VIACRYP SERVICES

Viacryp offers Privacy Enhancing Technologies (PETs) for the purpose of the safe and monitored pseudonymisation of personal data. Through our position as a trusted third party, our clients can analyse behaviour and create (consumer) profiles while maintaining respect for privacy. Our externally-validated technology and process assure that individual customer data cannot be derived from the processed data. We also offer archive services, real-time services and anonymisation services for subsequent processing.

We advise our clients on how to take proper measures when carrying out the pseudonymisation and anonymisation of personal data. We always do this with security in mind and in compliance with the conditions and requirements established by the European Union's General Data Protection Regulation (GDPR).

SOLUTIONS (PRIVACY ENHANCING TECHNOLOGIES)

PERSONAL DATA, PSEUDONYMISED

The heart of our basic service is the pseudonymisation of personal data. To do this, we make use of irreversible pseudonyms and make as little use of behavioural data as possible. The pseudonymised data can then be further analysed by our clients.

➔ *Practical example: insight into parking pressure and mobility behavior of visitors and residents of a city*

PROPORTIONALITY IN DATA SHARING

Viacryp has developed a unique service in which data can be proportionally shared while safeguarding full privacy protection. We process only pseudonyms and encrypted (and therefore inaccessible) information. This is professionally executed in two steps. First, we use the pseudonyms as a white list. The other party delivers the pseudonyms of its customers (also in two steps) together with the relevant encrypted information. Then, we filter the information based on the anonymised white list and forward only the information of individuals who appear on the white list.

➔ *Practical example: fraud detection, proportionality, processing based on opt-ins*

PRIVACY CONSULTANCY

Viacryp offers consultancy to support its pseudonymisation services. We can assist you in determining whether pseudonymisation would be necessary and/or prudent in relation to your privacy governance. In addition, we and our partners are able to advise you on setting up a process around data use. In this way, you remain in full control, and the way you use data in your organisation is transparent, auditable and reproducible.

CUSTOMER CASES

PSEUDONYMISATION IN AN ADVANCED ANALYTICS PLATFORM
for a large telecommunications provider

Our pseudonymisation services were integrated with an advanced analytics platform belonging to a large telecom provider. Via this platform, data scientists conducted data analyses using data from various internal and external sources. We also implemented a data assessment process for this organisation. Thanks to this process, their data use is now transparent, auditable and reproducible. The data process is set up in such a way that personal data is pseudonymised in advance, minimising the impact of a data breach or unlawful processing while allowing for the optimal use of the data in data analyses.

COMBATTING FRAUD BY FILTERING DATA
for a large financial services provider

In order to combat fraud, multiple parties have to link or exchange data. A strict purpose limitation principle must be adhered to, however, and it must be proportional. Viacryp provides a service to a large financial services provider which enables parties to exchange data. We apply filtering so that only data in which there is a legitimate interest is exchanged. This happens in a way that only grants the concerned parties access to data which they have a right to access.

WIFI TRACKING WITH PSEUDONYMISED MOVEMENT PROFILES
for numerous shops and shopping centres

It can often be difficult to find your way efficiently in large shops, shopping centres and public buildings. By tracking user movements, insights can be gained into how buildings are used and the findability of particular locations. This makes it possible to improve routing. Does a user find his destination immediately, does he look first and then go to the information desk, or does he ask the information desk straight away? Which locations can be found quickly and which cannot? To more easily navigate through buildings and shopping centres, visitors need to have a unique yet anonymous user profile which can be traced as they move throughout the space. The MAC address of smartphones can be used to this end. With assistance from Viacryp's real-time service, this personal data is immediately replaced by a pseudonym in order to protect the privacy of visitors.

PSEUDONYMISATION OF NUMBER PLATES
for a large Dutch municipality

A number of Dutch cities have created municipal environmental (i.e. low-emission) zones in order to exclude polluting cars, vans and lorries from certain areas of the city. Municipal cameras are used to scan number plates to ensure compliance. When carrying out analyses of these environmental zones, the necessary data is pseudonymised to protect the privacy of the drivers.