Leads événementiels

Le point aveugle de la cybersécurité

ÉTAT DES LIEUX
ET BONNES PRATIQUES

kayo

Sécuriser la collecte, la circulation et l'exploitation des données prospects ?

Salons, conférences, événements clients ou partenaires : les événements sont devenus un pilier de la génération de leads en B2B.

En quelques heures, une entreprise peut collecter des centaines de contacts qualifiés.

Mais derrière cette performance marketing se cache une réalité souvent sous-estimée :
les données collectées lors des événements circulent dans des écosystèmes numériques complexes et rarement sécurisés.

Plateformes SaaS, applications mobiles, scanners de badges, CRM, outils d'automatisation marketing…

Chaque étape introduit des risques de sécurité et de conformité.

Ce guide propose :

Une analyse du cycle de vie des leads événementiels

Une identification des risques cyber et réglementaires

Un cadre pour sécuriser la gestion de ces données

kayo

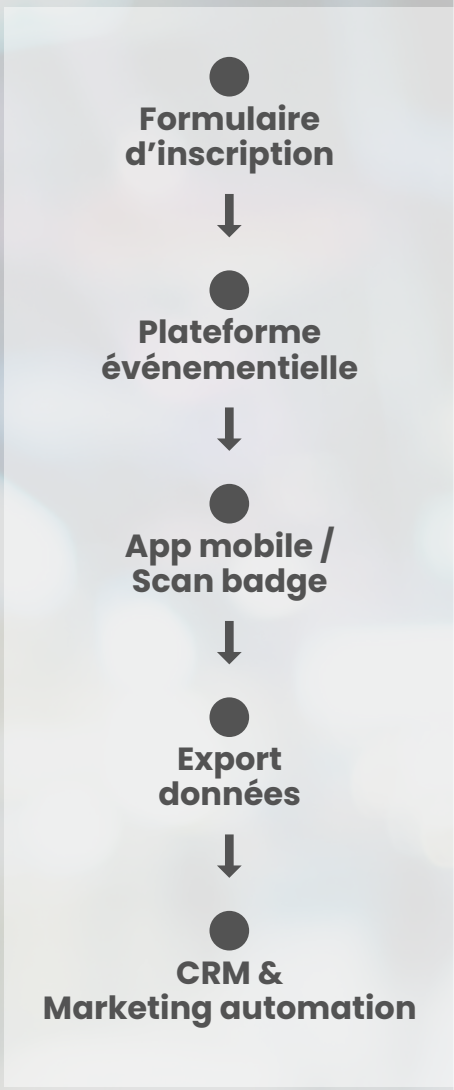
L’écosystème numérique de l’événementiel

La gestion d’un événement repose aujourd’hui sur un ensemble d’outils numériques interconnectés.

On retrouve généralement :

- **une plateforme d’inscription**
- **une application événementielle**
- **un système de gestion des badges**
- **un outil de scan de leads**
- **un CRM**
- **un outil marketing automation**

Ces outils échangent des données en permanence.



Un simple scan de badge peut déclencher :

1. **La récupération des informations du participant**
2. **Leur stockage dans la plateforme événementielle**
3. **Leur export vers le CRM**
4. **Leur exploitation dans des campagnes marketing**

Ce fonctionnement repose sur des flux de données multiples, souvent mal documentés.

Lorsque ces flux ne sont pas maîtrisés, les entreprises peuvent perdre le contrôle de leurs données prospects.

Les données circulent alors entre plusieurs acteurs sans cadre clair : organisateurs, agences, prestataires techniques, équipes marketing et commerciaux.

kayo

Le cycle de vie d'un lead événementiel

Pour sécuriser les données, il est essentiel de comprendre leur cycle de vie.

1. Collecte

Les données sont collectées via :

- formulaires d'inscription
- scans de badges
- applications mobiles

2. Centralisation

Les informations sont stockées dans la plateforme utilisée pour gérer l'événement.

3. Enrichissement

Les données peuvent être complétées avec des informations supplémentaires :

- qualification commerciale
- scoring marketing
- segmentation

4. Intégration

Les leads sont ensuite transférés vers le CRM ou les outils marketing.

5. Exploitation

Les équipes marketing et commerciales utilisent ces données pour :

- envoyer des communications
- déclencher des actions commerciales
- alimenter le pipeline.

6. Conservation ou suppression

Les données doivent être conservées pour une durée limitée.
Chaque étape introduit des enjeux de sécurité et de gouvernance des données.

Pourquoi ces données sont sensibles ?

Plusieurs situations fréquentes peuvent exposer les données collectées lors d'événements.

