bitglass

preparing for GDPR with Bitglass

The General Data Protection Regulation of the EU is designed to ensure that the collection, storage, and processing of member states' citizens' data is consistent, secure, and non-invasive.

In terms of the regulation's scope, it is not just European firms that are affected. In fact, the regulation isn't even limited to enterprises with physical operations in Europe. Any organization that stores or processes the personal data of European citizens must uphold GDPR.

Failure to comply with the regulation can lead to fines up to 20 million Euros, or 4% of the organization's revenue—whichever is higher. Data subjects, including employees, can also take legal action against organizations that misuse their data. In light of the above facts, organizations are turning to solutions like Bitglass, a cloud access security broker (CASB), to help meet the mandate before it comes into effect May 2018.

Bitglass protects data in real time, wherever it goes, all without agents. With comprehensive visibility and control over data, Bitglass helps organization meet various compliance requirements, including those of GDPR.

right to erasure and right to restriction

At any time, a data subject can request that an organization erase her or his information. This can happen for a number of reasons, including simple withdrawal of consent. Organizations must delete this data on-premises, in cloud apps, across devices, and from the public where possible. In some cases, data subjects can also request that an organization restrict processing their personal information for a limited period of time.

With API integration across major enterprise cloud apps, Bitglass can manage and delete data at rest in cloud apps, making it inaccessible from endpoints.

Through access control, organizations can prevent downloads by any or all users, by job function, and more.

Bitglass can restrict employee access to sensitive or regulated information with granular data patterns.

Block, quarantine, or encrypt data in real time to meet the right to restriction requirement.

consent and special data

Data is subject to consent constraints—organizations can only use it for the purpose to which subjects originally consented. However, some special categories of data require additional security and consideration. For example, biometric data, genetic data, racial information, political views, religious views, the data of children, and more. Essentially, personally identifiable information (PII) is heavily regulated under GDPR. Regardless of data type, organizations must be able to identify and control what happens to this PII.

Bitglass offers encryption and tokenization to mask special data in structured and unstructured formats.

Enforce access controls to safeguard special data.

Bitglass activity logs provide visibility across all applications. Track and monitor file activity to ensure that data is being used solely by relevant parties for consented purposes.

With Bitglass DLP, organizations can limit the viewing and downloading of restricted data types.

privacy by design and data protection

Enterprises must build their technical and organizational processes in a way that protects data privacy under GDPR. Steps must be taken to inhibit data misuse, prevent unauthorized access by internal and external parties, keep records of data processing, and demonstrate proof of compliance. To meet these requirements organizations need security capabilities that encompass cloud, endpoints, BYOD, and outside threats such as malware.

Unlike other CASB solutions, Bitglass is agentless and only monitors corporate data.

Bitglass offers encryption that is fully secure, searchable, and sortable—perfect for securing data-at-rest.

Bitglass DLP offers detailed dashboards for visibility, integration with leading on-premises DLP solutions, and remediation actions like watermarking, file encryption, and blocking.

Automated activity logs and audit capabilities leave data trails for users, files, and applications—helpful for showing security compliance and appropriate data usage.

With Bitglass ATP, powered by Cylance's predictive machine learning engine, organizations can protect from known and unknown malware at upload, at download, and in the cloud.

Through proxies, Bitglass provides real-time security that encompasses the above capabilities for both managed and unmanaged devices.

data residency and international data transfers

Under GDPR, some data can only be stored or transferred where the state has jurisdiction or where an agreement is in place that protects that data—the residency requirement. Whether data is being stored in another country or merely transferred abroad temporarily, organizations must keep track of where data is stored, sent, and accessed. Even when contracts or binding corporate rules (BCRs) permit risky international data transfers, visibility and control over data are still necessary.

Bitglass can ensure compliance under data residency rules (even when data is stored in other countries) by encrypting data at rest in the cloud and giving organizations local control of their own encryption keys.

Through customizable granular access controls, organizations can limit and even block access for devices based on geographic location, risk, and other factors.

With detailed activity logs and shadow IT discovery, Bitglass allows organizations to view and manage data as it moves through the cloud and unsanctioned apps.

When data is stored in or transferred to unsafe countries, tools like redaction and selective wipe can remove sensitive information from emails, files, and mobile devices.

breach alerts

GDPR mandates that organizations disclose when data is compromised with detailed documentation on the causes and effects of breaches, as well as the security measures taken. Organizations need solutions that proactively reduce the incidence of breaches and log activity involving corporate data.

Bitglass breach discovery can quickly identify data exfiltration from unsanctioned cloud apps, TOR networks, anonymizers, malware, and phishing—destinations can be ranked by their relative risk.

By integrating with organizations' existing analytics solutions, Bitglass logs provide additional data for rapid detection of stealthy, sophisticated threats.

Organizations have multiple options for limiting the impact of a breach with tools like watermarking, redaction, encryption, selective wipe, and others.

