BlastPoint Whitepaper

How BlastPoint Can Limit Your Exposure to GDPR Fines By Pseudonymization and Protection of Data

Contents

What is GDPR?

Pseudonymization: This is the data de-identification procedure of substituting a reversible and consistent pseudonymous identifier for Personally Identifiable Information (PII). This procedure preserves the integrity of a data-set for use in analysis and processing while also upholding GDPR privacy standards and protecting personal information[1].

GDPR (*General Data Protection Regulation*) is a series of regulations that passed into legislation in May 2016, with enforcement starting on the 25th of May, 2018. The new rules require transparency on what records companies keep on customers and the public, give EU citizens the right to request that certain records be deleted and put heavy fines on data breaches and requirements to disclose when personal data is compromised. Fines escalate based on the severity of the breach, the sensitivity of information and precautionary measures taken in advance of the breach itself.

[1] Williamson, Clyde. "Pseudonymization vs. Anonymization and How They Help With GDPR." *Protegrity*, Protegrity Blog, 5 Jan. 2017, www.protegrity.com/pseudonymization-vs-anonymization-help-gdpr/.

BlastPoint can help companies minimize risk from these regulations by aggregating and modeling data so that PII is not exposed to possible access by unauthorized persons. Highly sensitive data such as medical or banking records can be pseudonymized by aggregating them into a pool of information unlinked to any personal identity.

How does it work?

1. We build geographically aggregated data sets. That means that we can take data such as geocodes and addresses and total them up to a set of geographic boundaries such as a zip code, county or census block group. In this process we drop all personally identifiable information and pool the remaining information into records where individual results would not be identifiable.
2. We can also create categories so that exact numbers are not a part of the final data. We can create discrete ranges for sensitive information such as salaries, age values or quantitative medical results. An example would be “Salaries between 100K and 150K” rather than “Salary: $123K”. That means that individuals will not be recognizable from exact values.
3. Finally, our frontend system is architected to be completely separate from our backend system. That means that individual records are not able to be accessed from our web application, even if an account is compromised. This protects even records that have not been aggregated. We keep all of our data in secure databases that can be encrypted and restricted to a few authorized IP addresses for access.

BlastPoint Offerings for Privacy and Security

Additionally, based on your needs we can offer several layers of privacy:

- **Private data on our BlastPoint SaaS server**: we upload data to our BlastPoint server and assign it to specific users or groups. This is our least expensive way to upload data but might not be appropriate for sensitive personal data like payroll or medical records due to storage on a central server.
- **Private Cloud server**: your data is uploaded to a separate instance that is accessible only to authorized users. Customers in need of additional privacy can limit access to specific IPs to restrict unapproved access.
- **On premises deployment**: this is the best choice for customers that need to keep their extremely sensitive data on-site and available within a restricted network only

Our years of working with data in the banking industry has given us the insight that regulations are contagious. That is, they tend to filter into the global system over time. Some countries outside of Europe already have strong regulations that require personally identifiable information to be handled with care. For instance, Brazilian banking regulations require personal data, including names, national ID numbers, phone numbers and addresses to stay within the country's borders, which means that data cannot be processed in offshore data centers.

BlastPoint offers a way to protect your company by making sure that personal information from employees, users or customers is not exposed to potential and vulnerable to theft or blackmail. This means keeping the most sensitive data limited to a set of vetted, authorized users, while providing an pseudonymized pool of data to the broader company for better decision making without fear.