Trivalent Supports EU General Data Protection Regulation

Background

The General Data Protection Regulation (GDPR) is a new regulation that was implemented in the European Union (EU) on May 25th, 2018. It focuses on data protection and privacy for all individuals within the EU and the European Economic Area (EEA). The GDPR defines requirements for the processing of personally identifiable information (PII) of EU individuals by businesses.

Security Recommendations

The GDPR explains that business processes must use the highest possible privacy settings by default. It requires private data to be saved through pseudonymization, which is an obfuscation technique where data cannot be attributed to a specific individual without the use of additional information. This can be done using encryption and/or tokenization.

Possession does NOT equal Access

Organizations who employ EU citizens in order to meet GDPR mandates must treat their employee data in the same manner as consumer PII. To do so, they require the appropriate policy controls, processes, and technology to ensure the privacy of employee data generated on their networks and systems. Trivalent Protect ensures only authorized users gain access to the data through our unique process of encrypting and randomized shredding. The Trivalent security architecture is certified by the NSA to secure Top Secret data on Android, and Trivalent utilizes the same methods across other platforms, like Windows, Linux, and iOS.

Endpoint

Trivalent Protect is designed from the ground up to secure end-user data independently of other security solutions like Endpoint Protection, Endpoint Detection and Response, Host based Firewall, etc. In this way, even if a bad actor bypasses these security countermeasures, or the endpoint is accessible by legit IT administrators, only the data owner and those users they have given permission will gain access to the data. This can be as granular as individual files or whole directories.

Data In-Transit

Trivalent has developed patent pending technology to secure transmitted data by using multi-channel so each data shred has its own transmission session. The receiving end only requires a certain number of shreds out of the total to recombine the full content, so if some shreds are dropped or hijacked data integrity is not compromised. This solution has been optimized for voluminous transactional data, like financial transaction processing.

Cloud

File Hosting - Since Trivalent does not store content as discrete files but instead breaks them up into randomized shreds, these shreds can be dispersed across cloud storage providers, like Box, Dropbox, and OneDrive, where the data owner and whoever they authorize will gain access to recombine the shreds.

AWS Cloud Infrastructure - Trivalent can be integrated with AWS S3 or Glacier buckets transparently protecting any sensitive data stored or processed by AWS supported cloud applications.