T-Identity Protector (T-IP)

Functional operation

Contents

1 Extract

Driven by the necessity to design solutions for processing personal data in a legally allowed way, T.Systems developed the T-Identity Protector (T-IP). T-IP is a product conception from to enable statistical analyses of personal data from various source systems by code numbers using pseudonymization. Furthermore, the conception is to enable subsequent re-identification under controlled conditions.

2 General description of application scenarios

One *example of application* is *company-wide analysis of personal data*. For example, a company could search its entire database for employees with a certain qualification profile as potential candidates for a foreign assignment. The legal problem of this situation is that normally the working relationship exists only with the respective legal entity, but not with the entire company. For lack of a contractual legal basis, the transfer of personnel data to other employers is therefore permissible only with the consent of the persons concerned. To avoid data privacy problems, T-Systems designed the conception so that an initial search run for persons with the required qualification profile would first take place using only the pseudonymized data records. After this search, re-identification would be necessary only for the returned set of employees so that the company could approach them directly. The legal requirements of re-identification must then be adhered to in this case. In this respect, the T-IP supports the protection of rights of the data subjects, because re-identification is possible only under controlled conditions.

A second example of application is the *management of billing data* of users of a telecommunications or online service. The billing data is managed in a pseudonymized manner using the T-IP and is not re-identified until it is needed for collecting the invoice amount or for sending the bill to the customer. Incidentally, T-IP would also enable the combined analysis of pseudonymized invoice data if different service providers are used.

Another example is the *outsourcing of processing of personal data* to a data processor located abroad, especially in a non-EU country without a level of protection comparable to that of the European Union. In this case, pseudonymization and re-identification would take place exclusively at the customer's site at home, while the computing processes of the vendor would be limited solely to the processing of pseudonymized data.

Eventually, the model could be used to enable processing of personal data with the computing capacities of different departments available at any given time. The T-IP would enable such applications if pseudonymization of the data appropriately takes into account the data privacy needs of the employees and customers concerned.

The goal of the conception is to offer a solution that enables qualitative statements about data records from different systems while safeguarding the data subject's interests warranting protection using as little personal data as possible within the meaning of §3 a of the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG). The model of pseudonymization makes it legal to conduct analyses that would be illegal according to data protection laws if individual personal data were used. At the same time, however, the system enables re-identification of the data records, but only under controlled and thus legally specified conditions. The aim of the T-IP is to contribute to the security of the data records by protecting them against improper use through pseudonymization. Incidentally, within the T-IP system, data privacy management plays a key role, because it protects customer or personal data from unauthorized access and processing and thus meets a crucial precondition for increasing the likelihood of the data subject's acceptance of processing.

3 Overview

The following items are distinguished in the conception of T-IP:

- The *source* of the data (source list) from which the personal data are obtained. For example, a source system may contain the personal data of a subsidiary company or the customer data of a system for issuing bills.
- The *recipient* (destination system) that normally receives the data in an anonymized state, but that can also receive this data in a pseudonymized state under "controlled and specified conditions" for the purpose of subsequent re-identification.
- The *T-IP* (T-Identity Protector) in which pseudonymization is performed or reversed according to the "*conception of knowledge distributed to different roles.*" The processing of data is distributed to different roles within the T-IP system.

Basic questions must be settled at all three levels:

➢ For the source system it is important to know how pseudonymization would be performed and in whose area of responsibility.

A *pseudonymization box* (T-IP Client) provided by the T-IP performs pre-pseudonymization within the legal responsibility of the source system. The T-IP Client lies in the area of responsibility of the department in charge of the source system. Strong pseudonymization takes place in the T-IP Master.

➢ For the recipient – the destination system – it is to be checked under which conditions it may receive pseudonymized data instead of anonymized data and what requirements must be placed on the degree of pseudonymization.

➢ In addition, it is important to define the conditions under which re-identification is permissible.

According to § 3 par. 6a BDSG, pseudonymized data are personally identifiable data, because by definition it should be possible in principle to match the pseudonym with the name of the person concerned. Conversely, however, pseudonymization should also practically rule out accidental re-identification or at least make it substantially difficult in accordance with § 3 par. 6a BDSG. Pseudonymization must therefore – apart from the existence of a match function – feature the quality of factually anonymized data for third parties. For this, appropriate mathematical procedures must be used, which also include the padding of data records to effectively prevent their re-identification.

The conditions under which re-identification is to be permitted must be clarified for the respective context of application. For instance, for re-identification of customer data, the scope of the contractual use must be taken into account and the necessity of compliance must be checked. For re-identification of personal data, in addition to the data privacy rights of those involved, the requirements for co-determination at operational level must be considered. In principle, applications that were already impermissible before pseudonymization will also be impermissible after re-identification of the pseudonymized data.

