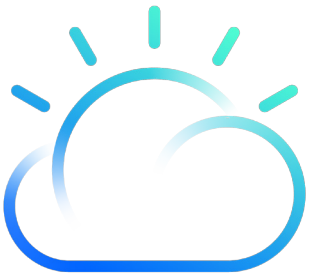


WHITE PAPER

# Understanding GDPR For Ad Tech

## A guide to IBM Cloud's commitment to data privacy and protection requirements

## EXECUTIVE SUMMARY

If your company or organization does business within the European Union (EU), then you'll need to understand the EU General Data Protection Regulation (GDPR). This regulation takes effect on May 25, 2018 and is a series of important changes to data privacy rules.

IBM

# What is the GDPR?

GDPR creates both harmonized data protection and a privacy framework across the EU. It returns control of personal data to the data subjects. “Data subjects” are defined as natural living persons who are residents, citizens, visitors, or employees in the EU.

The key provisions of the GDPR include:

- Tighter consent conditions for the collection of personal data
- Power to consumers to instruct companies to stop processing their data
- Required clarity in automated decision-making and profiling decisions
- Right to request cessation of automated processes
- Right to request automated processes be handled by a human
- Right to request an explanation of automated decision-making
- Right to request free access, rectification, and deletion of data

According the GDPR’s Recital 30, most cookies collect personal data. As a result, cookie usage policies must be part of your GDPR readiness plan. Opt-in for cookie consent must be clear. If not, first-time site visitors are blocked until a user action indicates clear consent to the sent cookies.

For each instance of noncompliance, an organization or company could be fined up to €20 million or 4 percent of worldwide annual turnover (revenue)—whichever is higher. Regulators may also impose stop-processing orders.

Ad tech companies that do not comply with GDPR may also face indirect negative impact on brand reputation. Before your organization sends data via an API to another service, make sure there is a basic level of data protection. If they don’t, raise a flag.

# Who is affected by GDPR?

The GDPR impacts more than just organizations across Europe. Any business anywhere with personal data from EU data subjects must abide by the regulation.

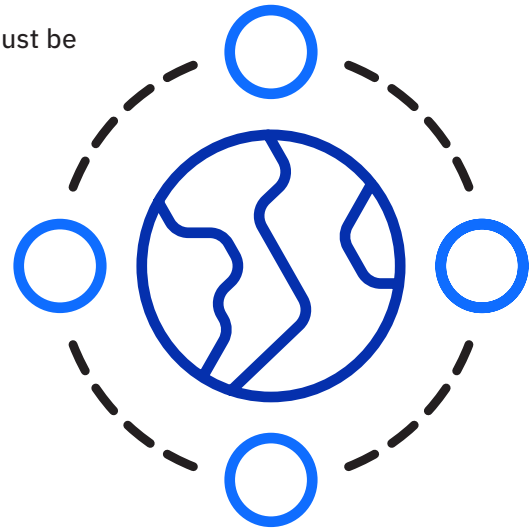
This includes, but is not limited to:

- **Controllers**: Determine the purpose and means of processing of personal data and are liable for breaches
- **Processors**: Process personal data on behalf of a controller only and are liable for breaches
- **Marketers**: Must reconnect with customers to ensure that consent statements (or other methods for collecting personal data) are compliant

## Ad tech and the GDPR

Ad tech companies must never assume that third parties are compliant with the GDPR and must follow instructions to assure GDPR compliance:

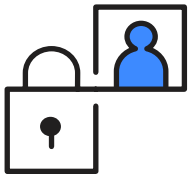
- Advertisers must secure explicit and informed consent from EU data subjects.
- Brands must obtain user consent without using pre-checked boxes.
- All relationships, transactions, and data flows must be transparent, documented, and auditable.



# IBM Cloud and the GDPR

IBM Cloud is one of the first companies to adopt the EU Data Protection Code of Conduct for Cloud Service Providers. Companies that adopt the Code agree to meet its stringent requirements.

IBM Cloud puts data responsibility and security first every day. In consideration of the GDPR, IBM Cloud follows these basic tenets:



## Data ownership and privacy

IBM Cloud was an early leader in developing and adopting the EU Data Protection Code of Conduct for Cloud Service Providers for several offerings, securing certification under the U.S.-EU Privacy Shield and the APEC Cross-Border Privacy Rules.

IBM Cloud is fully committed to protecting the privacy of data—a fundamental component of a data-driven society.

