PCI DSS 4.0 REQUIREMENTS AND EXATE

- Data Access Management

"Service providers and merchants must be able to control access to cardholder data."

Using eXate you can quickly and easily revoke or allow access to datasets or individual dataset attributes using the relevant techniques, for the right consumer, in the right form. eXate has been designed to fit as a part of an existing ecosystem, where proprietary data access controls can remain in parallel, and in addition to, new ABAC rules.

- Discovery and Remediation

"All such cardholder data must be protected using one or more industry-accepted techniques such as encrypted, truncation, tokenisation or hashing."

To enable the fastest possible ways to protect our data it's unrealistic to expect individuals to know the risks associated with each data attribute and the context it is being used. The eXate platform can analyse a data estate and based upon our analysis and industry models advise of any privacy or security issues or risks that may exist and automatically remediate if necessary.

eXate is an aggregator of Privacy Enhancing Techniques to ensure that data is protected in the right manner, for the right person, in the right job function, in the right location.

- Policy Management

"Implementing and maintaining an information security policy for all employees and other relevant parties."

All policies relating to data sharing can be captured in eXate. This includes policies from departments such as the Data Protection Officer (DPO), Compliance, Legal, the Chief Information Security Officer (CISO), and others, for internal data sharing, external data sharing, and cross border data sharing. As opposed to storing these policies in a Word document or PDF on the Intranet, and leaving the wording open to interpretation, the policies are automatically and consistently applied in the eXate platform.

- Audit and Reporting

"All access to cardholder data must be logged, including both successful and unsuccessful attempts."

The data flowing through the eXate platform is audited on a granular attribute by attribute basis. Items audited include who tried to access the data, for what purpose, was access granted, if not, then why, and what rules were in place at any time historically.

Additionally, eXate can protect log files with emergency break glass access to specified people.