

Smart City Data Privacy Guidelines

To protect personal privacy and ensure responsible data use in smart cities, follow these principles.

1 Transparent Data Collection

- Clearly inform citizens about what data is collected and why.
- Obtain consent for collecting personal data when required.
- Minimize data collection to what is strictly necessary.

2 Secure Data Storage and Transfer

- Encrypt data during storage and transmission.
- Use secure servers with regular security updates.
- Limit data access to authorized personnel only.

3 Anonymization and Minimization

- Anonymize personal identifiers whenever possible.
- Retain data only for the duration needed for its purpose.
- Avoid collecting sensitive data unless essential.

4 Responsible Data Sharing

- Share data only with trusted and approved entities.
- Require partners to comply with the same privacy standards.
- Keep records of all data-sharing activities.

5 Citizen Control and Access

- Provide mechanisms for individuals to view, correct, or delete their data.
- Allow opt-out from non-essential data collection.
- Ensure that privacy rights are easy to exercise.

6 Legal Compliance and Auditing

- Follow relevant privacy laws and international standards.
- Conduct regular audits to ensure data protection compliance.
- Maintain a clear breach response and notification plan.

7 Ethical Use of AI and Analytics

- Avoid bias in algorithms used for city management.
- Use AI responsibly, focusing on public benefit and fairness.
- Disclose the use of automated decision-making systems.

By applying these guidelines, smart cities enhance trust and protect citizens' rights while advancing technology and services.

1

2

3

4

5

6

7

A

1

2

3

4

5

6

7

Guía de Privacidad de Datos para Ciudades Inteligentes

Para proteger la privacidad personal y garantizar el uso responsable de los datos en ciudades inteligentes, siga estos principios:

1 Recolección Fina y Justificada de Datos

- **Identifique las razones claras de la recolección y su propósito.**
- **Otorga consentimiento informado y explícito.**
- **Límitela a la recolección de datos al estrechamente necesario.**

2 Almacenamiento y Transferencia Seguros

- **Guarde los datos durante el almacenamiento y la transmisión.**
- **Use servicios seguros con actualizaciones frecuentes.**
- **Límite el acceso a los datos a personas autorizadas.**

3 Autorización y Minimización

- **Autorice la información personal siempre que sea posible.**
- **Conservelos datos solo el tiempo necesario.**
- **Elimine o aplique datos sensibles si no es imprescindible.**

4 Uso Responsable de Datos Compartidos

- **Comparta datos solo con entidades confiables y autorizadas.**
- **Ejija que los socios cumplen normas estrictas de privacidad.**
- **Mantenga registros detallados de las actividades de intercambio de datos.**

5 Control y Acceso Ciudadano

- **Ofrezca canales sencillos para que las personas consulten conjuntamente sus datos.**
- **Permita y facilite la rectificación de datos no esenciales.**
- **Facilite el ejercicio de los derechos de privacidad.**

6 Cumplimiento Legal y Auditoría

- **Cumpla las leyes de privacidad y estándares internacionales.**
- **Realice auditorías periódicas para asegurar la protección de datos.**
- **Tenga una plena documentación y especificación de todas las políticas.**

7 Tratamiento de Datos y Análítica

- **Evite sesgos en los algoritmos de gestión urbana.**
- **Ofrece la API al público beneficiario y con equidad.**
- **Evite la dependencia de sistemas de decisión automatizados.**

Aplicar estas directrices refuerza la confianza y protege los derechos de los residentes.

Guide de Confidentialité des Données pour les Villes Intelligentes

Pour protéger la vie privée et garantir une utilisation responsable des données dans les villes intelligentes, appliquez ces principes

1 Collecte Transparente des Données

- Informez clairement les citoyens sur les données collectées et leur usage
- Obtenez le consentement lorsque cela est requis
- Limitez la collecte aux données strictement nécessaires

2 Stockage et Transmission Sécurisés

- Chiffrez les données en stockage et en transit
- Utilisez des serveurs sécurisés mis à jour régulièrement
- Restreignez l'accès aux données au personnel autorisé

3 Anonymisation et Minimisation

- Anonymisez les informations personnelles lorsque c'est possible
- Ne conservez les données que pour la durée strictement nécessaire
- Évitez de collecter des données sensibles sauf nécessité

4 Partage Responsable des Données

- Partagez uniquement avec des partenaires fiables et approuvés
- Exigez des partenaires qu'ils respectent les mêmes normes de confidentialité
- Conservez un registre des partages de données

5 Contrôle et Accès des Citoyens

- Permettez aux individus de consulter, corriger ou supprimer leurs données
- Offrez une option de refus pour les collectes non essentielles
- Facilitez l'exercice des droits liés à la vie privée

6 Conformité Légale et Audits

- Respectez les lois sur la protection des données et les standards internationaux
- Réalisez des audits réguliers pour garantir la conformité
- Préparez un plan d'air de réponse aux violations de données

7 Usage Éthique de l'IA et de l'Analyse

- Évitez les biais dans les algorithmes de gestion urbaine
- Employez l'IA pour l'intérêt public et l'équité
- Divulguez l'utilisation des systèmes de décision automatisés

Ces recommandations renforcent la confiance des citoyens et protègent leurs droits

1

2

3

4

5

6

7