## Data security

Securing the Internet of Things (IoT)—including all data, communications, and processing associated with these systems—is achieved if the design puts data security and privacy first.

# GDPR-compliant cloud offerings for ad tech companies

*IBM Cloud makes it easy for ad tech companies to comply with the GDPR.*

## Infrastructure-as-a-Service

**→ Expansive IBM Cloud data center network**

Ease data residency concerns with a growing network of almost 20 cloud data centers across Europe: The Netherlands, Germany, England, Italy, Norway, and France. Physical access to the data center is controlled by authorized IBM Cloud associates via proximity badge and biometric access.

**→ IBM Cloud bare metal servers**

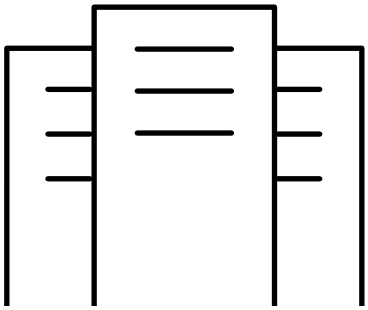
IBM Cloud offers bare metal servers on demand in a single tenant environment—meaning no shared resources, no access to your data, and root access to the server. IBM Cloud also offers complete transparency to your server down to the rack level.

**→ IBM Cloud secure virtualization**

Specifically geared toward clients in highly regulated industries, IBM Cloud secure virtualization gives enterprises control over where their data is located to address performance, security, and data privacy needs.

With IBM Cloud Secure Virtualization, clients benefit from:

- Accurate data location
- Verified boundary control
- Additional geo-fencing
- Smarter, faster decryption



**→ Firewall, IDS/IPS (Vyatta, Fortigate)**

Setting up firewall-based rules for region blocking.

## GDPR-compliant cloud offerings for ad tech companies *(continued)*

### Platform-as-a-Service

**→ IBM Geospatial Analytics for IBM Cloud**

Leverage real-time geospatial analytics to track when devices enter, leave, or hang out in defined regions.

### Consulting

**→ IBM Cloud Data Privacy Services**

Establish policies that govern the way your organization gathers and manages data to reduce risks and meet global privacy goals.

### Security

**→ IBM Security Identity Governance and Intelligence**

A business-centric approach to identity management and governance. It empowers business and IT to work together to address regulatory compliance and security goals across enterprise applications and data.

**→ IBM Guardium Data Protection for Databases**

Provides automated sensitive data discovery and classification, real-time data activity monitoring, and cognitive analytics to discover irregular activity around sensitive data.

**→ IBM Key Protect**

Cloud-based security service that provides life cycle management for encryption keys that are used in IBM Cloud services or customer-built applications.

**→ IBM Data Risk Manager**

Helps organizations proactively protect against data-related business risks.

**→ IBM Multi-Cloud Data Encryption**

Safeguards data from misuse whether it resides in single cloud, multiple clouds, or hybrid environments with encryption capabilities.

**→ IBM Security Key Lifecycle Manager**

Centralize, simplify, and automate the encryption key management process to minimize risk and reduce operational costs of encryption key management.

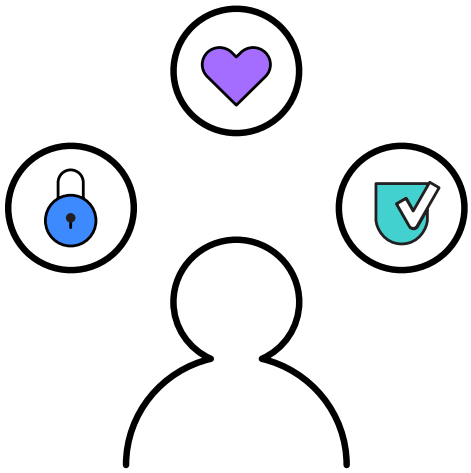
**→ IBM Resilient Incident Response Platform**

Creates actionable security alerts, provides insightful intelligence and incident context, and enables adaptive response to complex cyber threats.

# Conclusion

Organizations that collect, store, manage, or process data must manage it responsibly and follow all regulations that govern that data. The GDPR gives ad tech companies the opportunity to rethink the way they handle personal data.

Learn more about GDPR Readiness in the IBM Cloud:
**ibm.com/cloud/info/gdpr**



*Notice: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations.*

*The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting, or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.*