GENERAL DATA PROTECTION REGULATION

TechDefcon Readiness
2017
GDPR – Enterprise Challenges

Can I find all PII?

What is the Data Usage?

Is Data compliant with Privacy Regulations?

What Data belongs to Whom?

What is my Data Risk?

How and Where is Data processed and stored?

How is PII Data interconnected?

Was I breached?

Who has been Impacted?

How do I reuse & operationalize PII Data?

You Can’t Protect what you can’t find

You can’t Govern Data without Data Intelligence
The Core Values

That build our business - Delivered through a platform based approach using UDMF, TAP, DQMF, and other platforms.

- Stack Migrations
- ERP Migrations
- Data Integrations
- Data Archivals
- Warehouse Migrations

Data Governance
- Data Quality Management
- Data Analysis & Enrichment
- Keep it Clean (KIC)
- Problem Management
- Data Health Dashboards & Quality Blueprints
- Data Anonymization/Masking
- Test Data Management
- Data Reconciliations
- Master Data Management

Data Analytics
- Big Data Solutions
- Technology Implementations
- BI and Analytics

- Protect: EU citizens personal data
- Control: is provided to data subjects over their processed data
- Unify: the duties and responsibilities of controllers and processors
- Simplify: the means of data collection and processing
GDPR Value Proposition Across CPO / CDO / CSO

**PRIVACY (CPO)**
- GDPR Compliance
  - Automate Compliance
  - Regulator Reporting

**DATA (CDO)**
- GDPR Compliance
  - Automate Compliance
  - Regulator Reporting

**SECURITY (CSO)**
- De-Risk PII
  - Identify unprotected PII
  - Map usage & access

**PII Inventory**
- Build PII inventory
  - Identity
  - Residency
  - Application

**Data Quality /Governance**
- Simplify data mapping
  - Race relationship across identity attributes
  - Resolve ID entity differences across businesses

**Smart Enforcement**
- Data security
  - Enhance data security tools with risk & data awareness

**Data Flow Map**
- Document data usage
  - ISO
  - GDPR
  - HIPAA
  - Data stewardship needs

**Data Virtualization & Reuse**
- Isolate DB’s from dev access
  - Make ID data into a service
  - monetization

**Breach Response**
- Automate
  - Identify whether you were breached,
  - who was impacted,
  - where it occurred
Advisory Services (Consulting & Compliance)

We offer Advisory, Protection, Monitoring & Remediation services in our portfolio.

Strategic Consulting Services
- Digital Transformation Security Consulting
- IIoT SCADA Systems Consulting
- Enterprise Security & Information Protection Maturity Assessment (Security Assurance)
- Security Governance, Policies, Procedures
- ESRM awareness and change management
- Enterprise Security Architecture Review
- Data Classification/Protection/Privacy Governance/Leakage
- Cryptography Consulting

Operational Consulting Services
- Privacy Compliance Officer
- Inventory and classification of information assets
- Security risk assessment

Audit & Assessment Services
- Cloud Compliance Assessment
- CLOUD-BASED Application security testing
- Data Discovery Assessment/Data Security Compliance consulting
- Security audits (org, configuration, architecture)
- Governance & Regulatory compliance
- Third Party Security Assessment
- General Data Protection Regulatory
Data Privacy Compliance Framework

Privacy Governance

Privacy Program Management
- Privacy Strategy
- Data Discovery
- Data Classification
- Data Flow Mapping
- Privacy Impact Assessment
- Privacy Policy & Procedure

Privacy Operations
- Consent Controls
- Data Breach Reporting
- Pseudonymisation
- Infosec Controls
- Privacy Impact Assessment
- Monitoring & Compliance

Privacy Policy & Procedures (People, Process, Technology)

People
- Awareness
- Communication
- Support

Technology
ESRM Approach

Phase I – GDPR Readiness Assessment (8-12 weeks)
- Data Discovery
- Data Classification
- Data Mapping
- Privacy Impact Analysis
- Risk Analysis (Architecture & Controls)

Phase II – GDPR Solutioning & Implementation (20-24 weeks)
- Identify new & improved measures, both technical and organizational towards reduction of risk
- Determine priorities and actions towards implementation of measures
- Define privacy organization, policy & procedure
- Data Anonymization Techniques
- Data Retention /Erasure
- Setup automated data governance process compliance tracking
- Establish assurance via auditing of the effectiveness of the measures covering internal and third party

Phase III – Manage GDPR Privacy Operations (ongoing BAU)
- Monitoring of Privacy Rules & Compliance
- Privacy by Design - Architecture
- Privacy Impact Assessment & Assurance
- Automate Privacy Compliance
- Breach Notification & Response
Data Privacy Organisation Setup

- Inform and advise the controller or the processor and the employees who carry out processing of their data protection obligations
- Monitor compliance with the GDPR and other data protection provisions. Provide advice where requested as regards the data protection impact assessment
- Cooperate with the supervisory authority
- Act as the contact point for the supervisory authority on issues relating to processing, including prior consultation and to consult, where appropriate, with regard to any other matter

