Charte de confidentialité – Recrutement Kärcher France

Objet de la Charte

La présente Charte de confidentialité (ci-après, « **la Charte** ») a pour objet de vous informer sur les traitements réalisés par Kärcher sur vos données à caractère personnel (ci-après les « **Données** »).

Elle concerne exclusivement les traitements réalisés par Kärcher à des fins de recrutement à l'égard de candidats au recrutement, quel que soit le poste auquel ils candidatent (CDD, CDI, intérim, apprentissage, stage, alternance, etc.).

Néanmoins, certains traitements peuvent varier en fonction de la nature du contrat qui vous lie avec Kärcher (à titre d'exemple, la procédure de recrutement diffère pour les salariés et les stagiaires) ou du moyen technique que vous avez utilisé pour candidater.

Pour tous les traitements réalisés à des fins de ressources humaines et de gestion du personnel, veuillez-vous référer à la Charte de confidentialité – Collaborateurs Kärcher France ou solliciter notre DPO par email à l'adresse : dpo@karcher.com.

Pour tous les traitements réalisés dans le cadre des activités commerciales de Kärcher sur les Données de ses clients, fournisseurs, prestataires ou de tiers non-salariés de Kärcher (ex : free-lances), veuillez-vous référer aux dispositions du contrat conclu entre Kärcher et votre entreprise ou solliciter notre DPO par email à l'adresse : dpo@karcher.com.

Ce document complète les informations relatives au traitement de vos Données sur le site Kärcher Careers, disponible via l'URL « https://careers.kaercher.com/go/FR/8953055/ », et les informations relatives au traitement de vos Données par les ressources humaines via le module SAP SuccessFactors Recrutement**, que vous trouverez à l'annexe 1 «** *Administration du module SAP SuccessFactors "Recruitment" (interface « Recrutement »)* ».

Responsables de traitement

Les traitements visés par la Charte (hors SuccessFactors) :	**Les traitements liés à la plateforme Kärcher Careers** :	**Les traitements liés aux modules SuccesFactors** :
Kärcher France SAS - 5 Avenue des Coquelicots, ZAC des Petits Carreaux, 94380 Bonneuil-sur-Marne, France.	**Alfred Kärcher SE & Co. KG** - Alfred-Kärcher-Straße 28 - 40, 71364 Winnenden, Allemagne	**Alfred Kärcher SE& Co. KG** - Alfred-Kärcher-Straße 28 - 40, 71364 Winnenden, Allemagne Directeur des Ressources Humaines : Ruediger BECHSTEIN

Directrice des Ressources Humaines : Noémie Grésanleux noemie.gresanleux@karcher.com Délégué à la Protection des Données : Aurélien Boucher dpo@karcher.com	Directeur des Ressources Humaines : Ruediger BECHSTEIN ruediger.bechstein@karcher.com Délégué à la Protection des Données : Michael Apperger michael.apperger@karcher.com **ET** **Kärcher France SAS -** 5 Avenue des Coquelicots, ZAC des Petits Carreaux, 94380 Bonneuil-sur-Marne, France. Directrice des Ressources Humaines : Noémie Grésanleux noemie.gresanleux@karcher.com Délégué à la Protection des Données : Aurélien Boucher dpo@karcher.com	ruediger.bechstein@karcher.com Délégué à la Protection des Données : Michael Apperger michael.apperger@karcher.com

Plan de la Charte

Table des matières

Annexe 1 : Administration du module SAP SuccessFactors "Recruitment" (interface « Recrutement »). 12

1. Catégories de données traitées, finalités des traitements et durées de conservation

Kärcher traite vos Données, notamment pour :

→ **Traiter votre candidature** : examiner votre candidature, le cas échéant organiser un ou plusieurs entretiens ;

→ **S'assurer de la conformité de la procédure de recrutement** : démontrer le respect de ses obligations légales en matière de recrutement, notamment de non-discrimination.

Les données personnelles nécessaires sont en principe collectées par Kärcher directement auprès de vous (CV, lettre de motivation).

Ces données peuvent, le cas échéant, être complétées par les données récoltées via le site Kärcher Careers, disponible via l'URL « https://careers.kaercher.com/go/FR/8953055/ », par celles récoltées via les réseaux sociaux (Facebook, Instagram, Xing, LinkedIn…) ou par celles obtenues auprès de tiers (ex : agence d'intérim, cabinet de recrutement, université, sites spécialisés dans la mise en relation entre candidats et entreprises, ou ancien employeur), être mises à jour au gré de la procédure de recrutement ou être supprimées lorsqu'elles ne sont plus nécessaires.

