Politique de Sécurisation des Données Repartim

VERSION 1.2 du 01/12/2023

Politique rédigée sous l'égide du comité décisionnel RSE de Repartim :

- *Martial Heland : Président*
- *Le Comité de Direction Repartim*
- *Alex Pierson : Responsable RSE*

Rédaction par :

- *Le service DSI*

Repartim
DÉPANNAGE & TRAVAUX DEPUIS 1967

Table des matières

Le périmètre lié à la sécurisation des données - Repartim

La sécurisation des données revêt une importance capitale pour Repartim, entreprise du bâtiment résolument tournée vers l'avenir. Notre engagement envers l'excellence dans tous les aspects de nos activités inclut également une vigilance sans faille quant à la protection des informations sensibles qui nous sont confiées.

Le périmètre de la sécurisation des données chez Repartim englobe l'intégralité du cycle de vie de l'information, depuis sa collecte initiale jusqu'à sa conservation et, le cas échéant, sa suppression sécurisée. Cela concerne tant les données générées par nos équipes internes que celles transmises par nos partenaires et clients. Notre politique s'étend également à la sécurité de l'infrastructure technologique qui soutient nos opérations.

Notre ambition : « Nous positionner comme un prestataire de confiance pour nos clients et partenaires, tout en assurant une protection rigoureuse et proactive des informations qui nous sont confiées. »

Cette politique engage toutes les agences Repartim situées sur l'ensemble du territoire français, tous les collaborateurs qui œuvrent au quotidien mais aussi tous nos partenaires, fournisseurs et sous-traitants avec lesquels nous souhaitons déployer une force commune dans l'amélioration de notre impact sociétal.

Ainsi, chaque employé, partenaire et intervenant impliqué dans l'écosystème de Repartim est appelé à jouer un rôle essentiel dans cette démarche collective de protection des données. Ensemble, nous érigeons un rempart impénétrable contre toute menace potentielle, renforçant ainsi la confiance de nos clients et partenaires envers notre professionnalisme et notre intégrité.

Nous considérons la conformité légale et normative comme un pilier fondamental de notre engagement envers la sécurisation des données. Chez Repartim, nous nous engageons à respecter scrupuleusement toutes les lois et réglementations locales, nationales et internationales relatives à la protection des données, telles que le Règlement Général sur la Protection des Données (RGPD) de l'Union Européenne. Nous veillons également à nous maintenir en conformité avec les normes de l'industrie, notamment la norme ISO 27001 pour la sécurité de l'information, et à rester à jour quant aux évolutions législatives dans le domaine de la sécurité des données. Cette démarche nous assure non seulement de respecter nos obligations juridiques, mais aussi de garantir la confiance et la tranquillité d'esprit à nos clients et partenaires, renforçant ainsi notre réputation d'intégrité et de fiabilité.

1. Responsabilités et Obligations

Chez Repartim, la sécurisation des données est une responsabilité partagée qui implique chaque membre de l'entreprise, depuis la direction jusqu'aux partenaires externes. Chaque entité a un rôle crucial à jouer pour garantir la protection et l'intégrité des informations sensibles.

1.1. Responsabilité de la Direction

La direction de Repartim s'engage à fournir un leadership éclairé en matière de sécurisation des données. Elle est responsable de définir les objectifs stratégiques liés à la protection des données et de mettre en place les ressources nécessaires pour les atteindre. Cela inclut l'allocation de budgets appropriés pour les technologies de sécurité, la formation du personnel et la mise en place de politiques et de procédures conformes aux réglementations en vigueur.

De plus, la direction doit également définir une culture d'entreprise qui valorise la sécurité des données, en favorisant la sensibilisation et l'engagement des employés dans cette démarche.

1.2. Responsabilité des Employés

Chaque employé de Repartim a la responsabilité individuelle de contribuer à la sécurisation des données. Cela commence par une sensibilisation constante aux bonnes pratiques en matière de sécurité, ainsi que par le respect des politiques et des procédures établies. Les employés doivent être vigilants quant à l'accès aux données sensibles et signaler tout comportement ou incident suspect à leur supérieur hiérarchique ou au service dédié à la sécurité de l'information.

En outre, ils doivent également suivre les formations régulières proposées par l'entreprise afin de se tenir informés des dernières menaces et des meilleures pratiques en matière de sécurisation des données.

1.3. Responsabilité des Partenaires Externes

Les partenaires externes jouent un rôle essentiel dans l'écosystème de Repartim. Ils sont tenus de respecter les mêmes normes élevées en matière de sécurisation des données que celles appliquées en interne. La direction de Repartim s'assure que les contrats avec les partenaires intègrent des clauses spécifiques concernant la protection des données et que ces derniers soient en conformité avec les réglementations en vigueur.

