Lytics | WHITE PAPER

PRIVACY BY DESIGN

HOW LYTICS SUPPORTS PRIVACY-COMPLIANT MARKETING

TABLE OF CONTENTS

As an increasing number of companies experience data breaches, malware attacks, and other incidents where entrusted data is at risk of being exposed, the concept of "customer data vulnerability" has led to taking a closer look at how organizations are using the data collected.

Lytics cannot offer legal advice regarding any regulations, including the European Union General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) compliance. Lytics also cannot answer specific questions related to the interpretation of the GDPR, CCPA, or other similar regulations. Lytics recommends you consult your organization's legal counsel and/or privacy experts to determine what is required for your specific organization.

Executive Summary

- Keeping data secure is a shared responsibility. The protection of your data and privacy law compliance require the attention and dedicated efforts of both Lytics and each of our customers.
- Security best practices are a mandated aspect of all development activities at Lytics with risk management living at the core of the software development process. This includes evaluating the probability and impact of all vulnerabilities and changes to protect against attacks, disruption of service, and attempts to compromise the privacy, confidentiality, or integrity of customer data.
- Lytics respects the privacy of the individuals whose personal information we process and their rights regarding that data. We do not sell personally identifiable information or share it except as explicitly directed by our customers.
  We are focused on meeting, and helping our customers meet, the requirements of a fast-changing privacy regulatory environment while providing compliance-enabling technology.
- Lytics is committed to regular, independent audits of our platform as a means of enhancing data protection and reducing the risk of a security incident. We have retained an independent accounting firm to confirm the controls we have implemented to secure our platform and customer data entrusted to us meet the Service Organization Controls (SOC) 2 Type II Trust Services Principles for Security, Availability, and Confidentiality.
- Ensuring our customers' data is protected is a primary consideration at Lytics when identifying enhancements on the product roadmap. Lytics is also invested in reviewing any regulations that may influence our product or in how our customers conduct business via our platform.

Protecting Customer Data, Respecting Privacy, Facilitating Compliance

AS AN INCREASING NUMBER OF COMPANIES experience data breaches, malware attacks, and other incidents where entrusted data is at risk of being exposed, the concept of "customer data vulnerability" has led to taking a closer look at how organizations are using the data collected. This also includes understanding what protective measures are being enacted to limit exposure of their personally identifiable information (PII). The growing awareness of unauthorized disclosures of PII and other privacy abuses have focused attention on whether organizations are honoring their privacy commitments to customers and are compliant with current legal protections.

Lytics is prepared to help organizations adopt a new framework for privacy-compliant marketing. We believe in helping to mitigate security and privacy risks, technical and marketing teams need to partner together in being more vigilant on what data is collected, how it is collected, from whom it is collected, how the data is stored, where and how it's used, and who has access to it.

