MESURES TECHNIQUES ET ORGANISATIONNELLES POUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Groupe Computacenter
Système de Management de la Sécurité de l'Information

Group Information Systems

Version du document 3.4

- Sans restriction -

INFORMATIONS SUR LES DOCUMENTS

Documents factuels	
Sujet:	Group Data Privacy TOMs
Versions à partir de:	22/12/2023
Version:	3.4
Cycle de révision	1 an
Classification	Sans restriction
Propriétaire	Group Chief Information Security Officer

Avis

En l'absence de toute disposition spécifique, ce document n'a qu'un statut consultatif. Il ne constitue pas un contrat entre Computacenter et toute autre partie. En outre, Computacenter n'accepte aucune responsabilité quant au contenu du document, bien qu'il ait fait des efforts raisonnables pour en assurer l'exactitude et la bonne compréhension.

TABLE DES MATIÈRES

INTRODUCTION

Ce document présente les mesures de sécurité techniques et organisationnelles mises en œuvre par Computacenter pour protéger les informations et il est applicable à tous les systèmes gérés par Computacenter ainsi qu'à son personnel, ses partenaires et les tiers. Voir les annexes 1 et 2 pour plus d'informations.

Computacenter remplit l'obligation prévue par le Règlement Général sur la Protection des Données (RGPD) de garantir le traitement des données à caractère personnel par des mesures techniques et organisationnelles appropriées et, dans la mesure du possible, de rendre les données à caractère personnel anonymes ou de les *pseudonymiser*. Toutes les mesures mises en œuvre tiennent compte du risque associé au traitement des données concernées. En particulier, l'efficacité de chaque mesure tient compte des objectifs de protection que sont la confidentialité, la disponibilité et l'intégrité.

GESTION DE LA CONFIDENTIALITE DES DONNEES

1 Principes de protection des données

Les paragraphes suivants présentent les principes généraux qui sous-tendent les pratiques de Computacenter en matière de collecte, d'utilisation, de divulgation, de stockage, de sécurisation, d'accès, de transfert ou de traitement des données personnelles.

- **Légalité, équité et transparence**
  - Computacenter traite les données à caractère personnel de manière licite, loyale et transparente vis-à-vis de la personne concernée, uniquement à des fins commerciales légitimes et si le traitement est nécessaire pour respecter ses obligations légales.
- **Limitation de la finalité**
  - Computacenter ne collecte des données personnelles qu'à des fins spécifiques, explicites et légitimes.
  - Tout traitement ultérieur doit être compatible avec cette (ces) finalité(s), sauf si Computacenter a obtenu le consentement de la personne concernée ou si le traitement est autrement autorisé par la loi.
- **Minimisation des données**
  - Computacenter veille à ce que les données à caractère personnel qu'il traite soient adéquates, pertinentes et limitées à ce qui est nécessaire au regard de la ou des finalités du traitement.
- **Limitation du stockage**
  - Computacenter conserve les données à caractère personnel sous une forme permettant de les identifier pendant une durée n'excédant pas celle nécessaire à la réalisation de la ou des finalités, ou d'autres finalités autorisées, pour lesquelles les données à caractère personnel ont été obtenues.
- **Précision**
  - Computacenter prend des mesures raisonnables pour mettre à jour ou supprimer les données qui sont inexactes ou incomplètes. Les personnes ont le droit de demander à Computacenter d'effacer ou de rectifier sans délai les données erronées qui les concernent.
- **Intégrité et confidentialité**
  - Computacenter stocke les données personnelles en toute sécurité et les protège contre tout traitement non autorisé ou illégal et contre toute perte, destruction ou détérioration accidentelle, en utilisant des mesures techniques ou organisationnelles appropriées.
- **Responsabilité**
  - Computacenter établit des politiques, processus, contrôles et autres mesures appropriées nécessaires pour lui permettre de démontrer que son traitement des données à caractère personnel est conforme aux lois applicables en matière de protection des données.

