GDPR - The Role of Mobile Device Management

Angelo Chrysanthou
Information Security Manager

treatwell

Security of Personal Data

Confidentiality

Integrity

Availability

Security of Processing -Article 32

1. Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
   b. The ability to ensure the ongoing **Confidentiality**, **Integrity**, **Availability** and resilience of processing systems and services

2. Appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed

GDPR & ISO/IEC 27001

ISO/IEC 27001 Annex A

- **A.6 Organisation of information security** –controls for mobile devices and teleworking
- **A.8 Asset management** – controls related to inventory of assets
- **A.9 Access control** – controls for user access management, system and application access
- **A.10 Cryptography** – controls related to encryption
- **A.11 Physical and environmental security** – controls defining protection against threats, equipment security, clear desk and clear screen policy
- **A.12 Operational security** – controls related to malware, backup, logging, monitoring, installation, vulnerabilities

treatwell

Mobile Device Management and Apple

Jamf Pro

- Encrypt Drive
- Asset Management
- Location Tracking
- Screen Lock
- Password Policy
- Lockout after failed attempt
- Unlock/Unlock Device
- Control/Prohibit USB devices
- Access to System logs/activities
- System Integrity Protection and reporting
- System Patches & Application Patching
- Licence Management
- Reporting/Managing Xprotext – Protection for Potentially Unwanted Programs
- Firewall Status On/Off

treatwell