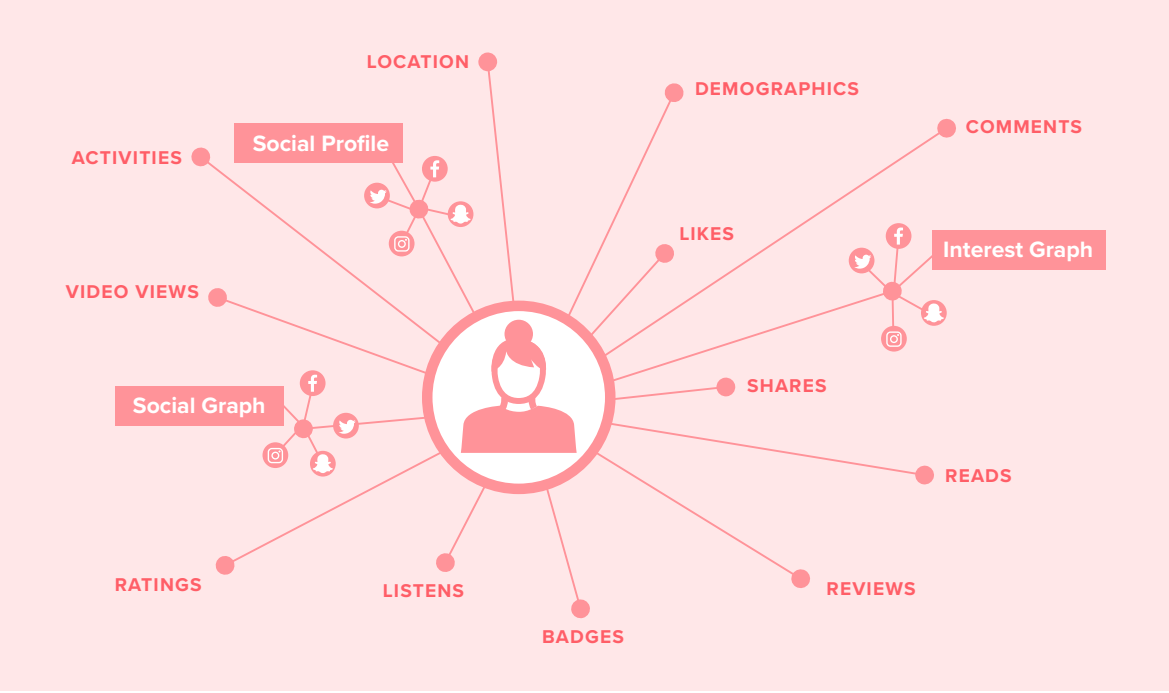
Although protecting data and securing its infrastructure are not new responsibilities for technical teams within an organization, it's likely a new world for many marketers regarding the implications and regulations surrounding data protection and privacy. Marketers seeking to leverage customer data for personalization, audience segmentation, or behavioral insights need to be aware of the need to proactively address privacy concerns and requirements and understand the steps to take to prevent information from being compromised.

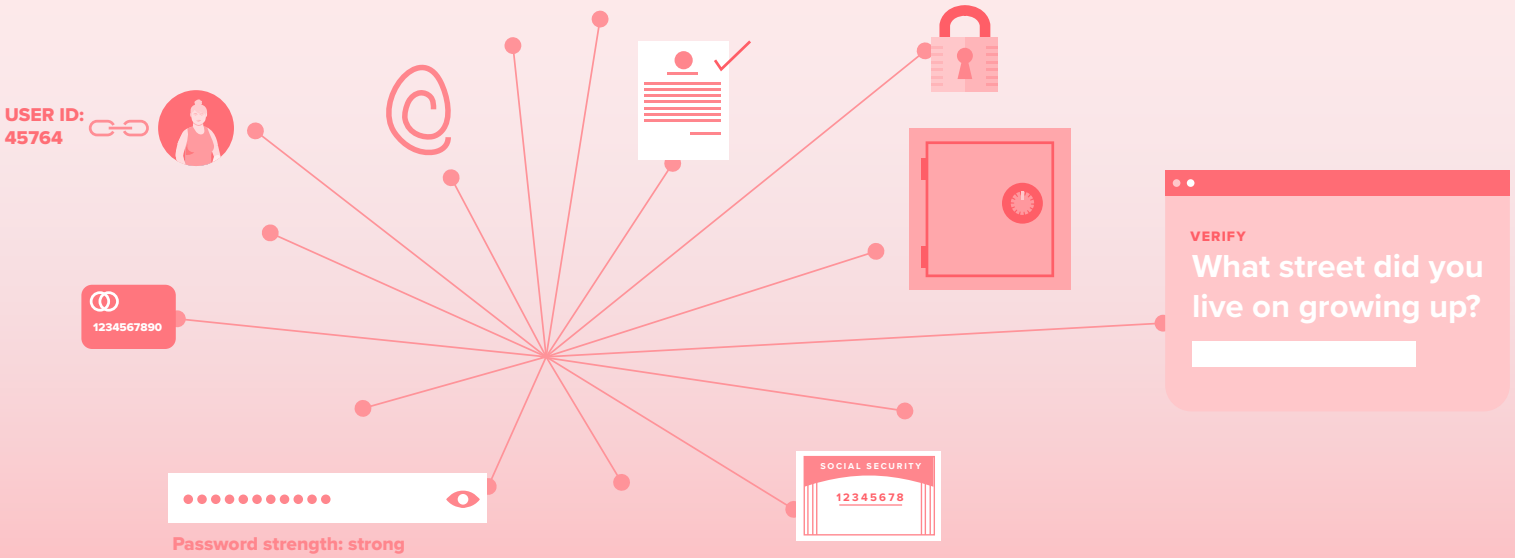
With the introduction of regulations such as the European Union General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), governments are stepping in on behalf of their constituencies to increase the responsibilities—along with increased financial and legal penalties—of companies to keep customer data secure, require controls on how data can be used, deliver a "plain English" understanding to consumers on how their personal data is used, and provide visitors/customers with the opportunity to have their PII be produced as well as deleted from databases.

