Kony Statement of Direction

Compliance with EU General Data Protection Regulation (GDPR)

Overview
The EU General Data Protection Regulation (GDPR) is the most significant piece of European privacy legislation in the last twenty years. It replaces the 1995 EU Data Protection Directive (European Directive 95/46/EC), strengthening the rights that EU individuals have over their data, and creating a uniform data protection law across Europe.

Where Do We Stand?
We are committed to address EU data protection requirements applicable. These efforts have been critical in our ongoing preparations for the GDPR.

Third-party audits and certifications: Kony has been successfully assessed against ISO 27001:2013. Here are ways ISO 27001 helping Kony Inc achieve GDPR compliance.

- ASSURANCE

The GDPR recommends the use of certification schemes such as ISO 27001 as a way of providing the necessary assurance that Kony is effectively managing its information security risks.

- NOT JUST PERSONAL DATA

ISO 27001 follows international best practice and helped Kony put processes in place that protect not only customer information but also all our information assets, including information that is stored electronically on cloud on premises and in hard copy format. Kony considers Privacy by Design, when working on adding new product features, we follow widely accepted models of threat risk analysis and data flow design review by architects and security subject matter experts, this ensure we provide the end developers of our apps with necessary tools and tricks to build privacy into an app which meets the most stringent of privacy regulations and privacy laws followed across the globe. We periodically analyse the kind of data an app collects and work with architects to build around the requirements of protecting against PII data elements from entering out analytics engines.

- CONTROLS AND SECURITY FRAMEWORK

The GDPR stipulates that organisations should select appropriate technical and organisational controls to mitigate the identified risks. The majority of the GDPR's data protection arrangements and controls are also recommended by ISO 27001. We have detailed, defined process controls looking in to various aspects of security such as:

- Access control
- Password management
- Patch management
- Vulnerability Assessment
- Penetration testing
- Asset Management
- Incident Management (Breach notification to customer and support investigation)
- Business Continuity and Disaster Recovery

- PEOPLE, PROCESSES AND TECHNOLOGY

ISO 27001 encompasses the three essential aspects of information security: people, processes and technology, which means we are protecting our business not only from technology-based risks but also other, more common threats, such as poorly informed staff or ineffective procedures. Our processes are built on security principles such as:

- Principle of least privilege
- Secure defaults,
- Fail securely
- Don't Trust Services

- Attack surface reduction
- Keep Security simple and avoid security by obscurity
- Fix issues correctly
- Defence in depth (encryption, anonymization,etc)

- ACCOUNTABILITY

ISO 27001 requires our security regime to be supported by top leadership and incorporated into the organisation's culture and strategy. It also requires the appointment of a senior individual who takes accountability for the ISMS. The GDPR mandates clear accountability for data protection throughout the organisation. We have dedicated teams who work on security and privacy requirements of the organization and the customer.

- RISK ASSESSMENTS

ISO 27001 compliance means conducting regular risk assessments to identify threats and vulnerabilities that can affect your information assets, and to take steps to protect that data. The GDPR specifically requires a risk assessment to ensure an organisation has identified risks that can impact personal data.

- CONTINUAL IMPROVEMENT

ISO 27001 requires that our ISMS is constantly monitored, updated and reviewed, meaning that it evolves as your business evolves using a process of continual improvement. This means our ISMS will adapt to changes – both internal and external – as you continually identify and reduce risks. We constantly keep updating the internal process and controls to meet the ever evolving external threat landscape, our secure software development lifecycle is based on OWASP guidelines on secure coding and testing with continuous integration, automated source code analysis and customer security queries on technical and compliance aspects of our products.

- TESTING AND AUDITS

Being GDPR-compliant means an organisation needs to carry out regular testing and audits to prove that its security regime is working effectively. Kony ISO 27001-compliant ISMS is regularly assessed according to the internal audit guidelines provided by the Standard. We are constantly audited by the best teams in the industry such as BSI, Ernest and Young, Cigitel, CheckMarx, Veracode .

- CERTIFICATION

The GDPR requires organisations to take the necessary steps to ensure the security controls work as designed. Kony having achieved accredited certification to ISO 27001 delivers an independent, expert assessment of whether you have implemented adequate measures to protect your data. We are also attested against the SOC 2 Type II security trust principles every year. Our customer facing infrastructure is PCI DSS V3.2 compliant.

Kony has also been issued SSAE16 SOC 2 Type 2 report. The report offers independent verification that our security practices offer a recognized standard of security measures. Furthermore, the program is designed to cover key elements of data processing and integrity, while maintaining auditing practices within our business and operational processes. As all customers are concerned with their data and its security, Kony has integrated its SOC controls into its operating procedures. These procedures span the organization, teams or functions that provide service or support to our clients on our platform.

Kony's is PCI DSS certified which establishes a set of controls for keeping cardholder data secure, supported by a regulatory framework. PCI DSS provides a head start in meeting the sixth principle of the GDPR (integrity and confidentiality). This principle requires data controllers and processors to assess risk, implement appropriate security for the data concerned and, crucially, check on a regular basis that it is up to date and that controls to protect it are working effectively.

Commitment Statement

Based on the security controls across these 3 standards, the majority of the requirements for GDPR are already in place. Kony will comply with applicable GDPR regulations when they take effect on 25th May 2018. Working in conjunction with our clients, we will explore opportunities within our services offerings to assist our customers to meet their GDPR obligations.