DATACAMPUS
HÉBERGEMENT DURABLE

Datacampus et la réglementation européenne GDPR (RGPD)

Réglementations en matière de protection des données à caractère personnel

Il existe différents textes de portée internationale, européenne ou nationale qui sont aujourd'hui applicables en matière de protection des données à caractère personnel. Les principaux sont les suivants :

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogée le 25 mai 2018 par le Règlement (UE) 2016/679.
- 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 (règlement général sur la protection des données).
- Charte des droits fondamentaux de l'Union européenne (2012/C 326/02).
- Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Datacampus s'engage à se conformer aux obligations lui incombant en vertu des réglementations suscitées et, particulièrement, du Règlement général sur la protection des données (RGPD). C'est notamment grâce à cet engagement de conformité que les clients de Datacampus sont également en mesure de respecter une partie de leurs obligations réglementaires. Nous encourageons vivement l'ensemble de nos clients à être particulièrement vigilant sur ces aspects de conformité.

D'autres réglementations plus spécifiques peuvent aussi exister, notamment pour certaines catégories particulières de données à caractère personnel. C'est le cas pour les traitements de données de santé, de données de militaires, etc. Il appartient au client de bien identifier les réglementations applicables à ses activités, afin de s'y conformer.
Bien choisir son prestataire, notamment en matière de cloud, est impératif pour respecter ses propres obligations en matière de protection des données à caractère personnel.

Le Règlement général sur la protection des données (RGPD) est le cadre juridique du traitement de données à caractère personnel en Europe, à compter du 25 mai 2018. Contrairement à la directive 95/46/CE, qui régissait jusqu'alors ces traitements, le RGPD est d'application directe dans l'Union et ne nécessite pas de transpositions nationales. À ce titre, il va favoriser l'harmonisation des régimes juridiques en matière de protection des données à caractère personnel en Europe. Mieux encore, le RGPD dispose d'un principe d'extraterritorialité qui permet, dans certaines circonstances, d'étendre son périmètre d'application en dehors des frontières européennes.

Si vous êtes une structure traitant des données à caractère personnel, il y a de fortes chances pour que vous soyez assujetti aux dispositions du RGPD. À cet égard, vous êtes soumis à des obligations auxquelles il faut vous conformer. Il en est de même pour Datacampus qui, au regard de sa situation, disposera d'obligations distinctes : en sa qualité de sous-traitant ou de responsable de traitement.

Définitions

Comprendre les enjeux réels et précis d'un règlement européen n'est pas toujours chose aisée, surtout lorsqu'il comporte 99 articles, 173 considérants et de nombreuses lignes directives servant à préciser son interprétation. C'est pourtant essentiel afin d'éviter tout risque pouvant résulter d'une interprétation trop large ou imprécise des obligations réglementaires incombant à votre structure. La bonne compréhension des quelques termes définis ci-dessous est donc essentielle :

- données à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable. Est réputée être une personne physique identifiable une personne physique qui peut être identifiée, directement ou indirectement.
- 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 (collecte, enregistrement, transmission, stockage, conservation, extraction, consultation, utilisation, interconnexion, etc.).
- responsable du traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.
- sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Datacampus en qualité de sous-traitant

C'est certainement en cette qualité que vos attentes envers Datacampus sont les plus importantes. Datacampus est qualifié de « sous-traitant » lorsqu'il traite des données à caractère personnel pour le compte d'un responsable de traitement.

C'est typiquement le cas lorsque vous utilisez les services de Datacampus et stockez des données à caractère personnel sur une infrastructure Datacampus. Dans la limite de ses contraintes techniques, Datacampus ne pourra traiter les données stockées que selon vos instructions, et ce pour votre compte.