GDPR Implementation

- Define Data Privacy Policy
- Develop & document the processes around Data Privacy
- Develop & document the procedures aligned to GDPR requirement
- Rights of Data Subject
- Data Portability & Transfer
- Consent & Data Usage
- Data Redaction / Masking
- Data Retention & Erasure
- Data Anonymization Techniques
- Security Controls & Protecting PII/SPI
- Incident Management & Reporting
- Monitoring Data Access
- Privacy by design

Key Deliverable

- Data Privacy Policy
- Data Security Process & Procedures
- Architecture Design Guidelines
- Non Functional Requirements
- Data Redaction & Encryption
- Data Retention Policy & Procedures
- Data Anonymization / Masking Guidelines
- Security Controls Enforcement
- IR & Handling Process Document
- Access Monitoring Controls
- User Awareness on Data Privacy
## Data Anonymization: ESRM Approach

### Need for Anonymization
- Regulatory compliance on data privacy and handling mechanisms
- Requirement for easy and appropriate levels of access to data for different stakeholders in/outside the organization including 3rd parties
- Data protection and security requirements
- Secondary usage of data for monetization

### Our Solution
- Data Anonymization Platform (DAP) to enable customers to jumpstart anonymization, data masking
- Anonymization Platform enabled by in-house built reusable library in conjunction with various open source platforms
- Proven solution that delivers high levels of performance and security
- Use of Hadoop technologies and platforms to achieve the flexibility & scalability
- An effective Jeopardy and Fallout Management
- Ability to handle huge amounts of data in near real time

### Benefits
- Reusable components leading to minimal time spent on development, reduced cost and quicker time to market
- Goodwill and customer trust through transparent usage policies as a result of anonymization
- High preparedness to comply with Data Protection laws and reforms saving potentially huge amounts in legal expenses and penalties
- Analytic Insights to formulate effective market strategies by identifying key trends and themes in data; Use real-time aggregation of anonymous customer data in multiple ways
- Monetization of existing data and new revenue stream; Potential for multiple new revenue models
TechDefcon Analytics Platform (TAP*)

Data Sources
- Streaming data
- Logs
- EDW
- Database
- MQ
- Website
- Web service
- Social Media
- Others

Data Lake Store
- Structured Data
- Unstructured Data
- Semi-Structured Data
- Time Sliced Data

Organize
- Data Transformation
- Data Quality
- Data Aggregation
- Data Correlation

Analytics engine
- Predictive
- Descriptive
- Recommender
- Mining
- Machine learning
- NLP

RDBMS
- Reports
- Queries

Analytics DB
- Dimensions
- Fact
- Cube
- Star schema

Near Real-time
- Analytics
- Filtering
- Data Transformation
- Data Indexers
- Real time search
- Complex Event Processing
- In Memory Analytics

Error Handling
- Workflow, Schedule & Automation
- Metadata Management

Monitoring & Tuning
- Reporting & Visualization

Reusable Components
- Pre-defined data model
- Pre-build transformations
- Advanced analytic algorithms
- Visualization templates

Reusable Components
- Pre-defined data model
- Pre-build transformations
- Advanced analytic algorithms
- Visualization templates
Technical Features

- Built for scalability using distributed processing platforms with Big data based technologies
- In-memory processing without persisting data anywhere before anonymization
- Choice of low cost open source or best of breed technologies
- In-built cross-cutting features to easily manage and monitor the platform
- Adherence to Service Oriented Architecture standards
- Security compliance with standards, like, PCI, ISO, HIPAA, RSA, PKCS

Functional advancement

- Deployed more than 50 variations of functional flows using different configurations for major telecom player
- Implemented advanced hashing (SHA5), encryption (RSA, ECC, AES) mechanisms with unstable seeds and keys for higher degree of data hiding
- Implementation of advanced algorithms K-Anonymity (K-5 to 1000), L-Diversity, and T-closeness for greater degree of anonymization
- Implemented API based (web services) interaction with different loosely coupled service components following SOA reference architecture for a telecom major
- Build in multi-tenant user management with O-Auth and JaaS implementation

Non-functional achievement

- Implemented for a European telecom major to process ~1 billion orders/per day, totalling to over 600GB of data per day.
- Deployed for a European telecom major in distributed cluster of 10 nodes for horizontal scalability using platforms like Apache Storm, Apache Hadoop.
Applicable Use Cases

**Data monetization with external parties**
- Anonymization and enrichment of data
- Allowing access of data with K-anonymity/ L-diversity proofing

**Data sharing with vendors**
- Generation of masked/anonymized datasets from actual data
- Controlling visibility of information with controlled lifespan of anonymization

**Third-party Analytics**
- Required for the purpose of getting analytics done on anonymized data
- Enables sending of entire (unmasked/ non-generalized) data for analytical purposes
- Controlled access to the data with layered encryption mechanism

We Partner with Companies from Around the World
We offer Advisory, Protection, Monitoring & Remediation services in our portfolio.
Thank You

• Contact us: sales@techdefcon.com