

Accord sur le traitement des données à caractère personnel (ATD)

ClubDesk pour les associations de l'Espace économique européen (EEE) et pour les associations ayant leur siège en Suisse

(EEE : États membres de l'Union européenne ainsi que l'Islande, le Liechtenstein et la Norvège)

entre

association mandante

– en tant que responsable, ci-après dénommé « client » –

et la société

reeweb ag (développeur de ClubDesk)

Picassoplatz 8

4052 Bâle

Suisse

– en tant que sous-traitant, ci-après dénommé « reeweb » –

1. Objet et durée du contrat, application de la loi sur la protection des données d'

1.1. Objet du mandat

L'objet du mandat est la mise à disposition du logiciel ClubDesk pour la gestion des données associatives en tant que service via Internet (Software-as-a-Service) conformément au contrat conclu en ligne entre le client et reeweb conformément aux conditions générales de vente.

La gestion du contenu des données de l'association et la responsabilité de la licéité du traitement des données, c'est-à-dire la demande de savoir si certaines données (par exemple les coordonnées des membres) peuvent être traitées, incombent au client ou à la personne habilitée à le représenter. Les personnes habilitées à représenter une association sont les membres actuels du comité directeur, la « personne de contact » définie dans ClubDesk et les administrateurs de l'association. Dans le cadre des accords conclus, reeweb traite uniquement les données saisies par le client pour le compte de celui-ci et selon ses instructions.

Le présent accord régit les droits et obligations du client et de reeweb dans le cadre du traitement des données à caractère personnel pour le compte du client. Les dispositions s'appliquent à toutes les activités liées au contrat et dans le cadre desquelles reeweb et ses employés ou les mandataires de reeweb entrent en contact avec des données à caractère personnel provenant du client ou collectées pour le compte du client.

1.2. Durée du contrat

La durée de cette commande (durée d'exécution) dépend de la durée du contrat principal. En cas de doute, la résiliation du contrat principal vaut également résiliation du présent contrat et la résiliation du présent contrat vaut résiliation du contrat principal.

En cas d'infractions simples, c'est-à-dire ni intentionnelles ni par négligence grave, le client fixe d'abord à reeweb un délai raisonnable dans lequel reeweb peut remédier à l'infraction. Le droit à une résiliation extraordinaire du présent contrat pour motif grave reste inchangé.

1.3. Application du RGPD

Le règlement général sur la protection des données (ci-après dénommé « RGPD ») s'applique aux clients qui sont des associations ayant leur siège dans l'Espace économique européen (EEE) ou aux associations dont les membres sont issus de l'EEE. Dans les autres cas, c'est la législation applicable en matière de protection des données qui s'applique au client. La société reeweb, dont le siège est en Suisse, respecte les dispositions applicables en matière de protection des données.

1.4. Lieu du traitement des données

Le traitement des données par reeweb a lieu en Suisse. Dans sa décision du 26 juillet 2000, la Commission européenne a constaté que la Suisse offrait un niveau adéquat de protection des données.

Le transfert du traitement et du stockage des données vers un État membre de l'Union européenne, vers un autre État signataire de l'accord sur l'Espace économique européen par reeweb, ainsi que vers un pays ayant fait l'objet d'une décision d'adéquation, est autorisé. La transmission éventuelle à des sous-traitants dans des pays ne disposant pas d'un niveau adéquat de protection des données est garantie par la conclusion de clauses contractuelles types de l'UE (Module 3). Si, à l'avenir, reeweb devait également transmettre des données à l' e sur la base d'autres mécanismes de transfert légalement autorisés, elle en informerait préalablement la cliente.

2. Concrétisation du contenu de la commande

2.1. Étendue, nature et finalité du traitement prévu des données

Le traitement des données sert à la gestion d'associations ou de groupes comme convenu dans le contrat. Cela peut inclure, par exemple, la gestion des membres, des personnes intéressées, des participants à des événements, des fournisseurs et des rendez-vous. L'étendue, la nature et la finalité du traitement des données à caractère personnel par reeweb pour le client sont décrites plus en détail dans la déclaration de confidentialité.