Les engagements de Datacampus en qualité de sous-traitant

En qualité de sous-traitant, Datacampus s'engage notamment à mettre en œuvre les actions suivantes :

- traiter les données à caractère personnel aux seules fins de la bonne exécution des services : Datacampus ne traitera jamais vos informations à d'autres fins (marketing, etc.).
- ne pas transférer vos données hors UE ou hors pays reconnus par la Commission européenne comme disposant d'un niveau de protection suffisant.
- vous informer de tout recours à des sous-traitants qui pourraient traiter vos données à caractère personnel : à ce jour, aucune prestation impliquant un accès aux contenus stockés par vos soins dans le cadre des services n'est sous-traitée en dehors du groupe Datacampus.
- à mettre en œuvre des standards de sécurité élevés afin de fournir un haut niveau de sécurisation à nos services.
- vous notifier dans les meilleurs délais en cas de violation de données.
- vous assister à respecter vos obligations réglementaires en vous fournissant une documentation adéquate de nos services.

Ces engagements sont concrètement retranscrits au travers des Conditions générales de service (CGS) de Datacampus. À ce titre, et sauf conditions particulières, elles sont opposables par tout client à Datacampus en sa qualité de sous-traitant.

Datacampus en qualité de responsable de traitement

Datacampus est qualifié de « responsable de traitement » lorsqu'il détermine les finalités et les moyens de « ses » traitements de données à caractère personnel.

C'est typiquement le cas quand Datacampus collecte des données à des fins de facturation, de gestion des recouvrements, de l'amélioration de la qualité des services et de la performance, de démarchage commercial, de gestion commerciale, etc. Mais aussi lorsque Datacampus traite les données à caractère personnel de ses propres salariés.

Dans cette hypothèse, « vos » données, celles que vous stockez sur les services de Datacampus, ne sont pas concernées. En revanche, certaines informations vous concernant ou étant relatives à vos salariés (identité et coordonnées de l'interlocuteur Datacampus dans le cadre d'une demande d'assistance technique, par exemple) peuvent l'être. C'est pourquoi Datacampus tient à vous donner des éléments de compréhension sur les garanties mises en œuvre afin d'assurer la protection de ces données à caractère personnel.

- limiter la collecte de données à celles strictement utiles : c'est dans le cadre de cette démarche que lors de la commande d'un service, vous ne renseignez que des données

nécessaires pour que Datacampus puisse assurer des services de facturation, de support ou encore respecter ses propres obligations légales en matière de conservation de données(notamment sur le fondement de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique).

- ne pas utiliser les données collectées à d'autres fins que celles pour lesquelles elles furent collectées.
- conserver les données à caractère personnel durant une période limitée et proportionnée. C'est ainsi qu'à titre d'exemple, les données traitées à des fins de gestion de la relation entre le client et Datacampus (nom, prénom, adresse postale, e-mail, etc.) sont conservées par l'entreprise pendant toute la durée du contrat et les trente-six (36) mois suivants. Au terme de ce délai, elles sont supprimées sur tous supports et sauvegardes.
- ne pas transférer ces données à des tiers autres que les sociétés apparentées de Datacampus qui interviennent dans le cadre de l'exécution du contrat. Dans le cadre de ces transferts intra-Groupe, certaines données peuvent être transférées en dehors de l'Union Européenne sur le fondement des règles d'entreprise contraignantes mises en œuvre par le Groupe Datacampus.
- mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un haut niveau de sécurité.

Datacampus et la protection des données à caractère personnel

Il est essentiel de faire la distinction entre la sécurité des données hébergées par le client et la sécurité des infrastructures sur lesquelles ces informations sont hébergées.

Sécurité des données hébergées par le client : le client est seul responsable d'assurer la sécurité de ses ressources et systèmes d'applications qu'il déploie dans le cadre de l'utilisation des services. Des outils sont mis à disposition par Datacampus afin d'accompagner le client dans la sécurisation de ses données.

Sécurité des infrastructures : Datacampus s'engage sur une sécurité optimale de ses infrastructures, notamment en ayant mis en place une politique de sécurité des systèmes d'information et en répondant aux exigences de l'état de l'art de la profession.