2. Classification des Données

La classification des données est un élément crucial de notre politique de sécurisation des données chez Repartim. Elle nous permet de mieux comprendre la nature et la sensibilité des informations que nous traitons, ce qui nous guide dans la mise en place de mesures de sécurité appropriées.

2.1. Données Sensibles

Les données sensibles englobent toute information qui, si elle était divulguée, pourrait causer un préjudice sérieux à notre entreprise ou à nos parties prenantes. Cela inclut, par exemple, les données financières confidentielles, les stratégies commerciales en cours de développement, les accords contractuels et les informations sur nos clients et partenaires.

La manipulation de ces données requiert une vigilance particulière. Elles doivent être stockées de manière sécurisée, avec un accès restreint uniquement aux personnes autorisées. De plus, leur transmission doit être cryptée et leur destruction doit suivre des procédures strictes.

2.2. Données Non Sensibles

Les données non sensibles sont des informations qui ne comportent pas de risques significatifs pour notre entreprise ou nos parties prenantes en cas de divulgation. Il peut s'agir, par exemple, de documents publics, de brochures d'information générale ou de matériaux promotionnels.

Bien que ces données ne nécessitent pas le même niveau de protection que les données sensibles, elles doivent néanmoins être traitées avec soin et conformément à notre politique de sécurisation des données.

2.3. Données Personnelles

Les données personnelles se réfèrent aux informations liées à des individus identifiés ou identifiables. Cela englobe les noms, les adresses, les numéros de téléphone, les adresses électroniques et d'autres éléments d'identification personnelle. Étant donné la sensibilité de ces données et pour respecter les réglementations telles que le RGPD, nous nous engageons à obtenir le consentement explicite des individus avant de collecter, traiter ou stocker leurs données personnelles.

De plus, ces données doivent être traitées de manière sécurisée et leur accès doit être restreint aux seules personnes autorisées, garantissant ainsi la protection de la vie privée de nos clients et partenaires.

2.4. Propriété Intellectuelle

La propriété intellectuelle comprend nos créations originales, telles que les dessins, les plans, les modèles et les brevets. Ces éléments sont des actifs précieux pour Repartim, et leur protection est essentielle pour maintenir notre avantage concurrentiel.

Nous mettons en place des mesures de sécurité spécifiques pour préserver la confidentialité et l'intégrité de notre propriété intellectuelle. Cela inclut des accès restreints, des procédures de partage sécurisées et la sensibilisation de nos équipes à l'importance de protéger ces actifs.

La classification précise des données garantit que chaque type d'information est traité avec les précautions appropriées, renforçant ainsi la sécurité et la confidentialité des informations au sein de Repartim.

3. Collecte et Traitement des Données

La collecte et le traitement des données sont des phases cruciales dans la gestion des informations au sein de Repartim. Elles nécessitent une approche réfléchie et respectueuse de la confidentialité et de l'intégrité des données.

3.1. Consentement de la Collecte des Données

La collecte de données débute toujours par l'obtention du consentement explicite des individus concernés. Que ce soit pour nos clients, partenaires ou employés, nous nous engageons à obtenir leur autorisation préalable avant de collecter leurs données personnelles. Cette transparence renforce la confiance et garantit que chaque individu est pleinement informé de la finalité de la collecte.

- Nous mettons également à disposition des canaux de communication clairs et accessibles pour permettre à tout individu de retirer son consentement à tout moment.

  Cf. ***Charte Vie Privée***, Repartim (https://www.repartim.fr/informations-personnelles/)

3.2. Limitation de la Collecte

Chez Repartim, nous adhérons au principe de collecte minimale. Cela signifie que nous ne collectons que les données strictement nécessaires pour atteindre les objectifs spécifiés. Cette approche préserve la vie privée des individus et réduit le risque associé à la conservation de données inutiles.

- Nous formons nos équipes à évaluer soigneusement quelles données sont réellement requises pour chaque processus ou projet, et à s'assurer que seules celles-ci sont collectées et traitées.

3.3. Transparence dans le Traitement des Données

La transparence est un principe fondamental dans notre démarche de collecte et de traitement des données. Nous nous engageons à informer clairement les individus concernés sur la manière dont leurs données seront utilisées, traitées et stockées. Nous mettons à leur disposition des informations détaillées sur les finalités du traitement, les destinataires éventuels et les mesures de sécurité mises en place.

- De plus, nous sommes disponibles pour répondre à toute question ou préoccupation concernant le traitement des données, afin d'assurer une compréhension totale et une confiance mutuelle entre Repartim et les parties prenantes.

4. Stockage et Conservation des Données

La sécurité et la durabilité du stockage ainsi que la gestion appropriée de la conservation des données sont des piliers cruciaux de la politique de sécurisation des données chez Repartim. Nous mettons en place des pratiques robustes pour garantir l'intégrité et la disponibilité des informations à long terme.