- Ultimately, a reliable model for pseudonymization must be developed in order to prevent the possibility of re-identification with the exception of the specified and legally permissible purposes.

The T-IP performs the task of pseudonymization according to a model designated here as the "*conception of knowledge distributed to different roles,"* the essential features of which will be summarized below.

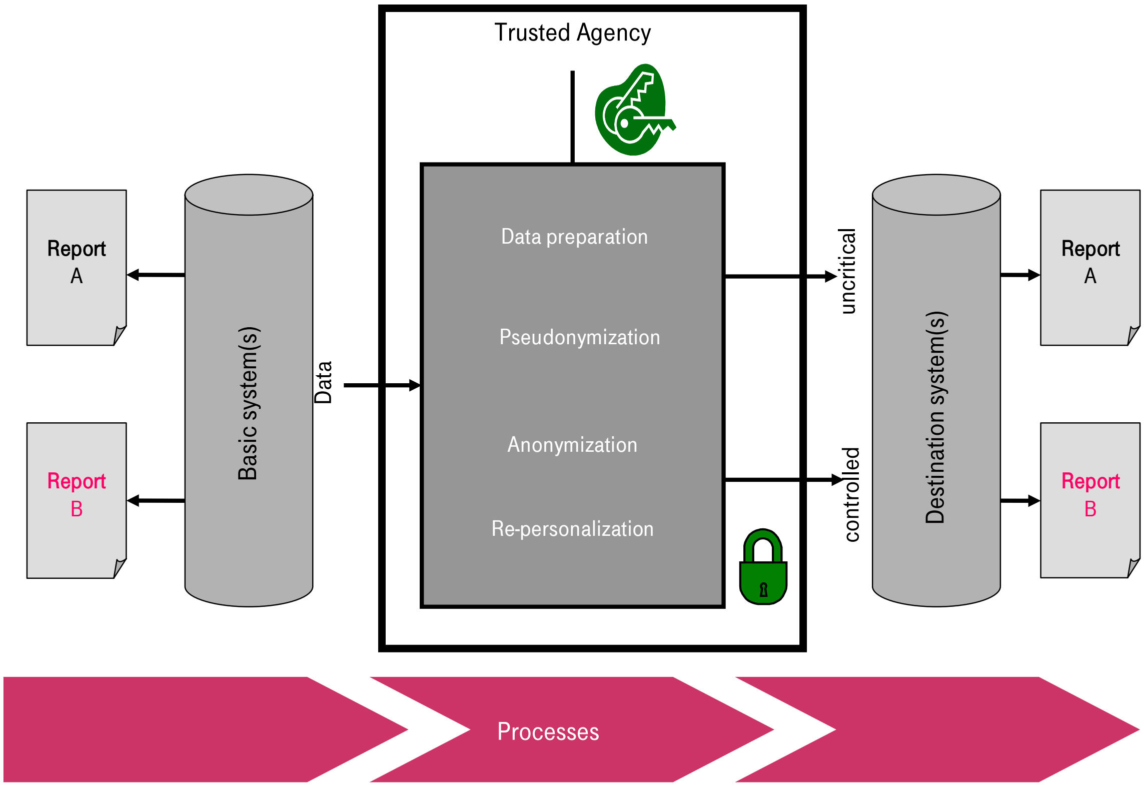
4 Conception of knowledge distributed to different roles

The principle of knowledge distributed to different roles is intended to enable effective pseudonymization and prevent unchecked re-identification. For this, the knowledge necessary for pseudonymization and for re-identification is distributed to different roles. The flow of information between these roles is regulated using technological means to prevent irregular re-identification. The security of the procedure can be increased by assigning individual roles to third parties outside of the department responsible for the T-IP.

The T-IP performs the following tasks:

- Pseudonymization
- Detection of erroneous data
- Encrypted transmission of the data to a recipient on the condition that the recipient has been reliably authenticated
- Retention of pseudonymized data for evaluation purposes
- Statistical interpretation of pseudonymized data
- Generation, administration and deletion of information for pseudonymization and re-identification
- Support of re-identification

-



T-IP: Process

Contact:

Frank Wagner

T-Systems Enterprise Services GmbH

Shared Service Center Privacy

Head of Privacy Central Functions

Hahnstr. 43d, D - 60528 Frankfurt

E-Mail: mailto:WagnerF@t-systems.com

Internet: http://www.t-systems.com