Les leads événementiels contiennent plusieurs types d'informations :

- données personnelles (nom, email, téléphone)
- données professionnelles (poste, entreprise)
- données comportementales (intérêt pour un produit, participation à un atelier)

Ces données peuvent être utilisées pour :

- **Cibler des prospects**
- **Identifier des opportunités commerciales**
- **Analyser les comportements des visiteurs**

Dans certains cas, elles peuvent révéler des informations stratégiques sur les projets d'une entreprise.

C'est pourquoi ces données doivent être protégées de la même manière que d'autres informations sensibles.

Les risques spécifiques aux leads événementiels

Plusieurs facteurs rendent ces données particulièrement vulnérables.

Solutions organisateurs

Les solutions événementielles sont souvent hébergées dans le cloud et gérées par des prestataires externes, souvent les organisateurs des événements.

Circulation rapide des données

Les leads peuvent être exportés et partagés entre plusieurs équipes.

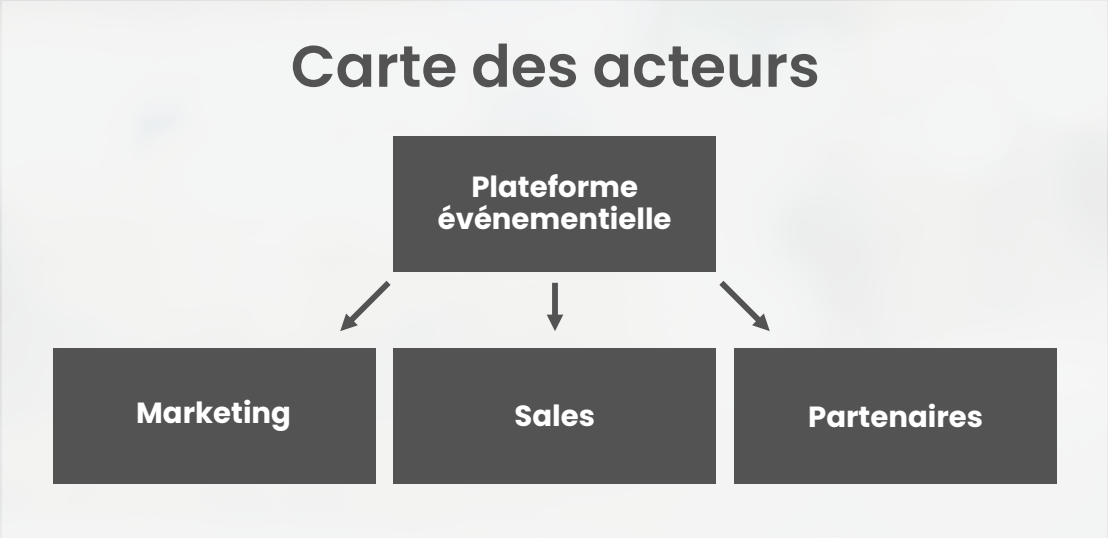
Accès multiples

Les utilisateurs impliqués peuvent inclure :

- marketing
- commerciaux
- agences
- partenaires

Absence de gouvernance

Dans de nombreuses organisations, ces flux ne sont pas intégrés dans la stratégie globale de gestion des données.



RGPD et gestion des données événementielles

Rappel sur la réglementation

Le RGPD impose plusieurs obligations pour la collecte et le traitement des données personnelles.

Transparence

Les participants doivent être informés de l'utilisation de leurs données.

Base légale

La collecte doit reposer sur :

- le consentement
- ou l'intérêt légitime.

Minimisation des données

Seules les informations nécessaires doivent être collectées.

Durée de conservation

Les données ne peuvent pas être conservées indéfiniment.

Droits des personnes

Les participants doivent pouvoir :

- accéder à leurs données
- demander leur suppression.

La conformité RGPD implique également de **contrôler les sous-traitants** impliqués dans la gestion des données.

IAM | Contrôler les accès aux données

L'Identity and Access Management (IAM) permet de contrôler qui peut accéder aux données et aux systèmes.

Dans le contexte événementiel, cela implique :

- **Attribuer des accès différents selon les rôles**
- **Limiter les droits d'accès aux données sensibles**
- **Tracer les actions réalisées sur les systèmes**

Exemples :

Un commercial peut accéder uniquement aux leads qu'il a collectés.
Un administrateur marketing peut accéder à l'ensemble des données.

L'IAM permet d'éviter les situations où tout le monde peut accéder à toutes les données.

kayo

PAM | Sécuriser les accès administrateurs

Les comptes administrateurs représentent un risque important.