4.1. Sécurité des Locaux et des Équipements

- Les locaux de Repartim sont sécurisés de manière à empêcher tout accès non autorisé. Des systèmes de contrôle d'accès, des caméras de surveillance et des alarmes sont en place pour protéger nos installations contre tout risque d'intrusion ou d'accès non autorisé.
- De plus, nos serveurs et équipements informatiques sont hébergés dans des centres de données sécurisés, répondant aux normes de sécurité les plus strictes de l'industrie.

La surveillance constante et les procédures d'urgence garantissent la protection des données physiques contre tout risque de perte, de vol ou de dommage.

4.2. Gestion des Archives Physiques et Électroniques

- La gestion des archives, qu'elles soient physiques ou électroniques, est effectuée de manière méthodique et organisée. Les documents physiques sont conservés dans des espaces sécurisés, sous clé et à l'abri de l'humidité et des intempéries. Un système de classification clair permet de localiser rapidement les archives lorsque nécessaire.

- Les données électroniques sont stockées sur des serveurs sécurisés, avec des mesures de protection avancées telles que le cryptage et les pare-feu. De plus, des procédures de sauvegarde régulières sont mises en place pour éviter toute perte de données due à des incidents techniques.

4.3. Durée de Conservation des Données

- La durée de conservation des données est établie en fonction des exigences légales et des besoins opérationnels de Repartim. Les données sont conservées le temps nécessaire pour atteindre les finalités pour lesquelles elles ont été collectées. Une fois cette période atteinte, les données sont soigneusement supprimées de manière sécurisée, conformément à nos procédures de destruction de données.
- Nous veillons à ce que cette durée de conservation soit régulièrement réévaluée pour garantir que nous ne conservons que les données essentielles à nos activités et en conformité avec la législation en vigueur. Cette approche nous permet de garantir la confidentialité et l'intégrité des informations tout au long de leur cycle de vie.

Cf. ***Charte Vie Privée***, Repartim (https://www.repartim.fr/informations-personnelles/)

5. Sécurité Informatique

La sécurité informatique est un élément essentiel de la politique de sécurisation des données chez Repartim. Nous mettons en œuvre des mesures de protection avancées pour garantir l'intégrité et la confidentialité de nos informations numériques.

5.1. Accès et Authentification

- L'accès aux systèmes et aux données est strictement contrôlé et limité aux seules personnes autorisées. Chaque utilisateur dispose d'identifiants uniques et de droits d'accès spécifiques en fonction de son rôle au sein de l'entreprise. Les accès sont régulièrement révisés et ajustés en fonction des besoins opérationnels et des changements dans les responsabilités des employés.

5.2. Gestion des Mots de Passe

- Une politique de gestion des mots de passe robuste est en place pour garantir leur complexité et leur confidentialité. Les employés sont tenus de choisir des mots de passe forts et de les mettre à jour régulièrement comme énoncé dans les propositions de l'ANSSI. En outre, l'utilisation de l'authentification à deux facteurs est encouragée pour renforcer la sécurité des comptes.

5.3. Cryptage des Données

- Toutes les données sensibles qui sortent du réseau interne sont systématiquement cryptées, que ce soit en transit ou au repos. Cette mesure de sécurité essentielle garantit que même en cas d'accès non autorisé, les informations demeurent illisibles et inutilisables.

5.4. Pare-feu et Antivirus

- Nous déployons des pare-feu et des logiciels antivirus de pointe pour protéger nos systèmes contre les menaces externes. Ces outils sont continuellement mis à jour pour assurer une défense efficace contre les virus, les logiciels malveillants et les attaques en ligne.

5.5. Mises à Jour Régulières

- Les mises à jour de sécurité sont appliquées de manière proactive pour garantir que nos systèmes bénéficient des derniers correctifs et correctifs de sécurité. Cela inclut non seulement les logiciels et applications, mais aussi les systèmes d'exploitation, les serveurs et les équipements réseau.

En adoptant ces mesures de sécurité informatique, Repartim renforce sa capacité à protéger ses données contre les menaces numériques en constante évolution, garantissant ainsi la sécurité et la confidentialité de nos informations numériques.

6. Gestion des Incidents de Sécurité

La gestion des incidents de sécurité est un aspect crucial de notre politique de sécurisation des données chez Repartim. Elle vise à minimiser les impacts en cas de faille de sécurité et à rétablir rapidement l'intégrité de nos systèmes et données.

6.1. Procédure de Signalement des Incidents

Tout employé de Repartim est tenu de signaler immédiatement tout incident de sécurité suspecté ou avéré. Pour ce faire, nous avons mis en place un canal de signalement dédié, accessible en interne et permettant de décrire en détail l'incident. Cette procédure garantit une réponse rapide et efficace face à toute menace potentielle.