Sécurité des infrastructures Datacampus

Datacampus prend les précautions utiles pour préserver la sécurité et la confidentialité des données à caractère personnel traitées, notamment afin d'empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Datacampus s'engage notamment à mettre en place :

Système de gestion de la sécurité

Engagements pris par Datacampus en sa qualité d'hébergeur: Une politique de sécurité des systèmes d'information (PSSI) est mise en œuvre et décrit l'ensemble de nos dispositifs en la matière. Notre PSSI est mise à jour chaque année au minimum ou en cas de changements majeurs entraînant des conséquences sur son contenu. La sécurité de nos solutions est, quant à elle, régie au sein de systèmes de gestion de la sécurité de l'information formels. Différents rôles coordonnent nos actions liées à la sécurité du périmètre : Le responsable de la sécurité des systèmes d'information (RSSI); Le responsable sécurité, chargé des processus et des projets associés à la sécurité du périmètre ; Le délégué à la protection des données (DPO), qui assure la préservation des informations à caractère personnel ; Le gestionnaire des risques, qui coordonne la gestion des risques de sécurité et les plans d'action idoines ; Le responsable des mesures de sécurité, qui implémente et applique les dispositions en relation avec les risques identifiés.

Conformité et certification

Engagements pris par Datacampus en sa qualité d'hébergeur: Afin de s'assurer du maintien de la conformité et d'évaluer la performance de nos systèmes, des audits de sécurité sont réalisés régulièrement. Il en existe cinq types : Les audits externes (certifications, attestations, clients) ; Les audits internes, réalisés par des auditeurs internes ou externes ; Les audits techniques (tests d'intrusion, scans de vulnérabilité, revues de code), réalisés par des auditeurs internes ou externes ; Les audits des activités des tiers, réalisés par le responsable de la gestion des tiers ; Les audits des datacenters, réalisés par des auditeurs internes. La nature et la fréquence des audits réalisés dépendent des solutions et des périmètres. Lorsqu'une situation non conforme est identifiée, elle fait l'objet d'une mesure corrective ajoutée aux plans d'action. Toutes ces mesures font l'objet d'un suivi formel, tracé, ainsi que d'une revue régulière où leur efficacité est réexaminée.

Audits client

Recommandations destinées au client responsable de traitement: Le client peut réaliser des audits techniques (tests d'intrusion) sur les services hébergés pour son compte, ainsi que sur les briques de gestion du service. Les conditions de réalisation des audits sont prévues dans les contrats ou gérées dans une base ad hoc sur demande.

Engagements pris par Datacampus en sa qualité d'hébergeur Les conditions de réalisation des audits sont prévues dans les contrats ou gérées dans une base ad hoc sur demande.

Gestion des risques

Recommandations destinées au client responsable de traitement: Le client doit s'assurer que les mesures de sécurité mises en place par Datacampus sont pertinentes par rapport aux risques associés à son utilisation de l'infrastructure.

Engagements pris par Datacampus en sa qualité d'hébergeur Une méthodologie formelle de gestion des risques est mise en place. Elle est revue chaque année au minimum ou en cas de changements majeurs. Elle concerne également les informations à caractère personnel et les données sensibles (santé, paiements, etc.). Cette méthodologie formalise les analyses effectuées : identification des actifs, des processus métier critiques, des menaces et des vulnérabilités. Elle est fondée sur la norme ISO 27005. Un plan de traitement des risques identifiés est mis en place à la fin de chaque analyse. Celui-ci est mis en œuvre sous 12 mois maximum. Il documente en détail l'analyse et hiérarchise les actions à effectuer. Chaque mesure corrective est ajoutée aux plans d'action et fait l'objet d'un suivi formel, tracé, ainsi que d'une revue régulière où son efficacité est réexaminée.

Gestion des changements

Recommandations destinées au client responsable de traitement : Le client doit s'assurer de la justesse de ses informations de contact, afin que Datacampus puisse lui notifier les changements ayant potentiellement un impact sur ses solutions. Le cas échéant, il appartient au client de mettre en œuvre les actions nécessaires sur la configuration de ses services pour prendre en compte ces évolutions.