However, the treatment of data is only one part of the equation. The security of data systems and infrastructure is also critical for protecting the integrity, availability, and confidentiality of customer data. The systems and infrastructure need to be secure with restricted, limited points of access. Getting in place the right team who have been verified and trained on their responsibilities is also important. Finally, it involves ensuring platforms with access to customer data, particularly those using PII, are audited regularly to vet the effectiveness of controls and to identify potential vulnerabilities that can be remediated to reduce risk.

This document discusses Lytics' approach to data protection and privacy, including the shared responsibility model. This document also discusses the data protection safeguards and privacy practices we have implemented and the compliance enabling technology we offer to our customers.

PRIVACY-COMPLIANT MARKETING REQUIRES TRANSPARENCY





Data Protection and Security Are Shared Responsibilities

WE VIEW THE PROTECTION OF YOUR DATA and privacy law compliance as shared responsibilities requiring the attention and dedicated efforts of both Lytics and each of our customers.

We have implemented—and maintain—appropriate administrative, physical and logical data protection safeguards and features designed to protect the security, availability, confidentiality, and integrity of customer data entrusted to Lytics and to facilitate our customers' compliance with the applicable laws.

For their part, Lytics' customers are responsible for enacting best practices around data privacy and security for the benefit of their customers and their data.

To support the new and ongoing compliance requirements, companies should consider the following questions:

» How do we manage our customer data to support new regulations?
» How do we provide more transparency to our consumers?
» How do we reduce our use of personal data in our marketing tools & campaigns?
» How do we develop a framework to execute privacy-compliant marketing programs?

A MUTUAL BENEFIT WITHIN YOUR ORGANIZATION

It's common for the introduction of a new platform to require cross-functional collaboration between marketers, data providers, and IT teams to facilitate a successful implementation.

While it may be tempting to skip over some teams to facilitate a faster time to getting started, it comes at the risk of having to stop and redo work and carries a higher risk of leaving customer data unnecessarily vulnerable.

Exporting data to any external source, such as Lytics, should require appropriate internal reviews and authorizations to ensure only the data needed for activation is exported. Having the resources aligned on which systems have been authorized, who has access, which data is being sent, and what data is being imported may require a new level of coordination between a number of teams.

LEVERAGING THE PLATFORM TO ENABLE CROSS-FUNCTIONAL TEAMS

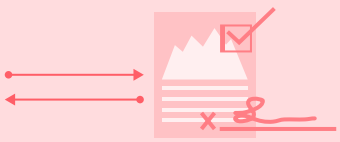
Providing access to a new platform may involve weighing who needs access and how much information should be visible to them. Lytics offers fine-grained role-based access to the Lytics platform and PII hosted by Lytics, but our customers determine access rights for their personnel.

Start with considering who should have the least access to the platform, following the security principle of least privilege. For instance, does the campaign manager need the ability to manage who has access to Lytics or will they only be responsible for building audiences and activating campaigns to downstream tools? Will third-party contractors need to log into the platform to authorize specific integrations?

If access to the platform is required for a significant number of people within your organization, the ability to restrict who can view private fields containing PII or other sensitive details is key. Lytics enables organizations to manage roles and permissions within their account, including limiting the visibility of sensitive customer data.

SHARED RESPONSIBILITY

Process on the Lytics side to receive imported data for building insights, recommendations, and delivering segments to external activation tools



Coordination of company's internal teams to identify the correct data, authorize integrations, imports and exports to Lytics

"If access to the platform is required for a significant number of people within your organization, the ability to restrict who can view private fields containing PII or other sensitive details is key. Lytics enables organizations to manage roles and permissions within their account, including limiting the visibility of sensitive customer data."