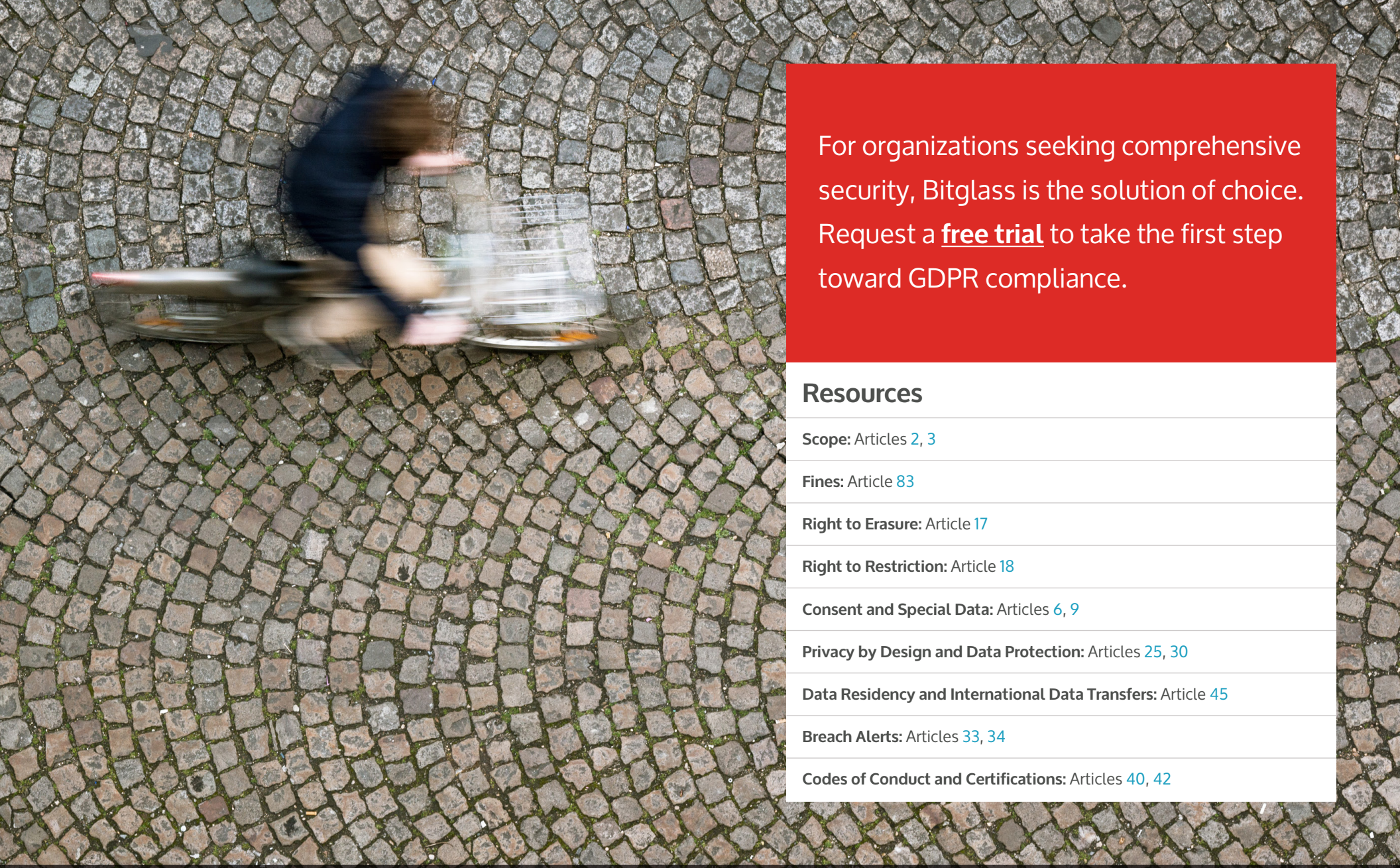
codes of conduct and certifications

Organizations are encouraged to have codes of conduct and certifications for data privacy, security, and compliance with GDPR. They can be established by individual firms or by associations and groups of companies. While they are intended to be a form of voluntary self-regulation, there will be accredited, independent bodies that determine if organizations are in compliance with the tools they select.

To maintain their codes and certifications, enterprises must show that they are meeting the relevant standards. Security solutions that provide transparency and security with respect to data storage, access, and usage can help demonstrate various levels of compliance.

Bitglass is fully transparent with data transmission, security, and processing.

Bitglass is certified under the EU-US Privacy Shield and meets all requirements under Privacy Shield.



For organizations seeking comprehensive security, Bitglass is the solution of choice. Request a **free trial** to take the first step toward GDPR compliance.

Resources

Scope: Articles 2, 3

Fines: Article 83

Right to Erasure: Article 17

Right to Restriction: Article 18

Consent and Special Data: Articles 6, 9

Privacy by Design and Data Protection: Articles 25, 30

Data Residency and International Data Transfers: Article 45

Breach Alerts: Articles 33, 34

Codes of Conduct and Certifications: Articles 40, 42

bitglass

The Bitglass Cloud Access Security Broker (CASB) solution provides end-to-end data protection from the cloud to the device. It deploys in minutes and works with any cloud app. Bitglass enables enterprises to understand and control usage of cloud apps like Office 365 and Salesforce, and internal apps like Exchange and Sharepoint. Cloud data-at-rest is protected with encryption and suspicious activity detection. IT security teams can enforce consistent access, sharing, and data leakage prevention policies across multiple cloud services and any device.