Engagements pris par Datacampus en sa qualité d'hébergeur : Une procédure formelle de gestion des changements est mise en place : Les rôles et responsabilités sont clairement définis ; Des critères de classification sont précisés pour identifier les étapes à suivre dans la mise en place du changement ; Les priorités sont gérées ; une analyse des risques associés aux changements est réalisée (si un risque est identifié, le responsable sécurité et le gestionnaire des risques participent à la validation du changement) ; Des tests d'intrusion sont éventuellement réalisés (si applicable) ; le changement est planifié et programmé avec les clients (si applicable) ; Le déploiement est progressif (1/10/100/1000) et, en cas de risque, une procédure de retour en arrière est prévue ; Une revue a posteriori des différents actifs concernés par le changement est réalisée ; L'ensemble des étapes est documenté dans l'outil de gestion des changements.

Politique de développement des systèmes et applications

Engagements pris par Datacampus en sa qualité d'hébergeur : Des processus à l'usage des développeurs de Datacampus sont mis en place et documentés. Ils contiennent les principes pour développer de façon sécurisée, les mesures de « privacy by design », ainsi qu'une politique de revue de code (détection des vulnérabilités, traitement des erreurs, gestion des accès et des entrées, sécurisation du stockage et des communications). Des revues de code sont aussi effectuées régulièrement ; Validation des nouvelles fonctionnalités avant le lancement, tests en environnement de validation (si applicable) et déploiement progressif (1/10/100/1000) ; Séparation des rôles et des responsabilités entre les développeurs et les personnes chargées de la mise en production.

Monitoring des services et des infrastructures

Engagements pris par Datacampus en sa qualité d'hébergeur: Une infrastructure de monitoring est mise en œuvre sur l'ensemble des services de Datacampus. Ses objectifs sont multiples : Détecter les incidents de production et de sécurité ; Surveiller les fonctions critiques avec une remontée d'alerte au système de supervision ; Prévenir les responsables et déclencher les procédures adéquates ; Assurer la continuité du service dans l'accomplissement des tâches automatisées ; S'assurer de l'intégrité des ressources monitorées.

Gestion des incidents

Recommandations destinées au client responsable de traitement: Le client doit s'assurer de la justesse de ses informations de contact, afin que Datacampus puisse le notifier en cas d'incident. Il doit également mettre en place des processus de gestion des incidents affectant son système d'information, en incluant Datacampus comme source potentielle d'alerte.

Engagements pris par Datacampus en sa qualité d'hébergeur: Un processus de gestion des incidents est mis en place. Il permet de prévenir, détecter et résoudre ces événements dans les infrastructures de management du service et le service lui-même. Ce processus intègre : Un guide

de qualification des événements de sécurité ; Le traitement des événements de sécurité ; Des exercices de simulation pour la cellule de crise ; Des tests du plan de réponse aux incidents ; La communication client dans le cadre d'une cellule de crise. Ces procédures bénéficient d'un processus d'amélioration continue pour la surveillance, l'évaluation, ainsi que la gestion globale des incidents et de leurs actions correctives.

Gestion des vulnérabilités

Recommandations destinées au client responsable de traitement: Le client doit s'assurer de la justesse de ses informations de contact, afin que Datacampus puisse le notifier en cas de vulnérabilité détectée sur son système d'information.

Engagements pris par Datacampus en sa qualité d'hébergeur: Une veille technologique sur les nouvelles vulnérabilités est assurée par le responsable sécurité et ses équipes. Elles sont identifiées via : Les sites d'information publics ; Les alertes des constructeurs et des éditeurs des solutions déployées ; Les incidents et les observations remontées par nos équipes d'exploitation, des tiers ou des clients ; Les scans de vulnérabilité internes et externes réalisés régulièrement ; Les audits techniques, ainsi que les revues de code et de configuration. Si une vulnérabilité est détectée, une analyse est réalisée par des équipes dédiées pour déterminer l'impact sur les systèmes et les scénarios d'exploitation potentiels. Des actions de mitigation sont mises en œuvre, si nécessaire, puis un plan correctif est défini. Chaque mesure prise est ajoutée aux plans d'action et fait l'objet d'un suivi formel, tracé, ainsi que d'une revue régulière où son efficacité est réexaminée.