2.2. Nature et catégories des données à caractère personnel

L'objet de la collecte, du traitement ou de l'utilisation est constitué de tous types/catégories de données, en fonction de la manière dont les fonctionnalités flexibles de ClubDesk sont configurées et utilisées par l'association/le groupe conformément au contrat principal. Les catégories de données suivantes sont notamment prises en compte :

- Données de base des personnes concernées, notamment des membres de l'association, parmi lesquelles
 - adresse et numéro de téléphone
 - adresse e-mail
 - Coordonnées bancaires
- Données comptables (telles que le solde du compte de cotisations, le solde des comptes débiteurs/crédeurs et des comptes salaires)
- Données relatives aux qualifications (telles que la participation à des événements et à des compétitions et les résultats obtenus, la formation continue des employés)

2.3. Groupe et catégories de personnes concernées

Le cercle ou les catégories de personnes concernées par ce traitement des données comprennent toutes les personnes, en fonction de la manière dont les fonctionnalités flexibles de ClubDesk sont configurées et utilisées par l'association/le groupe conformément au contrat principal. Les catégories de personnes suivantes sont notamment concernées :

- Membres de l'association/du groupe
- Personnes intéressées et invités
- Sponsors et mécènes
- Participants à des événements
- Collaborateurs
- Fournisseurs/prestataires de services

3. Description des mesures techniques et organisationnelles à prendre en matière de protection et de sécurité des données

(1) Les mesures techniques et organisationnelles nécessaires à la protection adéquate des données du client sont décrites dans l'annexe de reeweb. Si le client les accepte, les mesures documentées constituent la base de la commande. Si un contrôle du client révèle un besoin d'ajustement, celui-ci doit être mis en œuvre d'un commun accord.

(2) reeweb doit assurer la sécurité du traitement des données conformément à l'annexe du présent accord. Dans l'ensemble, les mesures à prendre sont des mesures de sécurité des données et d' visant à garantir un niveau de protection adapté au risque en termes de confidentialité, d'intégrité, de disponibilité et de résilience des systèmes, en tenant compte notamment du contrôle organisationnel, du contrôle d'accès, du contrôle des accès, contrôle des transmissions, contrôle des commandes, contrôle de la disponibilité et du principe de séparation. Il convient à cet égard de tenir compte de l'état de la technique, des coûts de mise en œuvre, de la nature, de l'étendue et des finalités du traitement, ainsi que de la probabilité et de la gravité variables du risque pour les droits et libertés des personnes physiques.

(3) Les mesures techniques et organisationnelles sont soumises au progrès technique et à l'évolution. À cet égard, reeweb est autorisé à mettre en œuvre des mesures alternatives adéquates. Le niveau de sécurité des mesures définies ne doit toutefois pas être inférieur. Les modifications importantes doivent être communiquées immédiatement au client par écrit.

4. Rectification, blocage et suppression des données ; Droits des personnes concernées et responsabilité

(1) reeweb n'est pas autorisé à rectifier, supprimer ou bloquer les données traitées dans le cadre de la commande de sa propre initiative, mais uniquement sur instruction documentée du client, ni à limiter leur traitement. reeweb est autorisé à bloquer l'accès du client à ClubDesk dans la mesure où cela est autorisé par les conditions générales de ClubDesk, par exemple en cas de retard de paiement ou de suspicion fondée d'utilisation abusive.

(2) Si une personne concernée (par exemple un membre d'une association) s'adresse directement à reeweb au sujet de ses droits en matière de protection des données, en particulier en matière d'information, de rectification, de suppression et de blocage conformément à la législation applicable en matière de protection des données, reeweb transmettra cette demande au client et/ou renverra la personne concernée vers le client, tout en informant ce dernier de la demande de la personne concernée. Reeweb ne prendra aucune décision quant à la légitimité des demandes des personnes concernées et ne répondra notamment à aucune demande d'accès de la part de ces dernières.

(3) reeweb aidera le client à satisfaire les demandes des personnes concernées dans la mesure de ses possibilités, dans la mesure où le client ne peut pas satisfaire ces demandes sans la coopération de reeweb. Reeweb peut exiger du client une rémunération supplémentaire raisonnable pour les frais occasionnés par cette coopération.

(4) Si une personne concernée s'adresse directement à reeweb en raison d'une violation présumée de la protection des données et obtient de celle-ci des dommages-intérêts, le client doit indemniser reeweb pour le préjudice subi, dans la mesure où reeweb n'aurait pas été responsable envers le client pour cette violation de la protection des données conformément aux dispositions du présent accord et du contrat principal, en particulier si elle s'est conformée à l'accord et aux instructions du client. Cela s'applique également en cas d'amende infligée à reeweb.