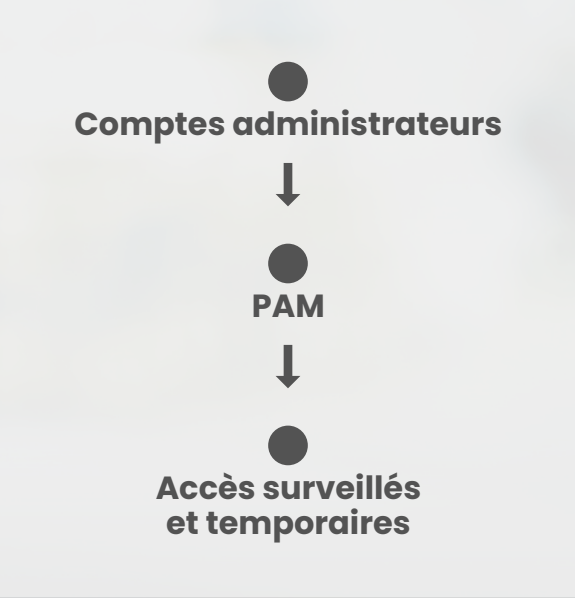
Ils permettent souvent :

- d'exporter l'ensemble des leads
- de modifier les paramètres de sécurité
- d'accéder à toutes les données.

Le Privileged Access Management (PAM) permet de sécuriser ces accès.

Il repose sur plusieurs principes :

- **Limitation des comptes administrateurs**
- **Authentification renforcée**
- **Journalisation des actions**
- **Accès temporaires**



Cela permet de réduire les risques liés à une utilisation abusive ou à la compromission de comptes.

kayo

Sécuriser les plateformes SaaS

Les solutions événementielles sont souvent fournies sous forme de services SaaS.

Cela signifie que les données sont hébergées par un prestataire externe.

Avant de choisir une solution, plusieurs éléments doivent être évalués :

- **Localisation des données**
- **Certification de sécurité**
- **Gestion des accès**
- **Capacités d'audit**

Les entreprises doivent également s'assurer que leurs prestataires respectent les exigences du RGPD.

Il est également important de bien comprendre le modèle de responsabilité partagée : le prestataire sécurise l'infrastructure, mail l'entreprise reste responsable de la configuration et des usages.

Une attention particulière doit être portée aux intégrations entre outils (API, connecteurs) :

- Limiter les permissions accordées
- Sécuriser les clés d'accès
- Surveiller les flux de données échangés

Enfin, les aspects contractuels ne doivent pas être négligés :

- Clauses en cas de violation de données
- Conditions de restitution des données (réversibilité)
- Transparence sur les sous-traitants utilisés

Une plateforme unique comme KAYO, intégrant l'ensemble des étapes (de la collecte à l'intégration CRM), permet de réduire le nombre de prestataires impliqués et donc les risques liés à la multiplication des points de vulnérabilité.

Gouvernance des données marketing

La sécurité des données marketing repose sur une gouvernance claire.

Cela implique notamment :

Une cartographie des flux de données

Des règles d'accès

Des procédures d'export

Une politique de conservation.

Cette gouvernance doit être définie conjointement par :

Les équipes marketing

Les équipes IT

Les responsables de la conformité

La définition des rôles est essentielle pour éviter les zones de flou :

- Qui est responsable des données collectées ?
- Qui valide leur utilisation ?
- Qui gère la suppression ?

La cartographie des flux doit être maintenues dans le temps, notamment lors de l'ajout de nouveaux outils ou partenaires.

Il est également recommandé de formaliser des règles d'usage des données :

- Types de segmentations autorisées
- Conditions d'utilisation en campagnes
- Limites dans le croisement de données

Une gouvernance efficace repose autant sur des règles que sur leur adoption par les équipes

Architecture cible sécurisée

Une gestion sécurisée des leads repose sur une architecture claire.

Collecte

↓

Plateforme événementielle

↓

Contrôle des accès

↓

CRM

↓

Marketing automation

Les données doivent circuler via des flux contrôlés et non par des exports manuels.

Il est recommandé de limiter la multiplication des copies de données entre outils afin de conserver un référentiel fiable.

Les échanges doivent être automatisés via des connecteurs sécurisés plutôt que réalisés manuellement (fichiers Excel, CSV), souvent sources de risques.

Chaque flux de données doit être traçable

- Qui envoie les données ?
- Vers quel système ?
- À quel moment ?

La séparation des environnements (production, test) permet d'éviter l'exposition de données réelles dans des contextes non sécurisés.

