données Personnelles sans en avertir la personne concernée et/ou sans demander son consentement. Cela est le cas lorsque la diffusion des Données Personnelles est nécessaire dans les buts suivants :

- Prévention ou détection d'un crime ;
- L'appréhension ou persécution des délinquants ;
- L'évaluation ou la collection des taxes ou des droits dédouane ;
- Par l'ordre d'un tribunal ou tout article de loi.

Si n'importe quel membre de la Société traite les données personnelles dans l'un de ces buts, il peut contourner les obligations de confidentialité, mais uniquement en cas de préjudice présupposé. Si l'un des membres de la Société reçoit une demande de la part d'un tribunal ou de toute autre autorité en lien avec la législation pour transmettre une information relative à une personne concernée, l'entité doit immédiatement notifier le Délégué à la Protection des Données qui fournira des conseils et une assistance adaptée.

Révision & réclamations

La Procédure est annuellement mise à jour avec l'ensemble des acteurs participant à la conformité de la Société en matière de données personnelles notamment le Délégué à la Protection des Données, le responsable techniques, assistants désignés ainsi que l'ensemble des membres de la société, ses partenaires et sous-traitants.

Toute modification de la réglementation en la matière ou amendement jugé nécessaire sera immédiatement notifié à la Société qui en implémente les modifications.

Toute question ou interrogation concernant cette Procédure et ses annexes peut être envoyée au Responsable de traitement, aux interlocuteurs internes ou au Délégué à la Protection des données.

Les personnes concernées par une réclamation relative au traitement de leurs Données Personnelles doivent transmettre leur demande par écrit au Délégué à la Protection des Données. Chaque enquête sur les réclamations sera effectuée de façon appropriée au cas spécifique. Le Délégué à la Protection des Données et/ou le Responsable de Traitement informera la personne concernée sur les suites données à la réclamation dans un délai de temps raisonnable.

Si le problème ne peut être résolu par une consultation entre la personne concernée et le Responsable de la Protection des Données, la personne concernée peut, au choix, avoir recours à un médiateur, à un processus d'arbitrage exécutoire, à un contentieux ou à une réclamation déposée auprès de l'autorité de la Protection des Données en charge dans la juridiction concernée.

Contrôles externes

En cas de contrôle d'une autorité compétente et habilitée notamment la CNIL ou l'AMF, Safebear ainsi que ses référents assistent les agents chargés d'effectuer tout audit et mettent à leur disposition l'ensemble des éléments techniques, juridiques afin de leur permettre de réaliser leur mission.

Etudes d'impact & Privacy by Design

Afin de garantir que toutes les exigences de la Protection des Données sont automatiquement identifiées et adressées lorsque de nouveaux systèmes ou de nouvelles procédures sont mises en place, ou lorsque les systèmes ou procédures existants sont revus ou élargis, la Société s'assure qu'une évaluation de l'impact de la Protection des données est effectuée pour tous les nouveaux systèmes ou nouvelles procédures pour lesquels il a la responsabilité par le biais d'Analyses d'Impact.

Celles-ci sont réalisées en coopération avec le Responsable de traitements, les interlocuteurs privilégiés, le Responsable Technique et le Délégué à la Protection des données afin d'évaluer l'impact de toute nouvelle technologie utilisée sur la sécurité des Données Personnelles.

Les réflexions préventives à tout nouvelle activité susceptible d'impacter des données personnelles sont réalisées dans le logique portée par les privacy by design et privacy by default - obligation de maximiser la protection des données - effectuées par le délégué à la protection des données avec l'aide du responsable de traitements et des effectifs de la société associées à la conception du projet.

Points d'attention

Transfert de données hors UE

Les données personnelles collectées sont conservées au sein de l'Union européenne. Toutefois, dans le cas où Safebear serait amené à transférer ces données à des sous-traitants ou entités hors de l'Union, la Société s'assure que le traitement soit encadré par les clauses contractuelles types de la Commission européenne qui permettent de garantir un niveau de protection suffisant de la vie privée et des droits fondamentaux des personnes.

Afin de compenser un éventuel manque de Protection des Données, le transfert de Données Personnelles à des tiers est sujet à des mesures de sécurité complémentaires.