5. Contrôles et autres obligations de reeweb

Outre les dispositions du présent contrat, reeweb est tenu de respecter les dispositions légales en matière de protection des données en vigueur à son siège en Suisse. Cette combinaison de dispositions contractuelles et légales entraîne notamment les obligations suivantes pour reeweb :

1. Reeweb n'est pas tenu de nommer un délégué à la protection des données. Les demandes relatives à la protection des données peuvent être adressées à datenschutz@clubdesk.com.
2. Reeweb n'emploie pour l'exécution des travaux que des employés qui se sont engagés par écrit à respecter la confidentialité et qui ont été préalablement familiarisés avec les dispositions pertinentes en matière de protection des données ou qui sont soumis à une obligation légale de confidentialité. En outre, reeweb veillera au respect de cette obligation avec toute la diligence requise. Reeweb et toute personne subordonnée à reeweb ayant accès à des données à caractère personnel ne peuvent traiter ces données que conformément aux instructions du client, y compris les pouvoirs accordés dans le présent contrat, sauf si elles sont légalement tenues de les traiter. Dans ce cas, reeweb informe le client de ces exigences légales avant le traitement, à moins que la loi en question n'interdise une telle notification pour des raisons d'intérêt public important.
3. Reeweb contrôle régulièrement les mesures techniques et organisationnelles de sécurité des données afin de garantir que le traitement relevant de sa responsabilité est conforme aux exigences en matière de protection des données qui lui sont applicables pendant toute la durée du traitement des données du client.
4. Reeweb tient un registre de toutes les catégories d'activités de traitement effectuées pour le compte du client.

6. Sous-traitance

(1) Au sens de la présente réglementation, on entend par sous-traitance les services qui se rapportent directement à la fourniture de la prestation principale. Cela n'inclut pas les prestations accessoires auxquelles Reeweb a recours, par exemple les services de télécommunication, les services postaux/de transport, la maintenance et le service utilisateur ou l'élimination des supports de données, ainsi que d'autres mesures visant à garantir la confidentialité, la disponibilité, l'intégrité et la résilience du matériel et des logiciels des systèmes de traitement des données. Reeweb est toutefois tenu de prendre des mesures contractuelles et de contrôle appropriées et conformes à la loi afin de garantir la protection et la sécurité des données du client, même dans le cas de prestations accessoires externalisées.

(2) Le client accepte par la présente de manière générale le recours à des sous-traitants avec lesquels reeweb a conclu un accord conforme au présent accord. Vous trouverez une liste des prestataires de services actuels sur le site web de reeweb à l'adresse www.clubdesk.com/unterauftragnehmer.

(3) L'externalisation à des sous-traitants ou le changement de sous-traitant existant sont autorisés dans la mesure où :

- un accord contractuel avec le sous-traitant comparable au présent accord est conclu,
- reeweb informe le client par écrit ou sous forme de texte, dans un délai raisonnable (généralement deux (2) mois) avant la sous-traitance, en indiquant la date de transmission des données, et
- le client ne s'oppose pas par écrit ou sous forme de texte à l'externalisation prévue avant la date de transfert des données à reeweb.

Une objection du client est considérée comme une résiliation extraordinaire du contrat principal à la date précédant immédiatement le transfert. Après cette date, le client ne peut plus utiliser les services de reeweb. Avant le transfert au sous-traitant, les données du client sont supprimées par reeweb. Il

incombe au client d'effectuer lui-même une éventuelle sauvegarde des données dans ses propres systèmes avant cette date.

(4) La transmission des données personnelles du client au sous-traitant et la première intervention de ce dernier ne sont autorisées que lorsque toutes les conditions requises pour la sous-traitance sont réunies. Si un sous-traitant ne respecte pas ses obligations en matière de protection des données, reeweb est responsable envers le client du respect des obligations de ce sous-traitant.

(5) Si le sous-traitant fournit la prestation convenue en dehors de l'UE/de l'EEE/de la Suisse, reeweb garantit les conditions particulières pour un transfert vers un pays tiers par des mesures appropriées. Il en va de même si des prestataires de services doivent être utilisés pour des prestations accessoires au sens du paragraphe 1, phrase 2 ci-dessus en dehors de l'UE/de l'EEE/de la Suisse.

