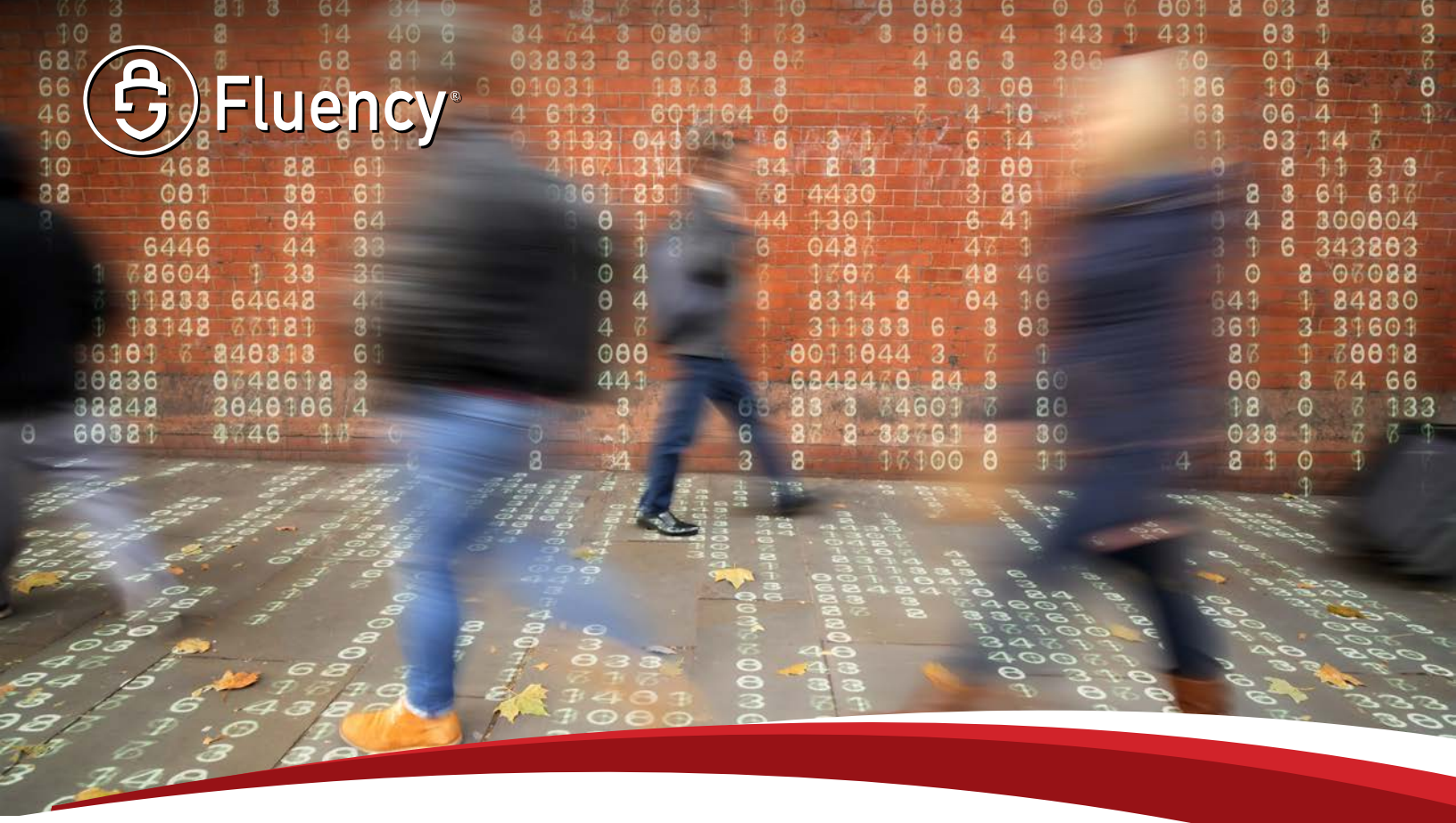

What are Pseudonyms?

With the increase in privacy regulations and laws, the technical term pseudonym is important. Pseudonym is a key piece of technology in implementing privacy. A pseudonym stores sensitive data elsewhere and replaces its appearance with a random token. It is a technical solution that is defined in the General Data Protection Regulation (GDPR). This solution is also required in meeting the California Consumer Protection Act (CCPA), as the right to be forgotten appears in it as well.

Pseudonym is a technology that protects a person's privacy information by presenting a random token instead of the actual data. The token represents the sensitive data that is stored elsewhere. When the user wants to be forgotten, deleting the token-value pair removes any knowledge of who that token was.

> *GDPR Art. 4 (5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"*

It addresses two key elements to privacy:

- Provides a control that limits viewing of personal identifiable data to people with authority to see it.
- Enables the right to be forgotten.

Why are derived cases so popular and what is the difference between a derived hash and a pseudonym?

- Derived one-way-hashes are popular as they creates a pseudo-random value whose original value cannot be determined by the result.

  This bypasses the need to look up a centralized token dictionary in order to keep the value-token mapping consistent, a task very challenging in a distributed computing environment.

- A pseudonym cannot be derived. There is no-way to delete a derived one-way-hash.

  The owner of the system can always recreate the token to value relationship. This means that even if the token-value is deleted, it can always be recreated.

In short, a derived token can never be a pseudonym.

Fluency® Corporation Proprietary and Confidential Copyright© 2012-2018

What other advantages do pseudonyms have?

- **Sharing of Data**
  GDPR allows sharing of data (Data Controller to Data Processor relationship), but this data needs to be transparent to the person. When a person asks to be forgotten, that request and action are passed to the data processor as well. Often, a data processor does not need all or any of the personal data. In these cases, a pseudonym avoids sharing fields of data that are related to privacy, simplifying the overall process of sharing data.

- **Keeping a Log of the Event**
  All the log data shouldn't be deleted. At times, part of the data, like the user's email, needs to be forgotten, but the audit of the event cannot. Often, audit contains some data that is required to be kept for years, while the privacy data needs to be able to be forgotten. Deleting the whole audit event addresses the right-to-be-forgotten but makes you noncompliant to other regulations. Pseudonyms allow certain fields to be removed when needed but leave the audit integrity intact.

- **Managing Access to Privacy Data**
  In a pseudonym, implementation access to the sensitive information is enforced in the pseudonym-value table. By having all sensitive data in this table, privacy access control is simplified and easier to validate.

Fluency Corp
387 Technology Drive | Suite 3119 | College Park, MD 20742
www.fluencysecurity.com

 Copyright© 2012-2018