1.1 Fonction de sécurité de l'information

- Computacenter dispose d'une fonction d'System de l'Information du Groupe, dirigée par le Responsable de la Sécurité de l'Information du Groupe (RSSI). Le RSSI du groupe est chargé de veiller à la mise en œuvre des éléments de sécurité de l'information tels que le cadre, les politiques, les processus et les mesures de conformité ;

- Le RSSI du groupe est soutenu par une équipe alignée sur les unités opérationnelles (Business Units) et les zones géographiques ;
- Le RSSI groupe coordonne avec le Délégué à la Protection des Données du Groupe les mesures techniques et organisationnelles de protection des données personnelles ;
- Computacenter a mis en place un système de gestion de la sécurité de l'information (SMSI) basé sur les meilleures pratiques internationales de la norme ISO/IEC 27001:2013 et des normes de sécurité connexes ;
- Le SMSI a été et continue d'être évalué par des auditeurs et reçoit une attestation régulière selon la norme ISO/IEC 270001:2013 ; et
- Computacenter dispose d'un ensemble complet de politiques de sécurité de l'information, approuvées par la Direction Générale et publiées à l'intention de l'ensemble du personnel.

Les principaux objectifs de Computacenter en matière de sécurité de l'information sont les suivants :

- Préserver la confidentialité, l'intégrité et la disponibilité des données internes et des clients, stockées ou traitées, sauf en cas d'autorisation ou d'obligation légale de les divulguer.
- Accepter la responsabilité de la prévention, de la détection et du signalement d'une perte de données et d'autres actifs de l'entreprise ou du client.
- Veiller à ce que les activités liées à la sécurité de l'information soient effectuées de manière fiable, responsable et efficace, et à garantir leur durabilité par des processus intégrés.
- Continuer à proposer des services, des solutions et des produits sécurisés à nos clients dans un environnement sécurisé et intégrer la sécurité dans les processus commerciaux majeurs.
- Procéder régulièrement à des évaluations des risques liés à la sécurité de l'information afin de s'assurer que ces risques sont traités de manière cohérente et efficace, de réduire la probabilité que des incidents liés à la sécurité de l'information se produisent et de limiter leur impact potentiel sur les activités et les clients.
- Continuer à accroître le niveau de compétences professionnelles de nos collaborateurs et fournisseurs en matière de sécurité de l'information.
- S'assurer que notre système de gestion de la sécurité de l'information nous aide à améliorer l'efficacité et l'efficience, et promouvoir une culture d'amélioration continue de la sécurité de l'information afin de renforcer la confiance des clients vis-à-vis de Computacenter, nous aidant à conquérir et à perpétuer des activités commerciales.

2. Respect de la vie privée dès la conception

2.1. Anonymisation et pseudonymisation (article 32, paragraphe 1 bis, et article 25, paragraphe 1)

- L'anonymisation, la pseudonymisation et la minimisation des données à caractère personnel sont envisagées pour les nouvelles activités de traitement des informations conformément aux principes d'un processus "privacy by design/security by design" visant à intégrer, dans la mesure du possible, les meilleures pratiques en matière de sécurité et de respect de la vie privée dans la conception des systèmes
- Des exigences minimales pour l'utilisation de la cryptographie, telles que le chiffrement, sont envisagées sur la base des résultats de l'évaluation des risques, conformément aux politiques et aux standards de Computacenter.

2.2. Alignement sur les normes mondiales

- Computacenter a obtenu un certain nombre de certifications de sécurité ; des politiques et des politiques de sécurité de l'information ont été élaborées pour répondre aux besoins de la norme ISO/IEC 27001:2013
- Les systèmes de Computacenter destinés aux clients sont pris en compte dans ces certifications, ainsi que les technologies internes utilisées par les utilisateurs, fournies par l'équipe des systèmes d'information du groupe.

2.3. Assurance de la sécurité et de la protection des données

- Les nouvelles activités de traitement des données sont évaluées en interne et la minimisation des données et le respect de la vie privée dès la conception sont pris en compte dans le processus de conception et de développement de nouvelles applications ou de nouveaux systèmes
- Lorsque les activités de traitement des données présentent des risques élevés pour la personne concernée, une évaluation d'impact sur la protection des données est réalisée. Toute constatation sensible est porté à l'attention du ou des Délégués à la Protection des Données compétents ou, lorsque ce traitement présente toujours un risque élevé pour les personnes concernées, en consultation avec l'Autorité de Contrôle compétente.

2.4. Droits des personnes concernées

- Les droits des personnes concernées sont garantis par le processus d'évaluation d'impact sur la protection des données de Computacenter, qui s'assure que le traitement des données personnelles par Computacenter respecte ces droits dans la mesure où ils sont applicables.