7. Droits de contrôle du client

(1) Reeweb veille à ce que le client puisse s'assurer du respect des obligations de reeweb en vertu du présent contrat. Reeweb s'engage à fournir au client, sur demande, les informations nécessaires et, en particulier, à prouver la mise en œuvre des mesures techniques et organisationnelles.

(2) Reeweb est en droit, à sa seule discrétion et dans le respect des obligations légales du client, de ne pas divulguer des informations sensibles pour les activités de reeweb ou dont la divulgation entraînerait une violation des dispositions légales ou contractuelles par reeweb. Le client n'est pas autorisé à accéder aux données ou informations concernant d'autres clients de reeweb, aux informations relatives aux coûts, ni à toutes autres données confidentielles de reeweb qui ne sont pas directement pertinentes pour les fins de contrôle convenues.

(3) Le client a le droit, en accord avec reeweb, d'effectuer des vérifications (contrôle des commandes) pendant les heures de bureau habituelles, à ses propres frais, sans perturber le fonctionnement de l'entreprise et dans le strict respect de la confidentialité des secrets d'entreprise et commerciaux de reeweb, ou de les faire effectuer par des auditeurs désignés au cas par cas, à condition que ceux-ci ne soient pas en concurrence avec reeweb. Le client doit informer reeweb en temps utile (en règle générale au moins quatre semaines à l'avance) de toutes les circonstances liées à la réalisation du contrôle.

(4) Au choix de reeweb, la preuve du respect des mesures techniques et organisationnelles peut être apportée, au lieu d'un contrôle sur place, par la présentation d'une attestation appropriée et récente, de rapports ou d'extraits de rapports d'instances indépendantes (par exemple, experts-comptables, révision, délégué à la protection des données, service de sécurité informatique, auditeurs de protection des données ou auditeurs de qualité) ou d'une certification appropriée par des audits de sécurité informatique ou de protection des données – par exemple selon la norme ISO 27001 ou conformément à l'article 42 du RGPD – (« rapport d'audit ») si le rapport d'audit permet au client de s'assurer de manière appropriée du respect des mesures techniques et organisationnelles. Le respect des règles de conduite approuvées peut également être considéré comme une preuve.

(5) Si le client charge un tiers d'effectuer le contrôle, il doit obliger ce tiers à respecter la confidentialité. Reeweb est également en droit d'exiger du tiers, avant l'audit, un engagement de confidentialité interdisant de communiquer au client des informations autres que celles relatives à la protection des données concernant la commande et au tiers toute information constatée dans le cadre de la commande et de l'audit. Le client n'est pas autorisé à confier le contrôle à un concurrent de reeweb.

(6) Pour l'assistance dans le cadre des contrôles du client, reeweb peut exiger une rémunération supplémentaire raisonnable pour les frais ainsi occasionnés.

8. Notification en cas d'infractions par reeweb et assistance au client

(1) Reeweb informe immédiatement le client dans tous les cas où lui-même, les personnes qu'il emploie ou les sous-traitants qui lui sont assignés ont enfreint les dispositions relatives à la protection des données à caractère personnel du client ou les dispositions convenues dans la commande et où reeweb en a pris connaissance. Le contenu des notifications est conforme à la législation applicable en matière de protection des données.

(2) Le client doit informer reeweb immédiatement et de manière exhaustive s'il constate, lors de la vérification des résultats de la commande, des erreurs ou des irrégularités concernant les dispositions relatives à la protection des données ou ses instructions.

(3) Reeweb aide le client, dans la mesure de ses possibilités et dans le cadre du présent accord, à respecter les obligations légales en matière de sécurité des données à caractère personnel, les obligations de notification en cas de violation de données, les analyses d'impact relatives à la protection des données et les consultations préalables avec l'autorité de contrôle. Cela comprend notamment la garantie d'un niveau de protection adéquat grâce à des mesures techniques et organisationnelles qui tiennent compte des circonstances et des finalités du traitement ainsi que de la probabilité et de la gravité prévues d'une éventuelle violation de la loi due à des failles de sécurité et qui permettent une détection immédiate des incidents pertinents.

(4) Pour les prestations d'assistance qui ne sont pas incluses dans le cahier des charges du contrat principal ou qui ne sont pas imputables à une faute de reeweb, reeweb peut réclamer une rémunération supplémentaire appropriée pour les frais ainsi occasionnés.