Le tableau ci-après fourni synthétise, en fonction de l'usage qui est fait de vos données personnelles, les finalités poursuivies par ces traitements, la base légale qui autorise Kärcher à les traiter et leurs durées de conservation ou la manière de déterminer ces durées. Lorsque plusieurs bases légales sont susceptibles de s'appliquer à une même catégorie de traitement, la base légale de la finalité principale est retenue.

Finalité(s) poursuivie(s)	Donnée(s) personnelle(s) traitée(s)	Base légale du traitement	Durée(s) de conservation des données personnelles
	Données d'identification : nom, prénom(s), second prénom, sexe, nationalité, pays, titre académique, photographie (si incluse dans le CV) ;		

Réception et gestion des candidatures sur le Kärcher Careers avec création de compte	**Données de contact** : coordonnées personnelles (courriel, téléphone principal et secondaire, adresse postale) ; **Données relatives au parcours scolaire, universitaire et/ou professionnel** : établissements d'enseignement fréquentés, diplômes obtenus, certifications obtenues, dates d'obtention, stages et emplois antérieurs (nom de l'employeur, poste et durée), etc. ; **Autres données relatives au candidat** : ensemble des postes sélectionnés par le candidat, motif(s) de la candidature (lettre de motivation), autres données du CV (langues maîtrisées, centres d'intérêt et loisirs, projets réalisés, mémoires et publications, titulaire du permis de conduire, statut de travailleur handicapé…), autres documents pertinents d'après le candidat, données bancaires si le candidat souhaite obtenir le remboursement de ses frais de déplacement.	Exécution d'une mesure précontractuelle prise à la demande du candidat (Art. 6§1 b) du RGPD).	**En l'absence d'entretien** : 2 mois **En cas d'entretien** : 2 mois
Réception et gestion des candidatures réalisées via Kärcher Careers sans création de compte (« *Postuler rapidement sans création de compte* »)	**Données d'identification** : nom, prénom, sexe, nationalité, photographie (si incluse dans le CV), pays, titre académique ; **Données de contact** : adresse courriel **Données relatives au parcours scolaire, universitaire et/ou professionnel** : établissements d'enseignement fréquentés, diplômes obtenus, certifications obtenues, dates d'obtention, stages et emplois antérieurs (nom de l'employeur, poste et durée), etc. ; **Autres données relatives au candidat** : poste auquel le candidat a postulé, motif(s) de la candidature (lettre de motivation), autres données du CV (langues maîtrisées, centres d'intérêt et loisirs,	Exécution d'une mesure précontractuelle prise à la demande du candidat (Art. 6§1 b) du RGPD).	**En l'absence d'entretien** : 2 mois **En cas d'entretien** : 2 mois

	projets réalisés, mémoires et publications, titulaire du permis de conduire, statut de travailleur handicapé…), autres documents pertinents d'après le candidat		
Réception et gestion des candidatures réalisées via les réseaux sociaux (LinkedIn…)	**Données d'identification** : nom, prénom(s). **Données de contact** : adresse email. **Autres données relatives au candidat** : données du CV, message personnalisé pour le recruteur, réseau social utilisé.	Exécution d'une mesure précontractuelle prise à la demande du candidat (Art. 6§1 b) du RGPD).	**En l'absence d'entretien** : 2 mois **En cas d'entretien** : 2 mois
Réception et gestion des candidatures réalisées via d'autres voies (candidature spontanée, agence d'intérim…)	**Données du CV, de la lettre de motivation (le cas échéant) et de la lettre de recommandation (le cas échéant), soit le plus souvent :** **Données d'identification** : nom, prénom(s), sexe, nationalité, photographie (si incluse dans le CV), titre académique. **Données de contact** : coordonnées personnelles (courriel, numéro de téléphone, adresse postale). **Données relatives au parcours scolaire, universitaire et/ou professionnel** : établissements d'enseignement fréquentés, diplômes obtenus, certifications obtenues, dates d'obtention, stages et emplois antérieurs (nom de l'employeur, poste et durée), etc. **Autres données relatives au candidat** : motif(s) de la candidature, langues maîtrisées, centres d'intérêt et loisirs, projets réalisés, mémoires et publications, titulaire du permis de conduire, statut de travailleur handicapé, etc.	Exécution d'une mesure précontractuelle prise à la demande du candidat (Art. 6§1 b) du RGPD).	**En l'absence d'entretien** : suppression immédiate **En cas d'entretien** : 2 mois
Organisation d'un ou de plusieurs entretien(s)	**Données d'identification** : nom, prénom(s).	Exécution d'une mesure précontractuelle prise à la	**En cas de recrutement** : La durée du contrat (présent dans le dossier salarié)

