BriteVerify

Ready for GDPR

Upholding the highest standards for your data

BriteVerify and GDPR

BriteVerify was built with a strong focus on data security and privacy. Our view is that customer data is one of the most valuable assets a company has, and when this data is provided to us for verification, our job is secure it and use it only for the purpose it was provided to us.

Since BriteVerify services are used by companies in over 150 countries, our security and privacy programs, at a minimum, must comply with the strictest controls set by our customers and their countries' regulators. Having been through numerous security and privacy audits, we believe BriteVerify is fully compliant with the General Data Protection Regulation (GDPR) and welcome the opportunity to discuss the below information further.

BriteVerify GDPR Controls

As it relates to the needs of our customers, BriteVerify is considered a processor. A processor provides services that include applying a set of operations on personal data. In our case, the set of operations includes determining whether personal data is valid, and the personal data in question consists of email address. When you submit an email address or list of addresses to BriteVerify, the data moves over a secure connection to BriteVerify's applications in Amazon Web Services region useast-1 or eu-west-1. BriteVerify then communicates securely with the email server associated with each email address to determine the address' validity. Once verification is complete, your data is delivered back to you over a secure connection to complete the process. This is the end of our interest and involvement with your email addresses.

While this is simple explanation of how your data will move through the verification process, there are many controls in the GDPR that processors like BriteVerify must comply with if they provide services to data controllers that have customers in the European Union. These controls include:

Follow the Rules

As the data controller, you own the right to tell us what we can and cannot do with your data. Since you have your own rules to follow on behalf of your customers, your responsibility is to make sure we're keeping your data safe and using it only for the purpose you have assigned to us. BriteVerify will follow your instructions and will inform you immediately if any of your instructions fall outside of BriteVerify's GDPR controls.

Confirm Sub-Processors

Since BriteVerify's applications are hosted in Amazon Web Services processing facilities, we make it clear that we use a sub-processor as a part of the verification process. Since AWS centers undergo annual compliance and certification by a comprehensive list of regulatory bodies, AWS is typically considered an acceptable subprocessor under GDPR.

Deletion of Data

At the end of your engagement with BriteVerify, you can request the deletion of any data sent to us for verification. We always comply with these requests and also provide you with the ability to delete your own data at any time in your BriteVerify account.

Support Compliance Audits

At your discretion and convenience, you may request an audit of BriteVerify's business offices and processing facilities. While you're more than welcome to come see us, BriteVerify does not store any of your customer data in our business offices. And for security purposes, Amazon does not allow BriteVerify or its customers to audit their facilities individually. However, Amazon's list of compliance and certification programs (https://aws.amazon.com/compliance/) provide the necessary proxy to an ad hoc audit and generally satisfy this component of GDPR.

Keep Things Secure

BriteVerify's Information Security Policy undergoes an annual independent review and ad hoc reviews throughout the year by BriteVerify customers. BriteVerify also undergoes semi-annual independent network penetration testing and quarterly vulnerability testing to ensure our network is secure and any potential weaknesses are fixed. Finally, all email addresses, when in our possession, are secured using AES 256 encryption, which makes it darn near impossible to get access to real email addresses even if the bad guys found their way into our systems.

Breach Notification

BriteVerify manages a formal Incident Response Plan, which outlines our communication and remediation strategy in response to the slightest possibility that a breach of our systems has taken place. In short, we are committed to immediate notification if a breach is ever discovered and ongoing communication throughout the remediation process. While there are other components to the Plan, the most important ones are that we will:

1: Notify you in the event of a breach
2: Let you know if we believe your data may have been compromised
3: What we're doing to not only fix the problems but also find the bad guys.

Restrict Data Movement

This is an interesting one. Until recently, BriteVerify had to move all email lists to the U.S. for verification. This is permissible under GDPR provided a processor like BriteVerify gained permission for the transfer from its controllers. While we would always request permission to perform this task, we have now changed the way we process lists. BriteVerify Customers in the EU are now able to process their lists locally in our AWS eu-west-1 (Ireland) EU processing facilities. This is not necessarily a mandate under GDPR, but our EU customers requested it of us, so we built it. These controls are available on request.

Record Processing Activities

Since BriteVerify's entire business is built on processing data for our customers, we must maintain a record of our processing activities to comply with GDPR. We provide this information to our customers in their BriteVerify accounts and maintain logs that identify the date, list name (if appropriate), processing location, and total records processed for each customer. The logs create an audit trail for each list processed by our systems and serve as a dispute resolution mechanism should you ever have a question about who loaded, processed, or downloaded a list.

Data Protection Officer

Since BriteVerify processes large volumes of email addresses every day, we have established the role of Data Protection Officer (DPO) as required by the GDPR. Our DPO is a part of BriteVerify's senior management team and is responsible for training and monitoring employees to ensure compliance with GDPR, managing the Information Security program, coordinating and reviewing penetration and vulnerability testing, and communicating, as necessary, with supervisory authorities. BriteVerify's DPO is available to discuss our preparedness on request. ■