BUILDING A CULTURE OF SECURITY AND PRIVACY

- Leaving PII, especially sensitive PII, in the wrong hands has led to trouble for many organizations, including corporate data breaches and resulting erosion of trust in a brand.
- How do you prevent it from occurring?
- Build a culture where all personal sensitive data is protected.
- Review the levels of access available to systems and people within your organization.
- Restrict what data can be used, sold, or shared to the minimum required for the business.
- Limit the data being exported to external systems based on business value.

HIRING AND TRAINING BEST PRACTICES

At Lytics, all employees are required to provide specific documents verifying their identity and undergo federal and state criminal background checks prior to being hired. Lytics also trains all new employees about our confidentiality, privacy, and information security obligations during onboarding and conducts refresher training periodically thereafter. We also require all of our employees and contractors to sign confidentiality agreements to protect customer information, including hosted personal data.

The Lytics Product Development team receives further in-depth training specific to the product development and deployment of secure applications. Lytics also communicates with all employees about privacy and information security through regular newsletters. We also address privacy and data protection topics of interest in company blog posts on our internal communications platform.

Additional access controls at Lytics include:

» Network accounts are mapped directly to employees using a unique identifier—generic administrative accounts are not used.

» Lytics periodically reviews employee access to internal systems. Reviews ensure that employees access rights and access patterns are commensurate with their current positions.

» Lytics follows a formal termination notification process which is initiated by the Human Resources department. Upon notification by HR, all physical and system accesses are promptly revoked.

» Lytics requires the use of strong passwords and requires employees to notify corporate IT immediately if they believe the security of their password has been compromised.

IT STARTS WITH HIRING THE RIGHT EMPLOYEES

APPLYING THE LEAST PRIVILEGE PRINCIPLE FOR YOUR DATA

Lytics believes in using the least privilege approach to limit access to production data and systems. This reduces access to customer data to only those who have legitimate business needs, such as providing support to organizations using the platform.

We facilitate the integration of systems to achieve marketing goals at the direction of each customer and does not use customer data beyond what each customer tell us. As a rule, Lytics does not sell or share any customer data.

As part of the shared responsibility between Lytics and our customers, you are only authorized to see what is in your Lytics account. By default, access to Lytics is managed with a username (email address) and a password. We ask customers to inform us immediately if they have a compromised credential so it can be revoked and reset.

LEVERAGING ACCESS CONTROLS WITHIN LYTICS

Our security features provide organizations with the ability to segregate duties and roles/permission with access controls to limit access to PII; pseudonymize/anonymize or hash any identifier for an account; and role-based access controls for access to different attributes stored on the user profiles.

Lytics supports enterprise Single Sign-On (SSO) by using Auth0 as a service provider using SAML protocol. We integrate with identity providers (IdPs) allowing the IdP to initiate SSO. This means, when a Lytics user logs into the IdP, they will use a global portal for your organization. Those with permission can then click a link or button to access Lytics seamlessly.

Two-Factor Authentication (2FA) is a technique that helps make accounts more secure by adding a second step to the login process while providing an extra level of verification. We enable the second factor from Authy SoftToken, which provides a secret token that changes every 20 seconds.

WANT TO LEARN MORE?

Connect with your Lytics Account Executive or Account Manager to discuss these access controls or additional options available.

How Lytics Protects Customer Data

SECURITY BEST PRACTICES ARE A MANDATED aspect of all development activities at Lytics with risk management living at the core of the software development process. The development team evaluates the probability and impact of all vulnerabilities and changes to protect against attacks, disruption of service, and attempts to compromise the privacy, confidentiality, or integrity of customer data.

KEEPING DATA IN THE CLOUD

Why store data in the cloud? It reduces the dependence on local equipment to house sensitive data. At Lytics, customer data is stored in Google Cloud, with the limited exception of customer-requested use of AWS S3 buckets. Lytics provides security at the system and application layers while our cloud providers provide security for their respective infrastructures and data centers.

We use the Google Cloud Platform infrastructure because it has been architected to be one of the most flexible, reliable, and secure cloud environments available today, allowing our customers to benefit from this data infrastructure.

NETWORK SECURITY AND COMPLIANCE

Lytics' Subscription Services infrastructure is divided into multiple, geographically dispersed facilities. Each facility is housed in a Tier 3 or Tier 4 data center, designed specifically for maximum security and availability. All locations employ industry best practices, including badge and biometric access entry systems, redundant power sources, redundant air conditioning units and fire suppression systems. Security personnel and cameras monitor these locations 24 hours a day, 365 days a year.