	Données de contact : coordonnées personnelles (courriel, téléphone). **Données relatives à l'entretien** : date, heure, lieu, aménagement particulier (cas des travailleurs handicapés), collaborateurs de Kärcher présents, notes d'entretien.	demande du candidat (Art. 6§1 b) du RGPD). Intérêt légitime de Kärcher (Art. 6§1 f) du RGPD), uniquement pour la conservation des données.	**En l'absence de recrutement** : 2 mois
Prise de décision finale concernant la candidature	**Données collectées au cours de la procédure de recrutement, complétées des :** **Données collectées lors de l'entretien** : impression d'ensemble et éléments objectifs d'évaluation renseignés par les responsables présents à l'entretien, conditions spécifiques posées par le candidat, etc. **Selon les cas, données obtenues auprès de tiers** (tels que cabinet de recrutement, établissement d'enseignement, sites spécialisés, ancien employeur ou maître de stage).	Exécution d'une mesure précontractuelle prise à la demande du candidat (Art. 6§1 b) du RGPD)	**En cas de recrutement** : 2 mois **En l'absence de recrutement** : 2 mois.
Gestion des contentieux (uniquement en l'absence de recrutement)	**Données collectées au cours de la procédure de recrutement, complétées des :** **Données relatives au contentieux** : dates de début et de fin du litige, objet et faits du litige, juridiction ou autorité administrative saisie et déroulement de la procédure, données comprises dans les documents et actes divers (constats, attestations, mises en demeure, PV, plainte, conclusions d'avocat…), données comprises dans les pièces exploitées à titre de preuve (notamment les données du processus de recrutement, les données relatives au parcours professionnel de la partie concernée, les données de connexion et données comprises dans les correspondances, les données bancaires, des données d'une sensibilité particulière telles que l'appartenance syndicale ou l'état de santé…).	Intérêt légitime de Kärcher (Art. 6§1 f) du RGPD) de se défendre dans l'hypothèse d'une réclamation ou d'une action en lien avec le processus de recrutement, en particulier fondée sur un motif de discrimination.	5 ans au plus à compter de la fin du processus de recrutement, sous forme d'archives intermédiaires.

	L'ensemble des données collectées lors du processus de recrutement ne sont pas systémiquement conservées.		

Aucun processus décisionnel automatisé concernant les personnes physiques et aucune activité de profilage ne seront effectués sur vos Données par Kärcher.

2. Destinataires

L'accès à vos données personnelles est strictement limité aux catégories de destinataires ou destinataires mentionnés dans le tableau ci-dessous.

Il est précisé que, dans l'exécution de leurs prestations, les tiers n'ont qu'un accès limité à vos données personnelles et ont l'obligation de les utiliser en conformité avec la législation applicable en matière de protection des données personnelles. Kärcher limite autant que possible l'étendue de vos données personnelles partagées avec eux.

	Catégories de destinataires ou destinataires
Au sein de Kärcher France SAS	Direction des Ressources Humaines, tout chef d'équipe responsable du poste pour lequel vous avez candidaté.
Autres sociétés du groupe Kärcher	La société Alfred Kärcher SE & Co. KG (co-responsable pour les traitements réalisés via Kärcher Careers).
Fournisseurs et prestataires de Kärcher	Agences d'intérim, cabinets/prestataires de recrutement, cabinets d'avocats (pour l'établissement du contrat), centres de formation.

3. Vos droits

Êtes-vous obligé(e) de mettre vos données à disposition de Kärcher ?

En tant que candidat(e) de Kärcher, vous devez fournir les données nécessaires pour permettre la gestion de votre candidature, pour remplir les obligations contractuelles associées, ainsi que fournir les données personnelles que Kärcher est tenue de traiter en vertu de la loi. Kärcher ne pourra réaliser de recrutement sans ces données.

Cette obligation ne s'applique pas aux traitements pour lesquels vous n'êtes pas obligé(e) de fournir des données personnelles.