3. Processus de contrôle et d'évaluation réguliers de l'efficacité (article 32, paragraphe 1, point d), et article 25, paragraphe 1, du GDPR

3.1. Audit interne

- Dans le cadre de la certification ISO/IEC 27001:2013, des programmes complets d'audit interne et d'audit externe sont en place pour garantir que les non-conformités sont identifiées et gérées jusqu'à leur résolution ;
- Des audits externes sont réalisés au moins une fois par an, et des audits internes en continu pour assurer la conformité à la norme ISO/IEC 27001:2013
- Les conclusions sont présentées sous la forme d'un rapport d'audit.

3.2. Programme de gestion des risques pour les tiers

- Les fournisseurs tiers qui traitent des données personnelles au nom des sociétés du groupe Computacenter sont tenus d'accepter des conditions spécifiques qui reflètent

les obligations de Computacenter en tant que responsable du traitement ou de sous-traitant de ces données personnelles ;

- Les capacités de sécurité des fournisseurs tiers sont évaluées par le département Group Information Systems de Computacenter sur la base des services fournis par ce fournisseur et des risques associés à un manquement
- Aucun traitement de données par des tiers n'est autorisé sans un accord contractuel visant à rendre le traitement des données conforme à la réglementation.

3.3. Configuration sécurisée

- Computacenter effectue des contrôles réguliers pour s'assurer que la configuration sécurisée de ses infrastructures respecte les exigences de ses politiques de sécurité de l'information ;
- Les analyses de vulnérabilité et les tests d'intrusion sont utilisés pour identifier le non-respect des politiques de sécurité et y remédier dans les délais convenus ;
- Un programme de correction des systèmes d'exploitation permet de remédier aux défauts des systèmes selon les planning publiés par le fabricant ;
- Le cas échéant, la possibilité pour les utilisateurs de modifier la configuration des systèmes est désactivée ;
- Les serveurs et les systèmes d'exploitation standardisés sont configurés conformément aux standards de l'industrie pour résister aux attaques
- La configuration des systèmes traitant les données personnelles est validée avant leur mise en service dans l'environnement de production.

Annexe 1 - Mesures techniques de sécurité

Contrôle d'accès logique

- Tous les utilisateurs accèdent aux systèmes de Computacenter avec un identifiant unique ;
- Les comptes génériques sont interdits sauf s'il existe une justification opérationnelle et si une exception à l'exigence de la politique de sécurité a été approuvée ;
- Les utilisateurs doivent choisir un mot de passe sécurisé ou un autre moyen d'authentification qui respecte le standard de gestion des justificatifs d'authentification de Computacenter ;
- Les règles d'expiration et de réutilisation des mots de passe sont préconfigurées selon les normes définies dans la le standard de gestion des justificatifs d'authentification de Computacenter ;
- Les comptes d'utilisateur des applications sont configurés avec un processus de déconnexion automatique et les systèmes d'exploitation sont configurés pour verrouiller les comptes après une période d'inactivité déterminée ;
- Pour l'accès à distance aux systèmes, une authentification à deux facteurs est mise en œuvre ;
- Un contrôle d'accès basé sur des rôles est utilisé dans tous les systèmes centraux ;
- Computacenter applique le modèle d'accès *du moindre privilège* pour chaque employé ; tout accès supplémentaire doit être approuvé par le supérieur hiérarchique de l'employé et les propriétaires du système/service ;
- Computacenter dispose d'un processus complet pour désactiver les utilisateurs et leur accès lorsque le personnel quitte l'entreprise ou une fonction
- Tout accès ou tentative d'accès aux systèmes est enregistré et contrôlé.

Mise en œuvre des exigences de séparation des données pour protéger la confidentialité

- Les environnements des plates-formes de services partagés que Computacenter fournit aux clients sont séparés et déployés conformément aux principes des meilleures pratiques en matière de sécurité ;
- Le traitement des données dans chaque environnement est effectué séparément pour chaque client (séparation logique ou physique)
- Les droits d'accès sont contrôlés par des regroupements appropriés et une gestion des droits associés afin de garantir une séparation logique des données entre les clients ;

Contrôles des transferts de données mis en œuvre pour l'intégrité des systèmes (article 32 (1b) du GDPR

Contrôle des médias amovibles

- Le transfert ou le stockage de données personnelles vers ou depuis un téléphone portable, un DVD/CD ou une clé USB est effectué conformément à la Politique de bon usage de l'informatique et à la Matrice de classification et de traitement de l'information de Computacenter ; et
- Il est interdit d'utiliser les supports amovibles pour stocker des données personnelles à des fins commerciales, à moins de demander des exceptions spécifiques et d'obtenir une autorisation.

