Teleran Addresses 5 Critical GDPR Mandates

Data Protection Assessment (Article 35)	Purpose Limitation (Article 5-1 b)	Data Security & Integrity (Article 5-1 f)	Accountability & Documentation (Article 5-2)	Breach Notification (Articles 33/34)
Audit where PII exists, how used, by whom. Identify / remediate gaps.	Confirm PII use limited to stated purpose and no other.	Protect PII from unlawful use, manipulation, destruction or loss.	Demonstrate and document compliance processes.	Establish process to: Identify data breaches. Notify authorities / citizens of breach.
Teleran				
Discovers and classifies PII. Audits who accessing PII to identify / remediate compliance gaps.	Monitoring documents adherence to purpose limits.	Monitoring / controlling PII access and use to ensure protection.	Audit reports demonstrate, document compliant PII access / control.	Identifies and alerts to suspected or actual PII breaches.
Applies access control policies to protect PII and ensure GDPR compliance.	Access controls enforce purpose limits, preventing inappropriate use/users/apps.	Delivers access policies to prevent: illegal data use, data manipulation, destruction.	PII access control and testing processes prove protection measures and GDPR-compliancy.	Documents breach activity for notification. Applies new control policies to prevent future like breaches.

Supports Oracle, DB2 (LUW/z), Teradata, SQL Server, Hadoop (Q3 2017)