De quels droits disposez-vous ?

Droit d'accès :	Vous avez le droit de demander à Kärcher quelles Données sont détenues vous concernant, de demander à ce que Kärcher vous les communique pour en vérifier le contenu, et de demander des informations complémentaires sur leur traitement.
Droit d'opposition :	Vous avez le droit de vous opposer à certains traitements de Données, en indiquant à Kärcher le ou les motif(s) impérieux motivant la demande d'exercice de votre droit d'opposition. Kärcher cessera alors de traiter ces Données, à moins que Kärcher ne démontre l'existence de raisons légitimes justifiant de procéder au traitement, raisons qui l'emporteraient sur vos intérêts, droits et libertés fondamentales, ou si un tel traitement est nécessaire pour l'établissement, l'exercice ou la défense d'un droit devant une juridiction.
Droit à l'effacement :	Vous avez le droit de demander à Kärcher d'effacer vos Données lorsque la base légale du traitement est l'intérêt légitime de Kärcher. Toutes vos Données seront effacées, à moins que l'intérêt en cause prévale sur vos droits ; dans ce cas, les Données seront effacées, à l'exception de celles étant strictement nécessaires à réaliser l'intérêt poursuivi. Lorsque le traitement repose sur l'exécution du contrat de travail ou du respect d'une obligation légale et/ou règlementaire, les Données seront effacées une fois la ou les finalité(s) poursuivie(s) achevée(s), conformément aux durées de conservation définies.
Droit de rectification :	Vous avez le droit de demander à Kärcher la rectification des Données inexactes ou incomplètes vous concernant.
Droit de limitation :	Vous avez le droit de demander à Kärcher de geler temporairement l'utilisation de certaines de vos Données, lorsque vous contestez l'exactitude des Données utilisées par Kärcher, que vous vous opposez à ce que vos Données soient traitées par Kärcher ou lorsque Kärcher s'apprête à les effacer alors que vous souhaitez qu'elle les conserve aux fins d'exercer un droit. Néanmoins, ce droit ne peut empêcher Kärcher d'utiliser vos Données dans le cadre d'une action en justice.
Droit à la portabilité :	Lorsque le traitement de vos Données est fondé sur votre consentement ou l'exécution d'un contrat, vous avez le droit de nous demander à récupérer les Données personnelles que vous avez fournies pour votre usage personnel ou pour les transmettre à un tiers de votre choix dans un format lisible et exploitable par une machine. Néanmoins, vous ne pouvez pas opposer ce droit lorsque Kärcher traite vos Données personnelles en exécution d'une obligation légale.
Droit de définir des directives :	Vous avez le droit de définir des directives relatives au sort de vos Données après votre décès.

Droit de saisir la CNIL :	Si vous considérez que vos Données ont été traitées en violation des dispositions du RGPD ou de la loi Informatique et Libertés, vous pouvez saisir la CNIL d'une plainte via le formulaire accessible à l'adresse https://cnil.fr ou par courrier adressé au 3 Place Fontenoy, TSA 80715 Paris, 75334 Paris cedex 07 (tel : 01 53 73 22 22).

Comment exercer vos droits ?

Vous pouvez exercer n'importe lequel de vos droits à tout moment, en adressant un courriel à l'adresse dpo@karcher.com.

Vous pouvez également contacter le Délégué à la protection des données de Kärcher à cette adresse pour toute question relative au traitement de vos Données par Kärcher ou à la présente Charte.

4. Nos engagements

Nous nous engageons à traiter vos Données dans le respect de la législation applicable, notamment le RGPD et la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (dite « Loi Informatique et Libertés »).

En application de ces textes, nous nous engageons à traiter vos Données :

- De manière licite, loyale et transparente ;
- Pour les seules finalités énumérées à la section 1 de la présente charte ;
- Uniquement dans la mesure de ce qui est nécessaire au regard des finalités énumérées à la section 1 ainsi qu'à l'annexe 1.
- En nous assurant qu'elles sont et demeurent exactes, et en apportant toute rectification nécessaire le cas échéant ;
- De manière sécurisée, en les protégeant contre tout traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle. Nous nous engageons à cette fin à mettre en place les mesures techniques ou organisationnelles appropriées.