Gestion de la continuité d'activité

Recommandations destinées au client responsable de traitement: La continuité du système d'information est de la responsabilité du client. Il doit s'assurer que les dispositifs standards mis en place par Datacampus, les options souscrites et les dispositifs complémentaires qu'il met en œuvre permettent d'atteindre ses objectifs.

Engagements pris par Datacampus en sa qualité d'hébergeur: La continuité d'activité des infrastructures (disponibilité des équipements, des applications et des processus d'exploitation) est assurée par différents dispositifs : La continuité du refroidissement liquide et par air ; La continuité et la redondance de l'approvisionnement en électricité ; La gestion de la capacité pour les équipements sous la responsabilité de Datacampus ; Le support technique du service ; La redondance des équipements et serveurs utilisés pour l'administration des systèmes. En parallèle, d'autres mécanismes, tels que la sauvegarde du réseau et la configuration des équipements, assurent la reprise du service en cas d'incident. En fonction du service, Datacampus pourra proposer des fonctionnalités de sauvegarde et restauration que le client pourra utiliser, soit en tant que fonctionnalités intégrées dans l'offre de base soit en tant qu'options payante.

Risques naturels et environnementaux

Engagements pris par Datacampus en sa qualité d'hébergeur : Des mesures sont mises en œuvre afin de prévenir les risques naturels et environnementaux : L'installation de paratonnerres, afin de réduire l'onde électromagnétique concomitante ; L'aménagement des locaux de Datacampus dans des zones non inondables et sans risques sismiques ; La présence d'alimentations sans interruption (UPS) de capacité suffisante et de transformateurs de secours avec basculement automatique de la charge ; Le basculement automatique vers des groupes électrogènes disposant d'une autonomie minimale de 48 heures ; Le déploiement d'unités de chauffage, ventilation et climatisation (HVAC) maintenant la température et l'humidité à un niveau constant ; La gestion d'un système de détection d'incendies (des exercices anti-incendie sont réalisés tous les 6 mois dans les datacenters).

Mesures générales sur la sécurité des sites physiques

Engagements pris par Datacampus en sa qualité d'hébergeur : L’accès physique aux sites de Datacampus repose sur une sécurité périmétrique restrictive, effective dès la zone d'entrée. Chaque local est ainsi classifié : Les zones de circulation privées ; Les bureaux accessibles à tous les employés et aux visiteurs enregistrés ; Les bureaux confidentiels, restreints à certains personnels ; Les zones hébergeant les équipements des datacenters ; Les zones confidentielles des datacenters ; Les zones des datacenters hébergeant des services critiques. Des mesures de sécurité sont mises en place afin de contrôler les accès aux sites physiques de Datacampus : Une politique des droits d'accès ; Des murs (ou dispositifs équivalents) entre chaque zone ; Des caméras situées aux entrées et sorties des installations, ainsi que dans les salles de serveurs ; Des accès sécurisés, contrôlés par des badgeuses ; Un système de détection de mouvement ; Des mécanismes anti-effraction aux entrées et sorties des datacenters ; Des mécanismes de détection d'intrusion (telesurveillance 24 heures sur 24 et vidéosurveillance) ; Un centre de surveillance permanent, contrôlant les ouvertures des portes d'entrée et de sortie.

Accès aux sites de Datacampus

Engagements pris par Datacampus en sa qualité d’hébergeur: Les contrôles d'accès physiques sont fondés sur un système de badge. Chaque badge est lié à un compte Datacampus, lui-même lié à un individu. Ce dispositif permet d'identifier toute personne dans les installations et d'authentifier les mécanismes de contrôle : Chaque individu entrant sur les sites de Datacampus doit avoir un badge personnel lié à son identité ; Toute identité doit être vérifiée avant la fourniture d'un badge ; Dans les installations, le badge doit être porté de manière visible ; Les badges ne doivent pas mentionner le nom de son propriétaire ou le nom de l'entreprise ; Les badges doivent permettre d'identifier immédiatement les catégories des personnes présentes (employés, tiers, accès temporaires, visiteurs) ; Le badge est désactivé dès que son propriétaire cesse d'être autorisé à accéder aux installations ; Le badge des employés de Datacampus est activé pour la durée du contrat de travail ; pour les autres catégories, il est désactivé automatiquement après une période définie ; Un badge non utilisé pendant trois semaines est automatiquement désactivé.