Transmission des données d'applications web

- Le transfert électronique de données au sein de l'entreprise (et en provenance ou à destination des clients et fournisseurs lorsque cela est stipulé) est effectué via des connexions chiffrées (y compris les VPN SSL/IPSec, TLS) et des circuits spécialisés, ce qui garantit l'intégrité et la confidentialité des informations en transit.

Sécurité des réseaux

- Des contrôles sont réalisés au sein de Computacenter et entre Computacenter et ses clients et fournisseurs pour effectuer le transfert de données en utilisant des connexions chiffrées (TLS, SSL, IPSec) et des lignes dédiées ;
- Les réseaux dédiés aux invités sont séparés des réseaux centraux de Computacenter ;
- L'analyse des vulnérabilités est effectuée par le biais de l'analyse interne du réseau ;
- Des examens périodiques des systèmes par des tiers sont effectués au moyen de tests d'intrusion; et
- L'administration des composants et des dispositifs de réseau est limitée aux personnes qui ont les autorisations appropriées pour la gestion de ces systèmes.

Travail à distance

- Les employés et les sous-traitants sont équipés de matériels de l'entreprise et de méthodes de sécurité appropriées pour se connecter à distance ;
- Un processus d'authentification à deux facteurs est nécessaire pour connecter l'ordinateur portable de l'entreprise au réseau ; et
- Les utilisateurs sont tenus de se conformer à la politique d'utilisation acceptable de Computacenter.

Suivi

- Computacenter exploite une solution de surveillance des informations et des événements de sécurité (SIEM) active 24 heures sur 24 et 7 jours sur 7 pour détecter les événements de sécurité ;
- Les journaux et les événements sont passés en revue quotidiennement par la plateforme SIEM, avec une équipe dédiée assignée et formée à la revue/analyse des journaux et au traitement des alertes/incidents ou à l'escalade si nécessaire ;
- Les événements au niveau du système et du réseau sont surveillés, enregistrés, analysés et les incidents sont signalés avec les priorités pertinentes. Ces incidents sont gérés par le biais d'un processus de gestion des incidents de sécurité
- L'enregistrement des activités des utilisateurs est effectué conformément à la Politique de journalisation et de supervision et la Standard de journalisation et de surveillance des événements de sécurité.

Classification et traitement des documents

- Toutes les données au sein du groupe Computacenter sont classifiées par référence à la Politique de bon usage de l'informatique et à la Matrice de classification et de traitement de l'information de Computacenter et sont utilisées conformément à celle-ci ; et
- Les données personnelles sont classifiées conformément à la Politique de bon usage de l'informatique et à la Matrice de classification et de traitement de l'information, en fonction des risques pour la personne concernée associés à une violation de la sécurité entraînant la perte de ces données personnelles.

Contrôles de disponibilité mis en œuvre pour protéger la disponibilité et la résilience des systèmes (article 32, paragraphe 1b, du GDPR)

Sauvegarde des données

- Computacenter assure la sauvegarde des systèmes centraux en utilisant la technologie des bandes virtuelles, répliquées dans les centres de données.

Prévention des logiciels malveillants

- Des systèmes antivirus sont mis en place pour protéger les composants de l'infrastructure et les terminaux ;
- L'analyse antivirus en temps réel est activée et des analyses régulières et programmées sont effectuées sur les terminaux
- Les courriers électroniques externes sont filtrés pour assurer un niveau d'hygiène supplémentaire, y compris l'antispam, l'anti-phishing et l'analyse antivirus.

Mesures de support au rétablissement d'activité après un sinistre

- Le processus de gestion des risques informatiques et de continuité des activités de Computacenter garantit que les programmes, les configurations et les données sont maintenus disponibles conformément aux processus et aux réglementations définis ;
- En cas de défaillance (catastrophe, désastre), les toutes dernières mesures sont en place pour garantir la récupération et la poursuite de l'utilisation ;
- Computacenter dispose de capacités de gestion de crise localisées, spécifiées dans les procédures de gestion des incidents majeurs et de gestion de la continuité des activités,
- Une documentation détaillée sur le rétablissement de l'activité est disponible pour tous les systèmes centraux, afin de garantir un rétablissement rapide du fonctionnement normal en cas d'incident ;
- Des tests de rétablissement individuels sont effectués régulièrement, et les plans de récupération sont alors mis à jour si nécessaire
- Les procédures de recouvrement sont soumises à un contrôle d'audit interne. Les centres de données du groupe Computacenter sont équipés des dernières technologies de résilience.