Vos Données sont susceptibles d'être transférées vers tous les recruteurs du groupe Kärcher. Afin de garantir la conformité de ces transferts aux législations applicables, des accords sont conclus entre les entreprises du groupe et documentés. Quelle que soit la modalité de "visibilité du profil" choisie, le traitement sera conforme aux législations en vigueur. Ainsi, vous continuerez de bénéficier de l'ensemble des protections et garanties prévues par la présente Charte. Vos Données ne seront par ailleurs transmises à aucun tiers situé en-dehors de l'Union européenne.

5. Lexique

Base légale du traitement :	Un traitement n'est licite que s'il correspond à l'un des cas de figure de l'article 6 du RGPD. Ce cas de figure est appelé la « base légale » du traitement.
CNIL :	Acronyme désignant la Commission nationale de l'informatique et des libertés, autorité administrative chargée en France du contrôle de l'application des dispositions du RGPD et de la Loi Informatique et Libertés.
Donnée à caractère personnel (ou « donnée personnelle ») :	Constitue une donnée à caractère personnel toute information se rapportant à une personne physique permettant de l'identifier directement ou indirectement. Sont par exemple des données personnelles : un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, toute information sur l'individu d'ordre physique, physiologique, génétique, psychique, économique, culturelle ou social.
Durée de conservation :	Durée pendant laquelle une donnée est conservée par le responsable de traitement dans ses systèmes, tant en base active qu'en archivage. Une donnée peut être licitement conservée pendant toute la durée du traitement. Une fois le traitement terminé, les durées de conservation des données varient selon les finalités justifiant la conservation et les durées légales applicables.
Finalité du traitement :	La finalité d'un traitement est l'objectif poursuivi par le traitement des données personnelles.
Responsable de traitement :	Le responsable d'un traitement est la personne physique ou morale, ici Kärcher, qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.
RGPD :	Acronyme désignant 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.

Sous-traitant :	Toute personne qui réalise un traitement de données personnelles pour le compte et sur les instructions du responsable de traitement. Le sous-traitant doit se conformer strictement à ces instructions. La relation entre responsable de traitement et sous-traitant est formalisée par un contrat écrit.
Traitement :	Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel. Constituent des traitements de données personnelles : la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction des données.

Annexe 1 : Administration du module SAP SuccessFactors "Recruitment" (interface « Recrutement »).

I. Les étapes du traitement des données

Dans le module SAP SuccessFactors Recrutement, les profils des candidats du groupe Kärcher sont créés et gérés de manière centralisée par le service RH de la société Alfred Kärcher SE Co. KG, auprès de laquelle les candidats postulent. La société Alfred Kärcher SE Co. KG est l'organisme responsable de la protection des données au sens de l'article 4§7 du RGPD (plateforme des candidats).

La société susnommée collecte, stocke temporairement, présente, transmet et, enfin, supprime les données personnelles des demandeurs.

II. Objet et finalité du traitement

Le traitement des données personnelles concerné a pour objet le recrutement et le rejet des candidats, ainsi que la planification et l'organisation du travail du groupe d'entreprises Kärcher conformément à l'article 88§1 du RGPD.

Grâce au module de recrutement de SuccessFactors, un processus électronique global de gestion des candidatures (workflow) est mis en place. Ce module permet de créer une plateforme numérique pour la recherche de postes vacants chez Kärcher, ainsi que de standardiser les offres d'emploi et les processus de candidature au niveau mondial.

En outre, un pool international commun de candidats est fourni aux services chargés de la protection des données, de sorte qu'après que les candidats aient donné leur consentement au traitement des données, un processus de candidature global peut être défini et respecté par les services.

III. Données collectées

Les champs de données sont les suivants :

Utilisateur actif, ID de l'utilisateur, prénom, nom, second prénom, suffixe, alias/nom, code d'emploi, sexe, adresse électronique, ID du site, lieu, fuseau horaire, date de la demande, titre, numéro de téléphone, adresse, ville, pays (fédéral), code postal, pays, ID du centre de coûts, désignation, code de la société, code de la devise, code de la langue, numéro de téléphone mobile du demandeur.

IV. Responsabilités

Le traitement (voir les phases du traitement au point I.) des données personnelles des candidats dans le module SAP SF Recrutement relève de la responsabilité de l'organisme collecteur respectif conformément à l'article 4§7 du RGPD.