En de telles circonstances, la pertinence du transfert et son niveau de protection associé sera évalué notamment sur la base des critères d'équivalences légales analysées par la CNIL et fréquemment mis à jour sur leur site internet. Une vigilance particulière est attachée aux pays ne proposant à ce jour pas d'informations suffisantes en matière d'encadrement de collecte et traitement de données personnelles.

Un complément d'informations est disponible dans les ressources du site de la CNIL.

Avant tout transfert de données à un tiers, la Société fait une enquête en bonne et due forme en appliquant la procédure et vérifie si le tiers se conforme aux règles applicables.

Cybersécurité & attaques informatiques

Conformément aux exigences réhaussées par le RGPD en matière de sécurisation des données personnelles, et dans un contexte marqué par l'augmentation des attaques informatiques à l'encontre des sociétés par une variété de processus (Attaque Ddos, rançongiciels, hameçonnage, etc.), Safebear a mis en place des procédures techniques et organisationnelles pour sécuriser ses serveurs dont les données personnelles collectées :

- Tenue un registre des violations de données ;
- Analyses d'impact et audit auprès de professionnels de cybersécurité ;
- Notifier et échanges avec la CNIL et les autres autorités pertinentes en cas de cyberattaque découverte ;
- Information des entités et personnes victimes d'une violation de données.

Annexes

Annexe 1. Référence documentaire

Annexe 2. Registre des données personnelles

Annexe 3. Planning de conservation

Annexe 4. Références règlementaires

Annexe 1. Référence documentaire

1.A. Feuille de route – Safebear

I. Délégué à la protection des données

Présentation organisme, DPO, relais & historique des anciens CIL, DPO
Déclaration de DPO - CNIL
Copie des Missions / Contrat de prestation / Convention d'honoraires /

II. Registre des traitements

III. Aspects contractuels

Politique d'éthique du choix des fournisseurs et partenaires (sous-traitants)
Liste exhaustive des sous-traitants RGPD, localisation et périmètre d'activité
Procédure sur le transfert des données personnelles hors UE
Convention intragroupe, BCR
Contrats sous-traitants / avenants RGPD
Contrat de travail des salariés (RH, DSI, marketing, etc.) traitant les données (clause sur obligation de confidentialité spécifique)

IV. Contrôle et audit de l'efficacité des mesures déployées

Politique d'audit interne (périodicité, périmètre contrôlé, plan d'audit, tests sur échantillons aléatoires)
Politique d'audit des sous-traitants (périodicité, périmètre contrôlé, plan d'audit)
Comptes rendus des audits internes et indépendants effectués
Plans d'actions de régularisation
Traçabilité des modifications et mises à jour apportées au dossier d'accountability
Rapport annuel du DPO

V. Sécurité, intégrité et confidentialité

Politique de Sécurité des Systèmes d'Informations (PSSI)
Procédure sur les durées de conservation des données, l'archivage et la suppression
Procédure sur la gestion et la notification des violations de données (data breach)
Procédure sur la gestion et la conduite des analyses d'impact
Procédure d'anonymisation/de pseudonymisation des données
Procédure sur la gestion des projets impliquant les principes de privacy by design/ by default
Codes de conduite par métier sur les conditions de traitement des données personnelles (DSI, RH, marketing, innovation)
Charte informatique
Règlement intérieur
Rapports des tests d'intrusion et plans d'actions de régularisation
Rapports des analyses d'impact effectuées sur les traitements à risque
Traçabilité des data breach et conditions de traitement des incidents rencontrés
PCA - PRA
Support de sensibilisation/formation RGPD des salariés, feuilles de présence et thèmes abordés
Certification ISO
Code d'éthique sur les principes fondamentaux appliqués par l'organisme

VI. Transparence et information des personnes

Procédure sur la gestion des demandes de droits d'accès RGPD par les salariés (suppression, opposition, portabilité, etc.)
Procédure sur la gestion des demandes de droits d'accès RGPD par les clients
Politique de confidentialité

A. Interne destinée aux salariés de l'organisme
B. Externe destinée aux candidats au recrutement
C. Externe destinée aux clients de l'organisme
D. Externe destinée aux partenaires/fournisseurs
E. Site web et gestion des cookies

Formulaires de consentement
Modalités de gestion des preuves des recueils de consentements (traçabilité)
Formulaires types permettant l'exercice des droits RGPD par les salariés et clients

VII. Formalités CNIL - Déclarations de conformité, demandes d'autorisations et demandes d'avis