Gestion des accès aux zones

Engagements pris par Datacampus en sa qualité d’hébergeur : L'accès aux portes par des badges Il s'agit du contrôle d'accès standard au sein des locaux de Datacampus : La porte est connectée au système centralisé de gestion des droits d'accès ; La personne doit utiliser son badge sur le lecteur dédié pour déverrouiller la porte ; Les accès sont vérifiés au moment de la lecture, afin de s'assurer que les personnes disposent des droits d'entrée appropriés ; En cas de panne du système centralisé de gestion des droits d'accès, les droits configurés au moment de l'incident sont valables pendant toute la durée de l'événement ; Les serrures des portes sont protégées contre les coupures électriques et restent fermées dans ces situations. L'accès aux portes par des clefs Certaines zones ou équipements sont fermés à l'aide de serrures à clef : les clefs sont stockées dans un emplacement centralisé et restreint pour chaque site, avec un référentiel ; toute clef est identifiée avec une étiquette ;• un inventaire des clefs est maintenu ; toute utilisation des clefs est traçable, via un mécanisme de livraison ou un journal papier ; le référentiel des clefs est vérifié quotidiennement selon l'inventaire. L'accès aux datacenters par des sas unipersonnels L'accès à nos centres de données s'effectue exclusivement via des sas unipersonnels : chaque sas comporte deux portes et une zone confinée entre les contrôles, afin de s'assurer qu'une seule personne passe à la fois ; une porte ne peut être ouverte que si l'autre est fermée (mantrap) ; les sas utilisent le même système de badge que les autres portes, avec les mêmes règles applicables ; des mécanismes de détection vérifient qu'une seule personne est présente dans le sas (anti-piggybacking) ; le système est configuré pour empêcher l'utilisation du

badge plus d'une fois dans le même sens (anti-passback) ; une caméra placée autour du sas permet de surveiller les entrées. L'accès aux sas de marchandise L'accès des marchandises aux datacenters est réalisé exclusivement par des passerelles dédiées : Le vestibule de livraison est configuré de la même manière qu'un sas unipersonnel, avec un plus grand espace, aucun contrôle sur le volume et le poids, ainsi que des badgeuses uniquement en extérieur ; Seul l'article livré passe par le vestibule, les individus doivent entrer via les sas unipersonnels ; Une caméra est située dans le vestibule, sans angle mort.

Gestion des accès physiques des tiers

Recommandations destinées au client responsable de traitement: Datacampus n'intervient jamais chez ses clients. Ils sont responsables de la sécurité de leurs locaux.

Engagements pris par Datacampus en sa qualité d'hébergeur: La circulation des visiteurs et prestataires occasionnels est strictement encadrée. Ces personnes sont enregistrées dès leur arrivée sur le site et sont munies d'un badge visiteur ou prestataire : Chaque visite doit être déclarée en amont ; Les tiers sont sous la responsabilité d'un salarié et sont toujours accompagnés ; Toutes les identités sont vérifiées avant l'accès aux sites ; chaque tiers possède un badge personnel attribué pour la journée, qu'il doit rendre avant de quitter le site ; Tous les badges doivent être portés de manière visible ; Les badges sont automatiquement désactivés à la fin de la visite.

Sensibilisation et formation du personnel

Engagements pris par Datacampus en sa qualité d'hébergeur : Le personnel de Datacampus est sensibilisé à la sécurité, ainsi qu'aux règles de conformité des traitements de données à caractère personnel : Des sessions de formation sur ces sujets sont dispensées annuellement aux équipes concernées ; Des sessions de formation sur la réalisation des audits sont dispensées annuellement aux équipes concernées ; Des sessions de formation sur les services techniques sont dispensées annuellement aux équipes concernées ; Une sensibilisation à la sécurité du système d'information (SI) est organisée lors de l'intégration des nouveaux salariés ; Des communications relatives à la sécurité sont régulièrement adressées à l'ensemble du personnel ; Des campagnes de tests sont organisées pour s'assurer que les salariés ont les bons réflexes en cas de menace.