La gestion et le traitement des données des candidats peuvent être effectués par une autre entreprise du groupe Kärcher uniquement dès lors (i) qu'un accord a été conclu à cet égard ; (ii) que l'administration et le traitement de ces données sont documentés. Seuls les collaborateurs investis d'une autorisation spécifique (annexe 2 du GBV SAP SF Recruiting 11/2018), devant être renseignée, disposent du droit d'accès aux données mentionnées.

Alfred Kärcher SE & Co. KG traite ces données de candidature afin de mettre à la disposition du groupe Kärcher un pool national et international de candidats. À cette fin, des processus et des normes sont établis au sein du groupe Kärcher. Ces derniers sont régulièrement révisés ou adaptés.

V. Ressources informatiques exploitées

SuccessFactors est fourni par SAP Deutschland SE & Co. KG, Hasso-Plattner-Ring 7, 69190 Walldorf. SAP Deutschland SE & Co KG agit en tant que sous-traitant conformément à l'article 28 du RGPD.

VI. Mesures techniques et organisationnelles (TOM)

https://www.sap.com/about/trust-center/agreements/cloud/cloud-services.html?sort=latest_desc&search=Technical+Organizational+Measures

Mesures techniques et organisationnelles (TOM) pour SAP Cloud Services

Les sections suivantes définissent les mesures techniques et organisationnelles actuelles de SAP et sont intégrées dans l'annexe 2 du DPA. SAP peut les modifier à tout moment sans préavis, à condition de maintenir un niveau de sécurité équivalent ou supérieur. Les mesures individuelles peuvent être remplacées par de nouvelles mesures qui poursuivent la même finalité, à condition de ne pas diminuer le niveau de sécurité protégeant les données personnelles.

1. CONTRÔLE D'ACCÈS PHYSIQUE

Les personnes non autorisées ne peuvent accéder physiquement aux locaux, bâtiments ou pièces où se trouvent les systèmes de traitement des données qui traitent des données personnelles.

1.1. Mesures :
1.1.1. SAP protège les informations en sa possession et ses installations en utilisant les moyens appropriés, conformément à la politique de sécurité de SAP.
1.1.2. En général, les bâtiments sont sécurisés par des systèmes de contrôle d'accès (par exemple, un système d'accès par carte à puce).
1.1.3. Au minimum, les points d'entrée les plus extérieurs du bâtiment doivent être équipés d'un système de clé certifié comprenant une gestion moderne et active des clés.
1.1.4. En fonction de la classification de sécurité, les bâtiments et zones individuelles et les locaux environnants peuvent être protégés par des mesures supplémentaires. Celles-ci comprennent des profils d'accès spécifiques, la vidéosurveillance, des systèmes d'alarme anti-intrusion et des systèmes de contrôle d'accès biométriques.
1.1.5. Les droits d'accès sont accordés aux personnes autorisées sur une base individuelle, conformément aux mesures de contrôle d'accès au Système et aux données (voir ci-dessous). Ceci s'applique également à l'accès des visiteurs. Les invités et les visiteurs des bâtiments SAP doivent s'inscrire à la réception et être accompagnés par des personnes autorisées par SAP.
1.1.6. Tout collaborateur de SAP, comme tout personnel externe présent sur un des sites de SAP devra se prémunir d'une carte d'identité valide.
1.2. Mesures supplémentaires pour les centres de données :

1.2.1. Tous les centres de données adhèrent à des procédures de sécurité strictes appliquées par des vigiles, utilisent des caméras de surveillance, des détecteurs de mouvement, des mécanismes de contrôle d'accès et d'autres mesures visant à empêcher que les équipements et les installations des centres de données ne soient compromis. Seuls les représentants autorisés ont accès aux systèmes et aux infrastructures dans les centres de données. Afin d'en préserver le bon fonctionnement, les équipements de sécurité physique (par exemple, les détecteurs de mouvement, les caméras, etc.) font l'objet d'une maintenance régulière.

1.2.2. Tout personnel (SAP ou externe) assurant la sécurité des centres de données SAP doit procéder à l'enregistrement du nom et de l'heure d'entrée du personnel autorisé accédant aux zones restreintes des centres de données.

2. CONTRÔLE D'ACCÈS AU SYSTÈME

Les systèmes de traitement des données utilisés pour fournir le service en nuage doivent être sécurisés de sorte qu'ils ne soient pas utilisés sans autorisation. A cette fin, les mesures suivantes ont été prises :

2.1. Plusieurs niveaux d'autorisation sont utilisés pour accorder l'accès aux systèmes sensibles, y compris ceux qui stockent et traitent les données personnelles. Les autorisations sont gérées via des processus définis conformément à la politique de sécurité de SAP.