ENCRYPTION OF DATA AT STORAGE AND IN TRANSIT

Lytics utilizes Google encryption to safeguard data at storage in the Google Cloud. (Encryption is deployed in AWS S3 buckets, too.) As Google states in its documentation, Google encrypts data at rest prior to storage and stores encryption keys with the data. The keys themselves are encrypted or wrapped by key encryption. The key encryption keys are stored and used inside Google's central Key Management Service.

Data is encrypted at storage using either AES256 or AES128 and applied to chunks of data, so that if any key were compromised, the "blast radius" would be limited to only the data chunk encrypted with the compromised key. Each chunk is distributed across Google's storage systems to further protect customer data from a malicious actor.

Additionally, Google encrypts data at the storage device level, using a device-level key that is different than the key used to encrypt the data at the storage level. AES128 and AES256 are used, but as older devices are replaced, only AES256 will be used for device-level encryption. Finally, the backup system further encrypts each backup file independently with its own data encryption key.

We encrypt data in transit using HTTPS/TLS. When our customers load the Lytics JavaScript tag on their website, it communicates with our CDN provider for encrypted communication with our APIs. The TLS version supported is currently 1.2 or newer.

> "Lytics' Subscription Services infrastructure is divided into multiple, geographically dispersed facilities. Each facility is housed in a Tier 3 or Tier 4 data center, designed specifically for maximum security and availability. All locations employ industry best practices, including badge and biometric access entry systems, redundant power sources, redundant air conditioning units and fire suppression systems."

PLATFORM OPERATIONS MANAGEMENT

The Lytics Platform Operations environment is kept separate from Development, QA, and corporate IT environments. Access to these resources are limited to Platform Operations employees and requires a separate set of credentials for authentication.

Lytics operates a commercial patch management solution to maintain all hardware systems, OS, and application level security patches. Each of these environments reside in a separate network domains and is managed by a separate team.

Lytics utilizes commercial anti-malware and vulnerability detection software and updates are managed and pushed out, as required, with definitions updated automatically.

APPLICATION SECURITY MANAGEMENT

Lytics follows an Agile Development Methodology, with security testing implemented throughout the entire software development lifecycle. Test areas include volume, stress, security, performance, resource usage, configuration, compatibility, installation, and recovery testing.

