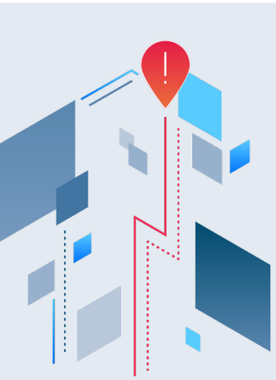
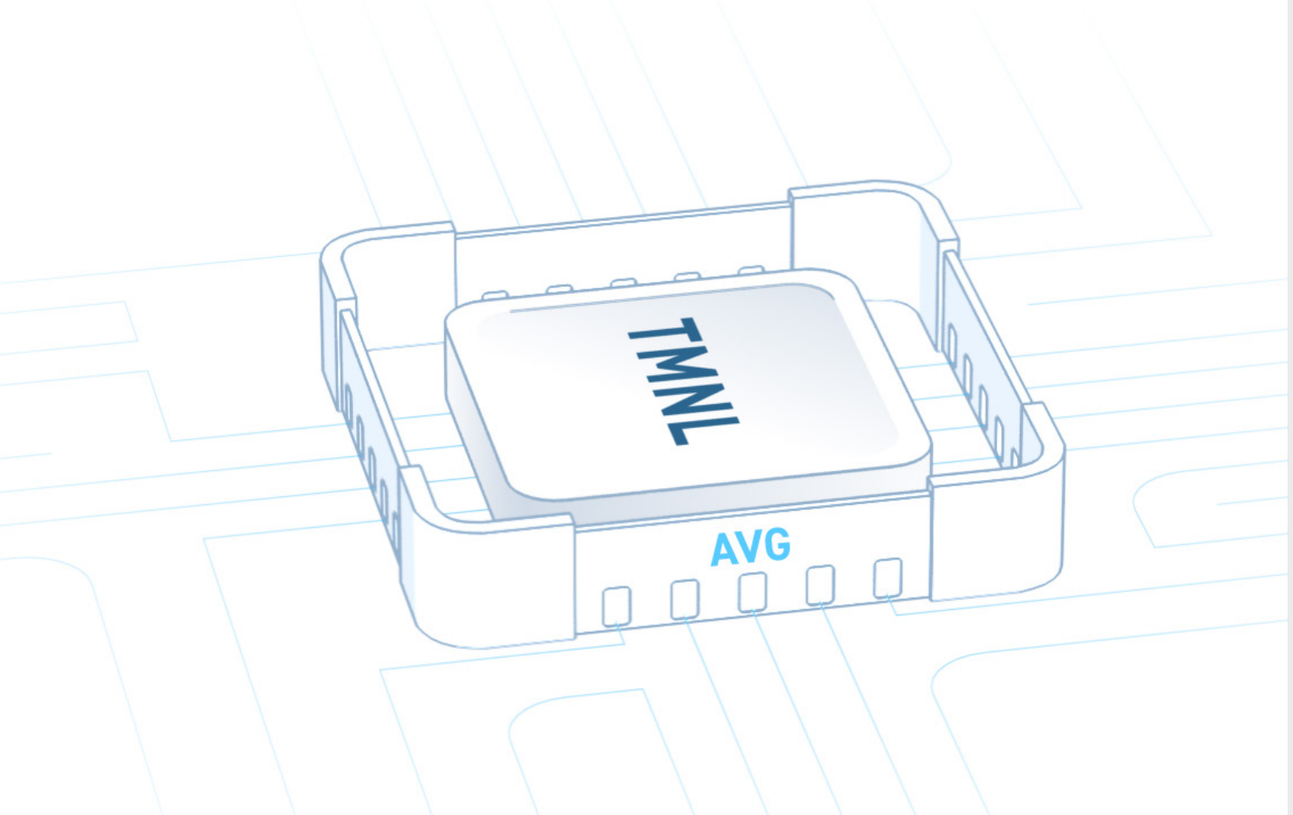


PILLAR 3

Privacy

TMNL only uses those data that are strictly essential for monitoring potentially unusual transactions. TMNL applies pseudonymisation of sensitive personal data, in order that data cannot be traced back to individual customers. Naturally, TMNL processes personal data in accordance with the General Data Protection Regulation (GDPR). At the moment, TMNL only monitors transactions by business clients.



Banks have been monitoring transactions for many years. What is TMNL doing differently?

Banks are required by law to monitor all of their customers' payment transactions. To do that, banks use transaction and customer data to detect potential signals of money laundering or terrorism financing.

But there are limits to what individual banks can see, because money laundering networks are often spread among multiple banks. TMNL brings together transaction data from individual banks to facilitate joint monitoring. This allows TMNL to be able to identify potential criminal cash flows that aren't visible to individual banks.

Which data does TMNL receive and use for monitoring purposes?

TMNL receives only the data that are absolutely necessary for monitoring purposes from the participating banks. At the moment, TMNL only monitors the transaction data of business accounts. Privacy-sensitive data, for example Chamber of Commerce numbers, IBANs or company names, are pseudonymised by the participating banks before any data is provided to TMNL. This is such that the transaction data that is provided to TMNL - such as the transaction time, destination and amount – can be used detect unusual transaction patterns, while the identity of the transacting parties is not itself known to TMNL.

How does TMNL respect privacy?

The participating banks trust TMNL with data to with the explicit goal of tackling money laundering and terrorism financing more effectively. TMNL treats individuals' privacy with the utmost care, as stipulated by the General Data Protection Regulations, or GDPR. TMNL only uses the data that are absolutely necessary for monitoring potentially unusual transactions.

The privacy-sensitive data that TMNL receives are made pseudonymous by the banks. What does that entail?

Privacy-sensitive information in the banking and transaction data is pseudonymised before being sent sent to TMNL by the participating banks. This is such that instead of a name (for example), TMNL receives a cryptographic hash of that name. This cryptographic hash then cannot be linked to a specific customer name by TMNL. TMNL uses this de-personalised data throughout the entire transaction monitoring process. When TMNL sends the bank an alert about a potentially unusual transaction, only the bank that is alerted is able to link the transaction to the original data.

The five participating banks share data with TMNL. Are the data also shared among the banks themselves?

The participating banks only share their (pseudonymised) transaction and customer data with TMNL, and not with one another. When TMNL identifies a potentially unusual transaction pattern, it sends data relevant only to that specific transaction pattern to the banks with a relation to that pattern.

TMNL has five main pillars that form the basis for everything it says and does.

Read more on tmnl.nl