9. Pouvoir d'instruction du client

(1) Le traitement des données s'effectue exclusivement dans le cadre des accords conclus et selon les instructions du client, sauf si des dispositions légales s'opposent à ces instructions. Les instructions relatives à la mise à disposition de données au client ou à des tiers désignés par celui-ci, par exemple pour l'exercice de droits légaux conformément au règlement (UE) 2023/2854 (Data Act), sont considérées comme des instructions autorisées au sens du présent accord. reeweb communique ces exigences légales au client, sauf si cette communication est contraire à un intérêt public important. Le client doit donner ses instructions générales de manière automatisée via les fonctions du logiciel ClubDesk fournies conformément au contrat principal, ses saisies et configurations côté client.

(2) Reeweb n'est pas tenu d'exécuter d'autres instructions individuelles. Cela ne s'applique pas à l'instruction individuelle de supprimer toutes les données traitées pour le compte du client, que reeweb doit toujours exécuter s'il est certain qu'elle provient du client ou d'une personne habilitée à le représenter. Le client confirme immédiatement les instructions individuelles verbales au moins par écrit. Une suppression nécessite toujours une instruction au moins sous forme écrite. Reeweb doit informer immédiatement le client s'il estime qu'une instruction individuelle au sens du présent paragraphe enfreint les dispositions relatives à la protection des données. Reeweb est en droit de suspendre l'exécution de l'instruction concernée jusqu'à ce qu'elle soit confirmée ou modifiée par le client. Si reeweb exécute une instruction individuelle conformément au présent paragraphe, il est en droit d'exiger une rémunération supplémentaire appropriée pour les frais ainsi occasionnés.

(3) Les personnes habilitées à donner des instructions sont celles qui peuvent représenter efficacement le client.

10. Suppression des données à caractère personnel

(1) Aucune copie ou duplication des données n'est effectuée à l'insu du client. Cela ne s'applique pas aux copies de sauvegarde, dans la mesure où elles sont nécessaires pour garantir un traitement correct des données. En outre, reeweb est autorisé à utiliser des copies des données du client à des fins de test de logiciels (par exemple, migration de données lors de nouveaux Releases) et d'assistance (par exemple, débogage sur des systèmes de test).

(2) À la demande du client et au plus tôt après l'achèvement des travaux convenus contractuellement (c'est-à-dire à la fin du contrat conformément aux conditions générales en vigueur), reeweb doit supprimer, conformément à la protection des données, toutes les données à caractère personnel relevant de la responsabilité du client qui sont en sa possession et qui sont liées à la relation contractuelle. Cela s'applique également aux copies des données du client chez reeweb, telles que les sauvegardes de données. Il incombe au client de sauvegarder lui-même ses données sur ses propres systèmes avant la fin du contrat ou avant de donner l'ordre de suppression. Reeweb confirmera la suppression au client par écrit.

(3) Les documents servant à prouver le traitement correct et conforme des données doivent être conservés par reeweb au-delà de la fin du contrat, conformément aux délais de conservation applicables. Il peut les remettre au client à la fin du contrat pour se décharger de sa responsabilité.

11. Divers

1) Sauf disposition particulière dans le présent accord, les dispositions du contrat conformément aux CGV en vigueur s'appliquent, en particulier les limitations de responsabilité conformément à l'article 14 des CGV.

(2) reeweb ne transmettra les données du client à des tiers que sur instruction documentée ou sur la base d'une obligation légale contraignante. Les demandes de tiers en rapport avec la loi sur les données (par exemple, les articles 5 ou 8) ne seront satisfaites que si le client en a été informé au préalable et a donné son accord, dans la mesure où la loi le permet. Les transferts ou synchronisations initiés de manière indépendante par le client via les interfaces ou fonctions mises à disposition ne sont pas considérés comme une transmission par reeweb.

Bâle, le 23 février 2026

12. Annexe – Mesures techniques et organisationnelles

1. Confidentialité

- Contrôle d'accès (aucun accès non autorisé aux installations de traitement des données) :

reeweb ag : aucun stockage de données chez reeweb ag, les logiciels et les données sont entièrement hébergés dans un centre de données externe (systèmes de production et de test) ;

Centre de données : aucun accès non autorisé aux installations de traitement des données ; la vidéosurveillance et le principe de contrôle d'accès à plusieurs niveaux garantissent la sécurité physique ;

