PSEUDONYMIZATION OF PERSONAL DATA

Fact sheet

VIACRYP B.V. Danzigerkade 19, 1013 AP Amsterdam, The Netherlands

Contents

Contents 1

1. Introduction 2

1.1. Viacryp and pseudonymization of personal data 2

1.2. Legislation regarding pseudonymization 2

1.3. Objective of this document 2

2. The pseudonymization street 3

2.1. Introduction 3

2.2. Isolation of data 3

2.3. Flow diagram 4

1. Introduction

1.1. Viacryp and pseudonymization of personal data

Viacryp is specialized in helping organizations that are involved with the General Data Protection Regulation GDPR). Organizations that require personal data in order to achieve their objectives are subject to strict guidelines as a result of the GDPR. Viacryp provides various services that contribute to the protection of personal data by minimizing and pseudonymizing the amount of legibly stored and processed personal data.

Viacryp is an independent organization, active since 1 July 2013 as Trusted Third Party in the field of pseudonymization of personal data.

1.2. Legislation regarding pseudonymization

The GDPR[1] sets strict conditions for processing data that can be traced in any way to natural persons. In this respect, this traceability must be interpreted in the broadest sense of the word, which means taking into consideration directly identifiable data, such as the citizen service number, social security number, name and address details or IP address, as well as indirectly identifiable data, such as a date of birth or a fully completed postal code.

In order to process personal data an organization needs a foundation. These fundamentals are stated in the GDPR. Furthermore, the GDPR is based on some general principals regarding processing and storing personal data.

- Data minimization (not storing more than necessary)
- Not storing longer than necessary
- Fitting precaution measures to prevent unnecessary collecting and further processing of personal data

Viacryp ensures that the following conditions are met when the Viacryp standard process is used:

I. Pseudonymization is applied in a professional manner, and the first encryption step is carried out by the supplier of the data;
II. Technical and organizational measures have been taken in order to prevent the repeatability of the encryption (‘replay attack’);
III. After processing, the data is not indirectly identifyable;
IV. These three conditions are subject to preceding and periodical audits;
V. Furthermore, the pseudonymization solution will be actively made public by way of a clear and complete document, so that all involved can check which guarantees the chosen solution offers.

1.3. Objective of this document

This document meets condition V., that the pseudonymization solution must be made available to the public.

With this objective in mind, Chapter 3 describes our solution (pseudonymization street) in detail.

[1] See https://gdpr-info.eu/

2. The pseudonymization street

2.1. Introduction

A pseudonymization street consists of one or more sources, which supply data to Pseudonymizer using a supply platform. After this data has been pseudonymized, it is supplied to a receiving party via a delivery platform. The receiving party can use pseudonyms to combine data from the various sources and analyse this data without it containing anypersonal information.

In particular configurations, the combining of various sources an be applied before delivery to the receiver. In this case, no pseudonyms are supplied to the receiver and the data is prepared for analysis purposes, in order to prevent indirect identification of this data.

2.2. Isolation of data

The streets Viacryp uses as Trusted Third Party ensure an 'Isolation of data', meaning personal information (Who) and behaviour (What) are split from each other early in the process. After this, hashing and encryption is appliced, in a way that ensures that at no time in the process (with the exception of the source of the original data), both the **Who** and the **What** can be read by any party.

This can be explained on the basis of the table below:

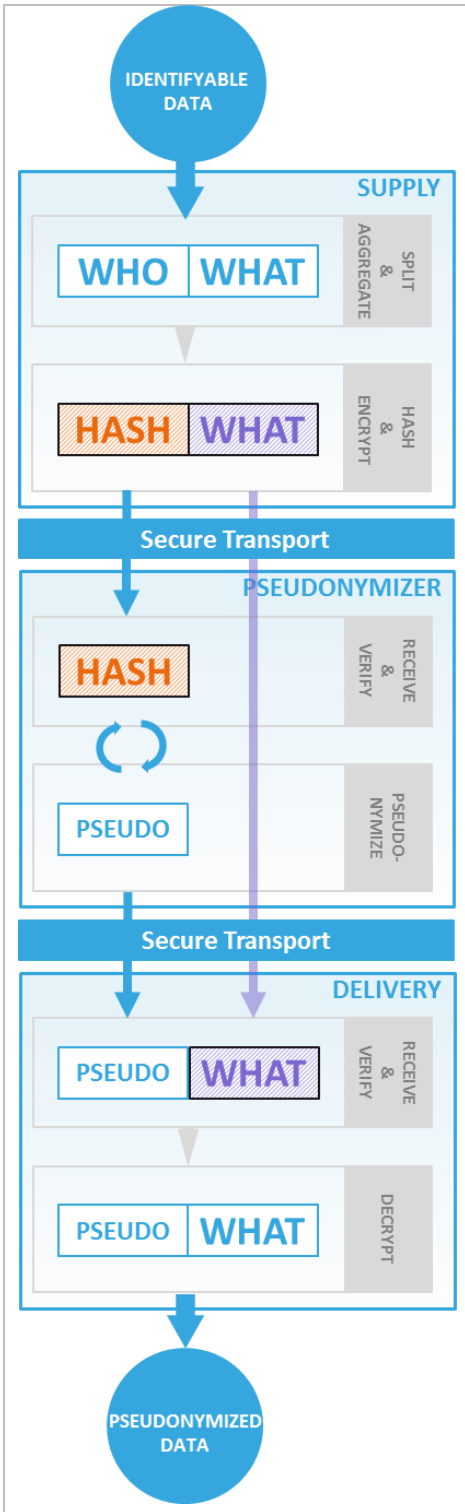
	Source	Supply	Pseudonymizer	Delivery	Receiver
Who	Original	Hashed	Hashed	Pseudonym*)	Pseudonym*)
What	Original	Encrypted	Encrypted	Encrypted	Original

*) Optional

- Only the source has the original **Who** and **What** available.
- On the supply platform, the **Who** is hashed and encrypted and the **What** encrypted before the data leave the domain of the source.
- Pseudonymizer only has the hashed **Who** available in order to be able to make pseudonyms of this which are then (along with the hashed **What**) used in order to prepare data for analysis purposes, or are combined with the encrypted **What.** Next, the data is supplied to the delivery platform at the receiver.
- On the delivery platform the data is decrypted and made available to the receiver, who can perform analysis of the data without identifiable information.

2.3. Flow diagram

The whole street source data travels through is can be represented using the following flow diagram:



Source

Supplies data in an agreed format to the Supply module, which operates in the domain of the source.

Split & Aggregate

Identifying data (**Who**) is separated from behaviour (**What**). **What** is aggregated at such a level that this cannot be traced indirectly to a person.

Hash & Encrypt

Who encrypted one-way (leading to a Hash). **What** is encrypted so that only the receiver can decrypt it.

Receive & Verify

Data is sent through a secured connection to the TTP, where the Pseudonymizer module validates the origin of the data.

Pseudonimyze

In the Pseudonimyze step, Hashes are translated to Pseudonyms.

Receive & Verify

Pseudonyms and (still) encrypted **What** are transported through a secured connection to the Delivery module, which runs at the receiver of the pseudonymized data.

Here, the origin of the data is validated again.

Decrypt

In the last step, **What** is decrypted by the receiver.

Receiver

Now has pseudonymized data, and can analyse it without having personal data available.