Gestion des accès logiques au système d'information Datacampus

Engagements pris par Datacampus en sa qualité d'hébergeur: Une politique stricte de gestion des accès logiques pour les salariés est mise en œuvre : Les habilitations sont attribuées et suivies par les managers, selon la règle du moindre privilège et le principe d'acquisition progressive de confiance ; Dans la mesure du possible, toutes les habilitations sont fondées sur des rôles et non sur des droits unitaires ; La gestion des droits d'accès et des habilitations attribués à un utilisateur ou à un système s'appuie sur une procédure d'enregistrement, de modification et de désinscription impliquant les managers, l'informatique interne et les ressources humaines ; Tous les salariés utilisent des comptes utilisateur nominatifs ; Les sessions de connexion ont systématiquement une durée d'expiration adaptée à chaque application ; L'identité des utilisateurs est vérifiée avant tout changement dans les moyens d'authentification ; En cas d'oubli du mot de passe, seul le manager du collaborateur et le responsable sécurité sont habilités à le réinitialiser ; Les comptes utilisateur sont automatiquement désactivés si le mot de passe n'est pas renouvelé au bout de 90 jours ; L'utilisation de comptes par défaut, génériques et anonymes est prohibée ; Une politique stricte en matière de mots de passe est mise en place ; Grâce à l'emploi d'un générateur automatique, l'utilisateur ne choisit pas son mot de passe ; La taille minimale d'un mot de passe est de 10 caractères alphanumériques ; La fréquence de

renouvellement des mots de passe est de 3 mois ; Le stockage des mots de passe dans des fichiers non chiffrés, sur du papier ou dans les navigateurs web est prohibé ; L'utilisation d'un logiciel local de gestion des mots de passe, validé par les équipes de sécurité, est obligatoire ; Tout accès distant au système d'information (SI) de Datacampus est réalisé par le biais d'un VPN, nécessitant un mot de passe connu uniquement de l'utilisateur ainsi qu'un secret partagé configuré sur le poste de travail.

Gestion des accès d'administration aux plateformes de production

Engagements pris par Datacampus en sa qualité d'hébergeur : Une politique de gestion des accès d'administration des plateformes est mise en place : Tout accès d'administration à un système en production est réalisé via un bastion ; Les administrateurs se connectent aux bastions via SSH, en utilisant des paires de clefs publiques et privées individuelles et nominatives ; La connexion au système cible est réalisée soit par compte de service partagé, soit par compte nominatif via des bastions ;• l'utilisation de comptes par défaut sur les systèmes et équipements est prohibée ; L'authentification à double facteur est obligatoire pour les accès des administrateurs à distance ainsi que les accès des salariés dans les périmètres sensibles, avec un traçage complet ; Les administrateurs ont un compte dédié exclusivement aux tâches d'administration, en complément de leur compte utilisateur ; Les habilitations sont attribuées et suivies par les managers, selon la règle du moindre privilège et le principe d'acquisition de confiance ; Les clefs SSH sont protégées par un mot de passe répondant aux exigences de la politique de mot de passe ;• une revue régulière des droits et des accès est menée en collaboration avec les services concernés.

Sécurité des postes de travail et des équipements mobiles

Recommandations destinées au client responsable de traitement : Le client doit s'assurer de la sécurité des postes de travail et des équipements mobiles permettant l'administration du service et des systèmes.