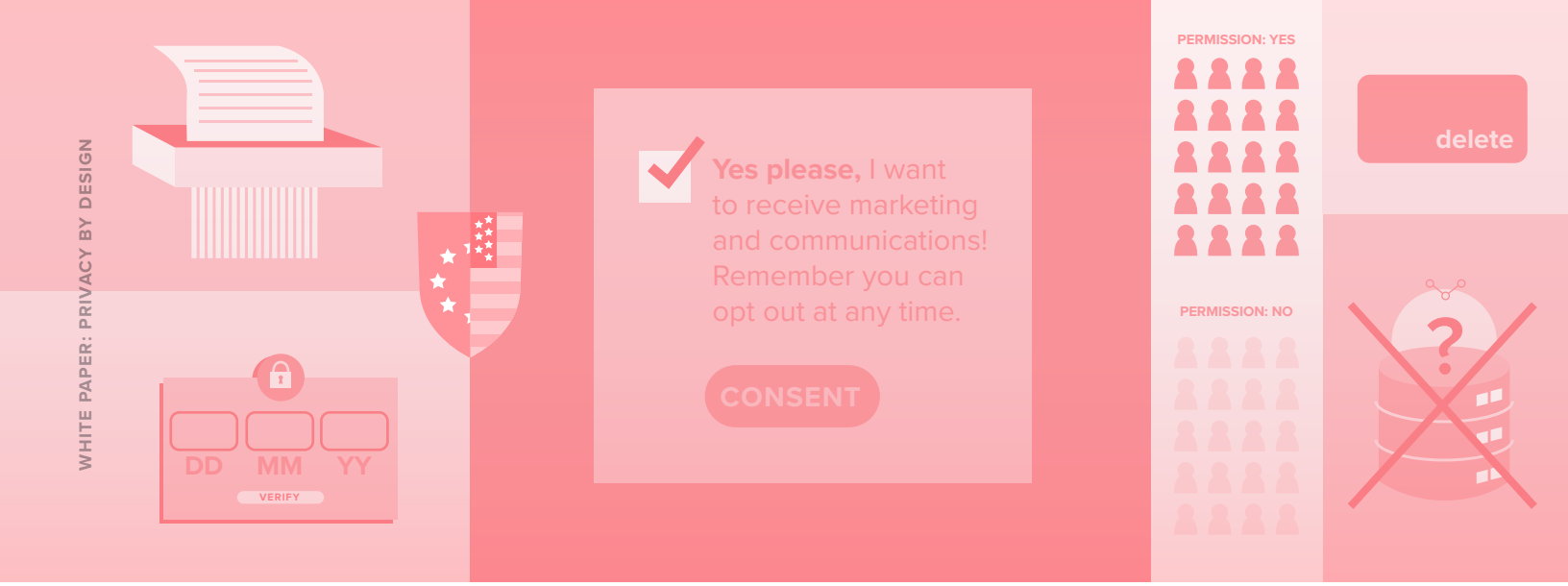
INCIDENT MANAGEMENT

Lytics operates a formal Security Event Management process. This includes escalation procedures to ensure timely and effective treatment of security incidents, including timely notification to any of our affected customers.

PREPARING FOR THE WORST AND A QUICK RECOVERY

Keeping the platform running smoothly requires significant work and effort. However, forces outside of our control may happen. To mitigate this, all aspects of the platform environment are designed and built with redundancies throughout.

Lytics maintains essential disaster avoidance, readiness, and recovery planning capabilities through the use of multiple geographically dispersed data centers, redundancy throughout our customer data platform (CDP) architecture, offsite backup media storage, and remote access capabilities.



Focused on Privacy and Delivery of Compliance-Enabling Functionality

LYTICS RESPECTS THE PRIVACY OF THE INDIVIDUALS whose personal information we process and their rights regarding that data. We do not sell personally identifiable information or share it except as explicitly directed by our customers. We are focused on meeting, and helping our customers meet, the requirements of a fast-changing privacy regulatory environment while providing compliance-enabling technology.

PERSONAL DATA MINIMIZATION AND MAPPING

Lytics services excel at providing insights and recommendations for our customers so they can deliver better marketing experiences to their customers. We champion personal data minimization as a key privacy principle.

We recommend our customers collect only the personal data they need for marketing purposes, minimizing or foregoing altogether third-party data in favor of first-party data reflecting individual consumer experiences. This data is not only more reflective of each consumer's engagement with your brand or their interests in brand-generated content and experiences, but more sound from a regulatory perspective.

Lytics provides a central hub for customer data, allowing each of our customers to collect personal information from their selected sources, such as a website or marketing platforms, and send the customer data to specific destinations, such as your CRM database or accounts with third-party applications or services.

Each Lytics customer maintains control over which sources and destinations they with within the CDP as well as the types and content of personal information shared between its sources and destinations. Each customer can use Lytics to develop a new, unified customer data schema and data dictionary. This new customer data schema can provide a clear understanding of how data is collected from different sources and how it is used to support use cases in different marketing destinations, providing traceability as to the origin of personal data received, hosted, and transferred by Lytics. We do not sell customer data or share it except with the destinations as authorized by each of our customers.

PRIVACY PROGRAM

Lytics has implemented a privacy program for our CDP as a framework to help us maintain compliance with the laws applicable to our business and to meet our privacy-related contractual commitments. We look to earn and retain the trust of our customers, website users, employees, and partners based on respect for their privacy concerns and protection of information with reasonable security safeguards.

CONTRACTUAL PROTECTIONS

Lytics contracts with our customers include confidentiality provisions that prohibit us from disclosing customer confidential information, including customer data, except under certain circumstances, such as when required by law. Our contracts make it clear that our customers own and control the data they submit to us and that we process it only in accordance with their instructions. We also agree to restrict our access to customer data to the extent necessary to provide our services and in connection with a customer support issue or where required by law.

PRIVACY POLICY

The Lytics Privacy Policy describes our practices regarding the personal information we process as a data controller operating a business. This policy also describes our role and practices in connection with personal information we may receive and otherwise process on behalf of our customers.