2.2. L'ensemble du personnel accède aux systèmes de SAP à l'aide d'un identifiant unique (ID utilisateur).

2.3. SAP a mis en place des procédures afin que les changements d'autorisation demandés ne soient mis en œuvre que conformément à la politique de sécurité SAP (par exemple, aucun droit n'est accordé sans autorisation). Si le personnel quitte l'entreprise, ses droits d'accès sont révoqués.

2.4. SAP a mis en place une politique de confidentialité impliquant l'interdiction de tout partage de mot de passe. Cette politique régit aussi les réponses à une éventuelle divulgation des mots de passe et exige ainsi que ces derniers soient (i) immédiatement modifiés lors de l'obtention du mot de passe par défaut ; (ii) régulièrement modifiés durant l'exercice des fonctions. Des identifiants uniques et personnalisés sont attribués pour l'authentification. Tous les mots de passe doivent répondre à des exigences minimales définies et sont stockés sous forme cryptée. Dans le cas des mots de passe de domaine, le système impose un changement de mot de passe tous les six mois, conformément aux exigences relatives aux mots de passe complexes. Chaque ordinateur nécessite aussi un déverrouillage par mot de passe.

2.5. Le réseau de l'entreprise est protégé du réseau public par des pare-feu.

2.6. SAP utilise un logiciel antivirus à jour, installé sur tous les points d'accès au réseau de l'entreprise (pour les comptes de messagerie), ainsi que sur tous les serveurs de fichiers et toutes les stations de travail.

2.7. La gestion des correctifs de sécurité est mise en œuvre pour assurer le déploiement régulier et périodique des mises à jour de sécurité pertinentes. L'accès à distance au réseau d'entreprise et à l'infrastructure critique de SAP est protégé par une authentification forte.

3. CONTRÔLE DE L'ACCÈS AUX DONNÉES

Les personnes autorisées à utiliser les systèmes de traitement des données n'ont accès qu'aux données personnelles auxquelles elles ont le droit d'accéder. Les données personnelles ne doivent pas être lues, copiées, modifiées ou supprimées sans autorisation au cours de la collecte, de l'utilisation et du stockage. SAP prend les mesures suivantes :

3.1. Dans le cadre de la politique de sécurité de SAP, un niveau de protection au minimum équivalent à celui appliqué aux informations « confidentielles » selon la norme de classification des informations SAP est appliqué aux données personnelles.

3.2. L'accès aux données personnelles est accordé en fonction de la nécessité d'avoir accès à de telles données. Le personnel dispose d'un accès limité aux seules informations dont il a besoin pour remplir sa mission. SAP utilise des systèmes d'autorisation qui documentent les processus d'octroi des autorisations et les accès attribués à chaque compte (ID utilisateur). Toutes les données des clients sont protégées conformément à la politique de sécurité de SAP.
3.3. Tous les serveurs de production sont exploités dans les centres de données ou dans des salles de serveurs sécurisées. Les mesures de sécurité qui protègent les applications traitant des données personnelles sont régulièrement vérifiées. À cette fin, SAP effectue des contrôles de sécurité internes et externes et des tests de pénétration sur ses systèmes informatiques.
3.4. SAP n'autorise pas l'installation de logiciels dès lors qu'ils n'ont pas été approuvés par SAP.
3.5. Une norme de sécurité SAP régit la manière dont les données et les supports de données sont supprimés ou détruits lorsqu'ils ne sont plus nécessaires.

4. CONTRÔLE DE LA TRANSMISSION DES DONNÉES

A moins que cela soit nécessaire pour la fourniture des Services de Cloud Computing conformément à l'Accord, les données personnelles ne doivent pas être lues, copiées, modifiées ou supprimées sans autorisation pendant le transfert. Lorsque les supports de données sont transportés physiquement, des mesures adéquates sont mises en œuvre chez SAP pour garantir le niveau de sécurité convenu (par exemple, le cryptage et les conteneurs plombés). SAP prend les mesures suivantes :

4.1. Les données personnelles transférées sur les réseaux internes de SAP sont protégées conformément à la politique de sécurité de SAP.
4.2. Lorsque des données sont transférées entre SAP et ses clients, les mesures de protection des données personnelles transférées font l'objet d'un accord mutuel et sont intégrées au contrat correspondant. Cela s'applique aussi bien au transfert de données physiques qu'au transfert de données sur réseau. Dans tous les cas, le client assume la responsabilité de tout transfert de données dès lors qu'il se trouve en dehors des systèmes contrôlés par SAP (par exemple, des données transmises en dehors du pare-feu du centre de données SAP).