Bonnes pratiques

Pour sécuriser la gestion des leads événementiels :

Limiter les exports manuels

Définir des rôles d’accès

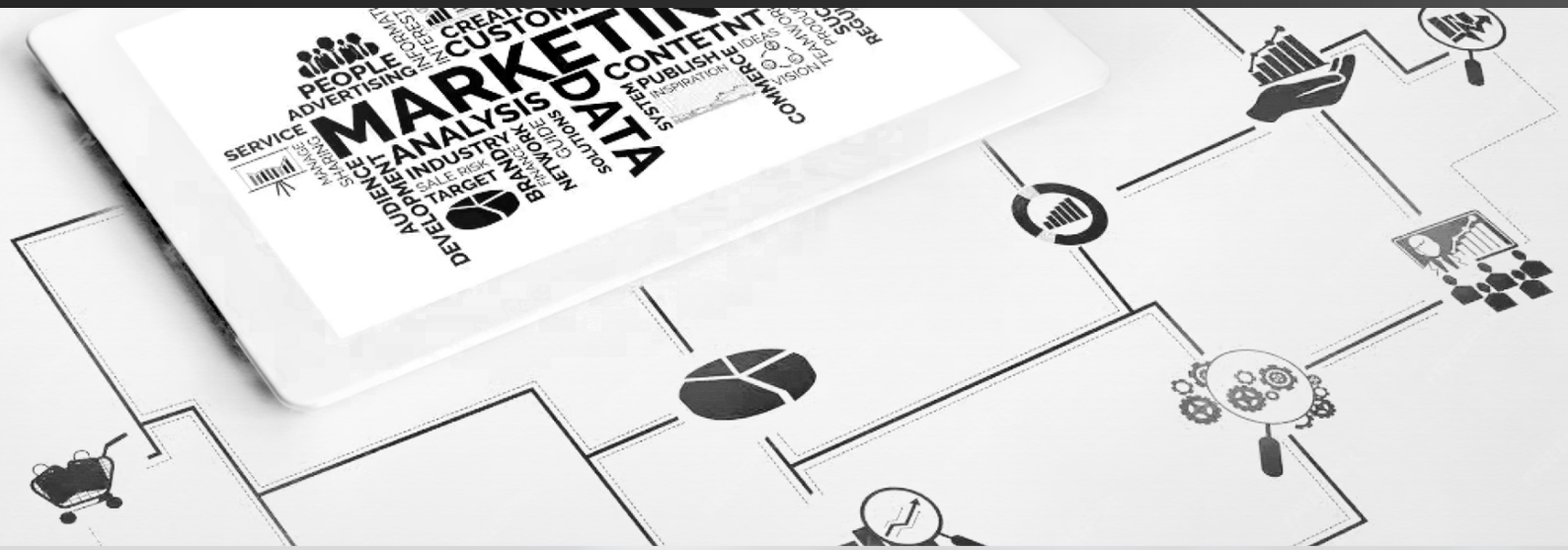
Utiliser des outils conformes au RGPD

Sécuriser les comptes administrateurs

Définir une durée de conservation.

Bien choisir ses solutions SaaS

Vers un marketing sécurisé



Les données marketing sont devenues un actif stratégique.

Les organisations qui sécurisent leur gestion des leads bénéficient de plusieurs avantages :

- **Meilleure qualité des données**
- **Réduction des risques réglementaires**
- **Confiance renforcée des prospects**

La sécurité des données devient progressivement un élément de différenciation, notamment dans les contextes B2B où les exigences de conformités sont élevées.

Une meilleure gestion des données permet également d'améliorer la performance opérationnelle :

- Ciblage plus précis
- Réduction des doublons
- Campagnes plus efficaces

Enfin, dans un contexte d'évolution des usages (automatisation, IA, exploitation avancée de la DATA), disposer de données fiables, traçables et bien gouvernées devient indispensable.

kayo

Conclusion

La cybersécurité ne concerne plus uniquement les systèmes informatiques.

Elle concerne désormais l'ensemble des données utilisées par l'entreprise, y compris celles collectées lors des événements.

En structurant la gouvernance des leads événementiels, les entreprises peuvent concilier :

- **Performance marketing**
- **Sécurité des données**
- **Conformité réglementaire**

Pour aller plus loin et renforcer la protection de vos données événementielles, notre solution SaaS centralisée et souveraine peut vous aider à tendre vers une sécurité optimale.

Prenez rendez-vous dès maintenant avec notre équipe pour explorer les bénéfices concrets d'une telle approche.

Prendre rendez-vous