PROTECTION FOR DATA TRANSFERS

Lytics participates in the EU-US and Swiss-US Privacy Shield Frameworks regarding the collection, use, and retention of personal data from European Union member countries and Switzerland. We have certified with the Department of Commerce that we adhere to the Privacy Shield Principles. Visit the Privacy Shield Principles website to learn more.

ACCOUNTABILITY

The Lytics VP of Legal and Data Protection Office is responsible for our privacy program, including compliance with applicable privacy and data-protection laws. The Lytics Information Security Team is responsible for service related security matters, certifications, and our SOC 2-based CDP security program. Additionally, all Lytics personnel are required to follow Lytics' confidentiality, privacy, and information security policies.

DATA RETENTION AND DESTRUCTION

Lytics retains customer data in accordance with customer instructions contained in their respective services agreement. Following termination of a service agreement with a customer, the customer data is effectively deleted with logical deletion and cryptographic erasure. When media that hosted customer data is no longer useful, it is destroyed in compliance with NIST SP 800-88 Revision 1 Guidelines for Media Sanitation and DoD security guidelines.

PRIVACY AND DATA PROTECTION COMPLIANCE-FACILITATING TECHNOLOGY

Our core CDP service includes technology enabling our customers to meet key privacy and data protection requirements. We also offer Strategic Services to help our customers implement best practices in the use of Lytics to meet regulatory requirements.

CONSENTS

GDPR and many other privacy regimes require that data controllers obtain the affirmative consent of individuals for the purpose of processing their data prior to processing it. Our customers may arrange for Lytics collection of personal information on their online properties through the use of the Lytics JS tag and are responsible for obtaining consent for the collection and transfer of personal information to Lytics for processing.

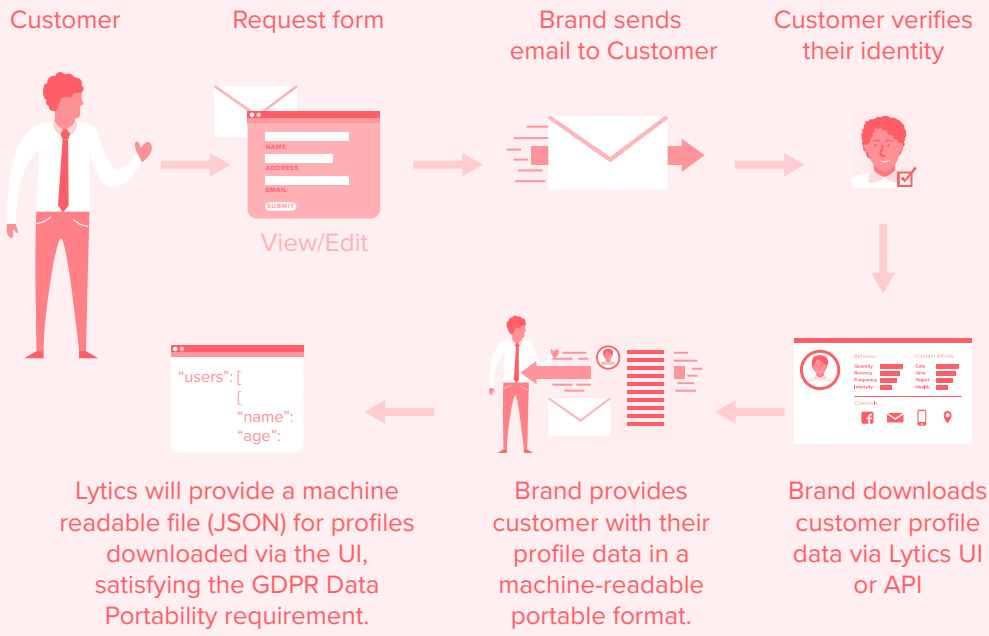
One consent mechanism available for our customers is to implement a custom tag and trigger in their Google Tag Manager account and assign that trigger to the Lytics JS tag. The custom tag will display the consent modal to the individual visiting your online property. When the site visitor gives their affirmative consent, the custom trigger will fire enabling the Lytics JS tag for that individual. If the individual does not give consent, the Lytics JS tag will be disabled and will not collect or process data for that individual.