Annexe 2 - Mesures de sécurité organisationnelle

Limitation du stockage et rétention

- Les données à caractère personnel sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées ;
- Il incombe au client de déterminer ses exigences en matière de conservation des données relatives aux données à caractère personnel traitées pour les prestations de services ; et
- Les données personnelles sont détruites ou renvoyées au client après l'expiration de la période de conservation des données concernées.

Sensibilisation et formation à la sécurité de l'information et à la protection des données

- Une formation de sensibilisation à la sécurité de l'information et à la protection des données est à la disposition des employés de Computacenter via le système de gestion de la formation en entreprise
- Les employés de Computacenter sont inscrits pour recevoir une formation obligatoire lors de leur entrée dans l'entreprise et à intervalles réguliers par la suite.

Sélection des employés

- Des contrôles préalables à l'emploi sont effectués dans le cadre des processus de recrutement des ressources humaines
- Des vérifications supplémentaires peuvent être requises pour des postes spécifiques ou pour les besoins de certains clients si la législation locale le permet.

Processus d'entrée, de mobilité interne et de départ des employés

- Le processus de recrutement, de mobilité interne et de départ contrôle les droits d'accès attribués à un utilisateur au cours de son emploi dans l'organisation ;
- Lorsqu'un employé quitte Computacenter, le compte utilisateur est immédiatement désactivé par un processus automatisé.

Gestion des incidents de sécurité de l'information et des violations de données

- Un processus de gestion de la sécurité de l'information est établi au sein de Computacenter pour identifier, enquêter et gérer les incidents jusqu'à leur résolution ;
- Les incidents de sécurité et les atteintes potentielles à la vie privée sont traités dans le cadre du processus de gestion des incidents de sécurité
- Les atteintes à la vie privée sont notifiées au responsable de la protection des données concerné et aux clients concernés par le biais du processus de gestion des incidents de sécurité, rapidement et sans retard injustifié.

Des contrôles d'accès physique mis en place pour protéger la confidentialité

- Des mesures de sécurité (contrôle des accès et autres éléments) sont mises en place sur chaque site où une zone de sécurité physique a été définie ;
- Chaque zone de sécurité est contrôlée par des systèmes de contrôle électronique des entrées et certains locaux spécifiques sont renforcés par des agents de sécurité et des fouilles personnelles à la sortie ;
- Les visiteurs des locaux se voient offrir une badge temporaire et doivent toujours être accompagnés par un membre du personnel de Computacenter ;
- Les centres de données de Computacenter ont un périmètre physique défini et protégé, des contrôles physiques comprenant des mécanismes de contrôle d'accès, des zones de livraison et de chargement contrôlées, une surveillance et des agents de sécurité ;
- L'accès aux locaux des centres de données contenant les données des clients est contrôlé par un processus d'enregistrement de sécurité nécessitant une pièce d'identité avec photo
- Le centre de données hébergeant les données des clients est protégé contre les pannes d'électricité et autres perturbations et est doté de systèmes de détection et d'extinction des incendies.

Protection des données strictement confidentielles

- Computacenter fonctionne selon le principe du *besoin d'en connaître* lorsqu'il traite des informations strictement confidentielles ;
- La Politique de bon usage de l'informatique et à la Matrice de classification et de traitement de l'information en vigueur au sein de Computacenter comprend des mesures spécifiques pour traiter les informations strictement confidentielles, y compris les exigences de chiffrement des documents ;
- La Politique de bon usage de l'informatique et à la Matrice de classification et de traitement de l'information indique quelles données personnelles sont considérées comme strictement confidentielles
- L'échange d'informations strictement confidentielles avec des tiers doit être effectué conformément à la matrice de classification et de traitement des informations de Computacenter ; et
- Le processus de gestion des risques, en collaboration avec les responsables et les gestionnaires des données, évalue et gère les risques associés aux données nécessitant une attention particulière.