6.2. Enquête et Documentation des Incidents

- Une fois l'incident signalé, une équipe dédiée est mobilisée pour mener une enquête approfondie. Cette équipe externe, composée d'experts en sécurité de l'information, analyse les détails de l'incident, détermine l'origine de la faille et évalue les dommages potentiels. Toutes les étapes de cette enquête sont soigneusement documentées pour une analyse post-incident et pour la mise en place de mesures correctives.

6.3. Notification des Parties Concernées

- En cas d'incident de sécurité susceptible d'entraîner une atteinte à la vie privée ou à la sécurité des données de nos parties prenantes, nous nous engageons à les informer dans les plus brefs délais. Cette notification sera effectuée de manière transparente, en fournissant des informations claires sur la nature de l'incident, les mesures prises pour remédier à la situation et les recommandations éventuelles à suivre.
- Nous nous engageons à être proactifs et transparents dans notre communication, démontrant ainsi notre engagement envers la protection des données de nos clients, partenaires et employés.

En mettant en œuvre ces procédures de gestion des incidents de sécurité, Repartim se dote des outils nécessaires pour faire face à toute situation critique, garantissant ainsi la préservation de l'intégrité et de la confidentialité de nos données.

7. Formation et Sensibilisation

La formation et la sensibilisation jouent un rôle essentiel dans la politique de sécurisation des données chez Repartim. Elles visent à garantir que chaque membre de notre organisation comprend et applique les meilleures pratiques en matière de sécurité des données.

7.1. Sensibilisation à la Sécurité des Données

La sensibilisation à la sécurité des données est un élément clé pour créer une culture d'entreprise axée sur la protection des informations.

- Nous organisons régulièrement des sessions de sensibilisation pour familiariser notre personnel avec les risques potentiels liés à la sécurité des données et les bonnes pratiques à adopter.

  Ces sessions mettent en lumière les menaces actuelles, les techniques d'ingénierie sociale, les pratiques de phishing et les moyens de prévenir de telles attaques. Elles rappellent également l'importance de la vigilance et du respect des procédures de sécurité établies.

- En 2023, 100% des collaborateurs administratifs ont été testés au phishing et environ 12% de ces derniers ont été sensibilisés par nos équipes DSI après être tombés dans le piège.

7.2. Formation Régulière du Personnel

La formation régulière du personnel est cruciale pour maintenir un niveau élevé de sensibilisation et de compétence en matière de sécurité des données.

- Nous imaginons des programmes de formation adaptés aux différents niveaux de l'organisation, avec des modules spécifiques pour les employés, les gestionnaires et les équipes IT. Nous prévoyons un premier programme e-learning sur la sécurisation des données pour 2024.

Ces formations abordent des sujets tels que la gestion des mots de passe, la protection contre les logiciels malveillants, la manipulation sécurisée des données sensibles et les procédures d'urgence en cas d'incident de sécurité. Elles permettront à notre personnel d'acquérir les compétences nécessaires pour contribuer activement à la protection de nos données.

En investissant dans la formation et la sensibilisation, Repartim s'assure que chaque membre de notre équipe est un maillon fort de la chaîne de sécurité des données, renforçant ainsi la protection de nos informations sensibles.

L’engagement de Repartim

Un mot du Président

Chers collaborateurs,

Je tiens à prendre un moment pour vous parler d'un sujet d'une grande importance pour notre entreprise : la sécurisation des données. En cette ère où l'information est une ressource précieuse, il est de notre devoir de la protéger avec la plus grande rigueur.

Aujourd'hui, je m'engage formellement envers vous et envers nos parties prenantes à mettre en œuvre et à respecter rigoureusement notre nouvelle Politique sur la sécurisation des données. Cette politique n'est pas seulement un document, c'est un engagement envers la confiance que vous nous accordez chaque jour.

Je vous appelle à vous engager avec moi dans cette démarche. Chacun de nous, quel que soit notre rôle au sein de l'entreprise, a un rôle crucial à jouer. Que ce soit en respectant les procédures établies, en signalant tout incident de sécurité ou en participant activement à nos programmes de formation, nous sommes tous acteurs de la sécurité de nos données.

En adoptant cette politique, nous renforçons la confiance de nos clients et partenaires, et nous nous positionnons en tant qu'entreprise responsable et fiable. Ensemble, nous formons une équipe engagée dans la protection de notre patrimoine le plus précieux : nos données.

Je vous remercie pour votre dévouement envers Repartim et pour votre engagement envers la sécurisation de nos informations. Ensemble, nous sommes plus forts.

Avec toute ma confiance,

Martial HELAND
Président de Repartim