- Contrôle d'accès (aucune utilisation non autorisée du système) :

mots de passe sécurisés (longueur minimale des mots de passe pour ClubDesk, chiffres et caractères spéciaux requis, etc.), mécanismes de verrouillage automatiques (les comptes utilisateurs sont automatiquement verrouillés après plusieurs tentatives de connexion infructueuses), seule la valeur de hachage des mots de passe est enregistrée ;

- Contrôle d'accès (pas de lecture, copie, modification ou suppression non autorisée dans le système) :

ClubDesk offre un système complet de rôles pour des droits d'accès adaptés aux besoins de chaque utilisateur d'un club, la journalisation des connexions et des accès en écriture (les modifications apportées aux données sont enregistrées dans un historique, avec horodatage et nom d'utilisateur) ;

les modifications apportées aux données personnelles au sein de l'application sont enregistrées par le système. Les données enregistrées peuvent notamment contenir les informations suivantes :

- type de modification,
- date et heure de la modification,
- utilisateur autorisé ayant effectué la modification.

L'accès aux historiques des connexions et des modifications est techniquement limité aux utilisateurs disposant des droits d'accès correspondants à ClubDesk (par exemple, les administrateurs et autres personnes disposant de droits d'accès aux modules ClubDesk correspondants).

Tout accès par d'autres utilisateurs est exclu. Le traitement des données enregistrées dans les journaux est effectué exclusivement dans le but de respecter les instructions du responsable du traitement et de garantir l'intégrité et la sécurité du traitement.

- Contrôle de la séparation (traitement séparé des données collectées à des fins différentes) :

les données sont stockées par association dans une base de données distincte avec un identifiant de connexion séparé.

2. Intégrité

- Contrôle de la transmission (pas de lecture, copie, modification ou suppression non autorisées lors de la transmission ou du transport électronique) :

Connexion web sécurisée avec les serveurs d'application via HTTPS, y compris pour les sites web des associations créés dans le logiciel ClubDesk.

Envoi et réception sécurisés d'e-mails via TLS (si le serveur de messagerie récepteur ou émetteur le prend en charge). ClubDesk utilise également différentes technologies pour garantir l'intégrité et l'authenticité des e-mails et de leurs expéditeurs : Domain-based Message Authentication (DMARC), Domain Keys Identified Mail (DKIM) et Sender Policy Framework (SPF). Le client est seul responsable de l'envoi non crypté d'e-mails (si le serveur de messagerie destinataire ou expéditeur ne prend pas en charge TLS) à l'aide de la fonctionnalité correspondante de ClubDesk.

- Contrôle des entrées (déterminer si et par qui des données à caractère personnel ont été saisies, modifiées ou supprimées dans les systèmes de traitement des données) :

Enregistrement des connexions et des accès en écriture : les modifications apportées aux données sont enregistrées dans un historique, avec l'horodatage et le nom de l'utilisateur.

3. Disponibilité et résilience

- Contrôle de la disponibilité (protection contre la destruction ou la perte accidentelle ou intentionnelle) :

reeweb ag : entre autres, mise en miroir des disques durs (RAID), sauvegardes quotidiennes dans le centre de données, pare-feu, protection antivirus pour les fichiers téléchargés, surveillance externe des composants logiciels et matériels importants avec alerte SMS au support de niveau 3 ;

Centre de données : détecteurs d'incendie ; lignes redondantes et complètement séparées pour l'énergie et les données ; Internet à sécurité intégrée, composants réseau redondants ; alimentation électrique sans interruption (ASI) ; sauvegarde des données à la pointe de la technologie : sauvegarde multiple, séparée localement dans différentes zones de protection contre les incendies ;

- Restauration rapide :
grâce aux sauvegardes et à la configuration standardisée des serveurs, le fonctionnement peut être rapidement rétabli en cas d'urgence.

4. Procédure de contrôle, d'évaluation et d'analyse réguliers

- Gestion de la protection des données :
Dispositions relatives à la protection des données dans tous les contrats de travail et directives sur le wiki interne ; la direction est sensibilisée à la question de la protection des données ;

- Gestion des incidents :
Outil externe de gestion des incidents d'assistance, dans lequel toutes les demandes d'assistance sont gérées et surveillées ;
- Paramètres par défaut favorables à la protection des données :
par exemple, rôles prédéfinis pour les fonctions typiques au sein d'une association ;
- Contrôle des commandes (pas de traitement des données pour le compte d'un client sans instruction correspondante de sa part) :
rédaction claire des contrats, sélection et contrôle rigoureux du centre de données.