5. CONTRÔLE DE L'ENTRÉE DES DONNÉES

Il sera possible d'examiner rétrospectivement et d'établir si et par qui les données personnelles ont été collectées, modifiées ou supprimées des systèmes de traitement des données de SAP. SAP prend la mesure suivante : SAP ne permet aux personnes autorisées d'accéder aux données personnelles que dans le cadre de leurs fonctions.

SAP a mis en place un système de journalisation pour l'entrée, la modification, la suppression ou le blocage des données personnelles par SAP ou ses Sous-Traitants au sein du Service Cloud, dans la mesure où cela est techniquement possible.

6. CONTRÔLE DU TRAVAIL

Les données personnelles traitées sur commission (c'est-à-dire les données personnelles traitées pour le compte d'un client) sont traitées uniquement conformément à l'Accord et aux instructions connexes du client. SAP prend les mesures suivantes :

6.1. SAP met en place et applique des contrôles et des processus pour surveiller le respect des contrats entre elle-même et ses clients, sous-traitants ou autres fournisseurs de service.
6.2. Dans le cadre de la politique de sécurité de SAP, est au minimum appliqué aux données personnelles un niveau de protection équivalent à celui appliqué aux informations « confidentielles » selon la norme de classification des informations SAP.

6.3. Tous les collaborateurs de SAP et les sous-traitants ou autres prestataires de services sont contractuellement tenus de respecter la confidentialité de toutes les informations sensibles, y compris les secrets commerciaux des clients et partenaires de SAP.

7. CONTROLE DE DISPONIBILITE DES DONNEES

Les données personnelles sont protégées contre toute destruction, perte accidentelle ou accès non autorisé. SAP utilise des processus de sauvegarde réguliers pour permettre la restauration des systèmes essentiels à l'activité. SAP prend les mesures suivantes :

7.1. SAP utilise des systèmes d'alimentation sans interruption (par exemple : UPS, batteries, générateurs, etc.) pour protéger la disponibilité de l'énergie dans les centres de données.
7.2. Des plans d'urgences ont été élaborés par SAP en cas d'urgence critique – comme la survenance d'un risque élevé – englobant notamment des mesures et stratégies permettant la reprise de l'activité. Ces procédures sont exposées dans les documents pertinents et dans le formulaire de commande du service en nuage concerné.
7.3. Les plans et processus d'urgence sont régulièrement testé par SAP afin de vérifier qu'ils fonctionnent bien.

8. CONTROLE DU CLOISONNEMENT DES DONNEES

Les données personnelles collectées pour différentes finalités sont cloisonnées et traitées séparément. En ce sens, SAP met en œuvre les mesures suivantes :

8.1. SAP utilise les capacités techniques du logiciel déployé (par exemple : multi-location, ou paysages système distincts) pour réaliser la séparation des données entre les données personnelles provenant de plusieurs clients.
8.2. Le client (y compris ses contrôleurs) n'a accès qu'à ses propres données.
8.3. Si des données personnelles sont nécessaires pour traiter une demande d'assistance du client, les données sont affectées à cette unique demande et utilisées uniquement pour traiter ladite demande ; elles ne sont pas accessibles pour traiter d'autres demandes. Ces données sont stockées dans des systèmes d'assistance dédiés.

9. CONTRÔLE DE L'INTÉGRITÉ DES DONNÉES

Les données personnelles resteront intègres, complètes et actuelles pendant les activités de traitement. SAP prend les mesures suivantes :

9.1. SAP a mis en place une stratégie de défense à plusieurs niveaux pour se protéger des modifications non autorisées.
9.2. En particulier, SAP utilise les éléments suivants pour mettre en œuvre les mesures de sécurité précédemment exposées :
9.2.1. Pare-feu ;
9.2.2. Centre de surveillance de la sécurité ;
9.2.3. Logiciel antivirus ;
9.2.4. Sauvegarde et récupération ;
9.2.5. Tests de pénétration externes et internes ;
9.2.6. Audits externes réguliers pour prouver les mesures de sécurité.

Dernière mise à jour : 10 avril 2024