Lytics platform enables customers to understand and operationalize marketing choices made by a consumer once they are ingested from a customer data Source and stored as preferences in the Lytics platform. For example, Lytics customers can establish audiences in the Lytics CDP to enforce consumer suppression and "do not market" choices and prioritize those choices when establishing marketing journeys for their respective consumers. In addition, these audiences can be synched by Lytics customers to Sources to which they export data from the Lytics CDP.

LEARN MORE

Additional resources on consent management solutions are available at learn.lytics.com.

LOGISTICS OF CONSENT MANAGEMENT



RIGHT OF ACCESS AND DATA PORTABILITY

The GDPR, CCPA, and other privacy regimes provide your customers and other identifiable visitors to your online properties the right to know if their personal data is being processed, and if so, access to that data. These individuals also have the right to receive their personal data in a structured, commonly-used and machine-readable format, and have the right to transmit that personal data to another organization of their choice.

Your organization is responsible for managing the request for access and the verification of your customer's identity. As a data processor and service provider, Lytics supports the export of profile information via the user interface or API. An individual's profile data from Lytics will be downloaded as a JavaScript Object Notation (JSON) file. JSON is a common, machine-readable file format.

RIGHT TO RESTRICT PROCESSING

The GDPR confers on individuals in scope the right to restrict the processing of their data under certain circumstances. Lytics customers can edit and delete consumer data based on subject access requests so that a particular identifiable individual's personal information is not further processed during the period the restriction is in effect.

RIGHT OF ERASURE (DELETION)

The GDPR, CCPA, and other privacy regimes grant individuals the right to erasure of personal data without undue delay. Lytics, as a data processor and service provider, supports our customers' ability to comply with this regulatory requirement by providing a Delete User option in the Lytics UI. Our API may also be used for this purpose. This will send a deletion request to the Lytics platform, which will process the request for the customer identifier provided.

MORE ON GDPR SUPPORT

Lytics has answered some frequently asked questions regarding using Lytics to support GDPR. You can also visit the official GDPR portal to learn more.

NOT MARKETING TO CHILDREN

To facilitate compliance with the Children's Online Privacy Protection Act (COPPA) and other laws prohibiting marketing to underage individuals, Lytics will not ingest any user data of individuals who have not declared themselves to be over the age of 13 via a customer website's age gate.

Independent Audits and Certifications

LYTICS IS COMMITTED TO REGULAR, INDEPENDENT AUDITS of our platform as a means of enhancing data protection and reducing the risk of a security incident. We have retained an independent accounting firm to confirm the controls we have implemented to secure our platform and customer data entrusted to us meet the Service Organization Controls (SOC) 2 Type II Trust Services Principles for Security, Availability, and Confidentiality.

Independent auditors have also examined the controls present in the Google Cloud Platform, including its infrastructure and operations, against the following standards:

- SSAE16 / ISAE 3402 Type II with a publicly available SOC 3 audit report;
- ISO 27001 certification for the systems, applications, people, technology, processes and data centers serving Google Cloud;
- ISO 27017:2015, Cloud Security, which is an international standard of practice for information security controls based on ISO/IEC 27002 specifically for cloud services; and
- ISO 27018, Cloud Privacy, which is an international standard of practice for protection of personally identifiable information (PII) in public clouds services.

The Google Cloud Platform also supports HIPAA covered customers by entering into a Business Associates Agreement (BAA). The Cloud Platform BAA currently covers numerous systems utilized by Lytics.

Conclusion

AS REGULATIONS ARE PASSED AND ENACTED, keeping your customers' data secure, reviewing the levels of access to data, and receiving the appropriate consent from customers/site visitors will remain a critical duty across your entire organization. The data privacy and customer consent landscape is under the microscope and will continue to be subject to high levels of scrutiny from all levels of government (domestic and international), your organization's key stakeholders, and your customers.

Ensuring our customers' data is protected is a primary consideration at Lytics when identifying enhancements on the product roadmap. Lytics is also invested in reviewing any regulations that may influence our product or in how our customers conduct business via our platform.

We are equally committed to ensuring levels of security are maintained, taking preventive measures against potential vulnerabilities.

LEARN MORE

Lytics Privacy Policy can be found online here.

For more information and the latest updates, please visit lytics.com.