Engagements pris par Datacampus en sa qualité d'hébergeur: Sécurisation des postes de travail standards Des mesures pour assurer la sécurité des postes de travail standards du personnel de Datacampus sont mises en place : Gestion automatique des mises à jour ; Installation et mise à jour des antivirus, avec des scans réguliers ;• installation uniquement des applications issues d'un catalogue validé ; Chiffrement systématique des disques durs ; Procédure de traitement d'un poste de travail potentiellement compromis ; Standardisation des équipements ; Procédure de suppression des sessions et de réinitialisation des postes lors des départs des salariés. Sécurisation des terminaux mobiles Des mesures pour assurer la sécurité des terminaux mobiles personnels ou fournis par Datacampus sont mises en place : Enregistrement obligatoire des terminaux dans le système de gestion centralisé, avant d'accéder aux ressources internes (WiFi, e-mails, calendriers, annuaire, etc.) ; Vérification de la politique de sécurité déployée sur le terminal (code de déverrouillage, délai de verrouillage, chiffrement du stockage) ; Procédure d'effacement à distance des terminaux en cas de vol ou de perte.

Sécurité du réseau

Recommandations destinées au client responsable de traitement Le client est seul responsable du chiffrement du contenu à communiquer à travers le réseau Datacampus.

Engagements pris par Datacampus en sa qualité d'hébergeur: Datacampus gère un réseau privé de fibres optiques haute performance, interconnecté avec de nombreux opérateurs et transitaires. Datacampus gère son backbone en propre ; elle distribue la connectivité aux réseaux locaux de chaque datacenter et les interconnecte. Tous ces équipements sont sécurisés par les mesures suivantes : La tenue d'un inventaire au sein d'une base de gestion des configurations ; La mise en place d'un processus de durcissement, avec des guides décrivant les paramètres à modifier pour assurer une configuration sécurisée ; Les accès aux fonctions d'administration des équipements sont restreints via des listes de contrôle ; Tous les équipements sont administrés au travers d'un bastion, appliquant le principe du moindre privilège ; Toutes les configurations des équipements réseau sont sauvegardées ; Les logs sont collectés, centralisés et monitorés en permanence par l'équipe d'exploitation réseau ; Le déploiement des configurations est automatisé et fondé sur la base de gabarits validés.

Gestion de la continuité d'activité

Engagements pris par Datacampus en sa qualité d'hébergeur: Une politique de sauvegarde est mise en œuvre sur les serveurs et équipements utilisés par Datacampus pour fournir ses services : Tous les systèmes et données nécessaires à la continuité des services, à la reconstruction du système d'information ou à l'analyse après incident sont sauvegardés (fichiers des bases de données techniques et administratives, journaux d'activité, codes sources des applications développées en interne, configuration des serveurs, applications et équipements, etc.) ; Les fréquences, durées de rétention et modalités de stockage des sauvegardes sont définies en adéquation avec les besoins de chaque actif sauvegardé ; la réalisation des sauvegardes fait l'objet d'un monitoring, ainsi que d'une gestion des alertes et erreurs.

Journalisation

Recommandations destinées au client responsable de traitement : Le client est seul responsable de la politique d'enregistrement pour ses propres systèmes et applicatifs.

Engagements pris par Datacampus en sa qualité d'hébergeur : Une politique de journalisation est mise en œuvre sur les serveurs et équipements utilisés par Datacampus pour fournir ses services : Sauvegarde et conservation centralisée des journaux ; Consultation et analyse des logs par un nombre restreint d'acteurs autorisés, conformément à la politique d'habilitation et de gestion des accès ; Séparation des tâches entre les équipes responsables de l'exploitation de l'infrastructure de monitoring et celles chargées de l'exploitation du service.Voici la liste des activités faisant notamment l'objet d'une journalisation : Logs des serveurs de stockage hébergeant les données des clients ; Logs des machines gérant l'infrastructure du client ; Logs des machines pour le monitoring des infrastructures ; Logs des antivirus installés sur l'ensemble des machines équipées ; Contrôle d'intégrité des logs et des systèmes, le cas échéant ; Tâches et événements effectués par le client sur son infrastructure ; Logs et alertes de détection d'intrusion réseau, le cas échéant ; Logs des équipements réseau ; Logs de l'infrastructure des caméras de surveillance ; Logs des machines des administrateurs ; Logs des serveurs de temps ; Logs des badgeuses ;

Des questions? -> support@datacampus.fr