ODYSSEY™
Impossible Challenges, Possible Solutions

MSS / MDR Services for GDPR Compliance

Mr. Angelos Printezis | Head of Services | IthacaLabs™

April 2018

Agenda

1. Who We Are
2. MSS/MDR Line Of Services
3. General Data Protection Regulation – Key Requirements
4. How MSS/MDR can help You meet GDPR compliance
5. Conclusion

ODYSSEY™

Who We Are

Founded in 2002

Odyssey was founded in 2002 with the main objective to provide High-Quality, Cutting-Edge, Cybersecurity, Managed Security and Risk Management Services to organizations that value their information assets.

Regional Leader

In the provision of **Information Security Solutions, Services and Products**, helping organizations in effectively and efficiently manage Information Risk.

Offices

Headquarters Nicosia-Cyprus, Athens-Greece, and **New York-USA** as well as an extensive international network of **Value Added Resellers and Distributors** of the ClearSkies™ NG SIEM and Managed Security Services.

Certifications

Certified with **ISO 27001** and accredited by the Payment Card Industry Security Standards Council (PCI SSC) as a **Qualified Security Assessor (QSA**) and an **Approved Scanning Vendor (ASV).**

Who We Are – Our People

- Currently we employ more than 120 highly skilled professionals
- Their **Talent, Experience** and **Dedication** drives our success
- They possess:
  - Extensive Education
  - Deep Knowledge & Expertise
  - Hands-On Experience

Our motto:

Impossible Challenges, Possible Solutions

“There’s really nothing we can’t accomplish if we put our mind to it”

MSS/MDR Line Of Services

MSS/MDR Line Of Services

- Delivering **Managed Security Services (MSS) & Managed Detection and Response (MDR)** services using Odyssey's award-wining **ClearSkies™ Big Data Security Analytics Platform** to help organizations address:
  - **Targeted Attacks** and **Data Breaches** from diverse threat vectors
  - Meet compliance obligations for ISO 27001, PCI DSS, SWIFT & GDPR

MSS/MDR Line Of Services – PCI DSS 3.2

ODYSSEY™

MSS/MDR Line Of Services – ISO 27001

ODYSSEY™

MSS/MDR Line Of Services – SWIFT

MSS/MDR Line Of Services – GDPR

ODYSSEY™

The Cybersecurity landscape is evolving every day…!

Odyssey's MSS/MDR Services help your organization:

- **Predict, Detect, Prevent** and **rapidly Respond** to cyberattacks for protecting your data, trade secrets and reputation
- **Meet Compliance requirements**

ODYSSEY™

Streamline your Threat Management Process with MSS/MDR

Significantly accelerates your **proactive Cyber-Threat Detection and Response capabilities**, thus drastically reducing your "**Detection Deficit**" (time between breach and discovery)

ODYSSEY™

General Data Protection Regulation – Key Requirements

General Data Protection Regulation – Key Requirements

Applies to **all companies worldwide, either European or not, that store and process Personal Data of European citizens**.

- 72-hour notification for breaches related to personal data
- Fines of up to **€20 million or 4% percent of annual turnover**, whichever is greater, for infringements such as:
  - Failure to comply with basic principles
  - Failure to notify of a personal data breach
  - Etc…..

General Data Protection Regulation – Key Requirements

- Inventory of all personal data processed
- Increased rights for data subjects, i.e. the right to “be forgotten” and data portability
- Software developed with security in mind *(privacy by design and by default)*
- Pseudonymisation or encryption of personal data *(privacy by design and by default)*
- Secure processing of data

How MSS/MDR can help You meet GDPR compliance

How MSS/MDR can help You meet GDPR compliance

Article 25
Data Protection by design and by default

Requirement:
Data privacy by design means that appropriate organizational and technical measures to ensure personal data security and privacy are embedded into the complete lifecycle of an organization's products, services, applications, and business and technical procedures. Technical measures can include, but are not limited to, pseudonymization and data minimization.

Data privacy by default means that (a) only necessary personal data is collected, stored, or processed and (b) personal data is not accessible to an indefinite number of people.

Help your organization monitor the **status of your personal data security and privacy** by leveraging features such as

- Asset Inventory
- Privileged User Activity Monitoring
- User Rights Monitoring

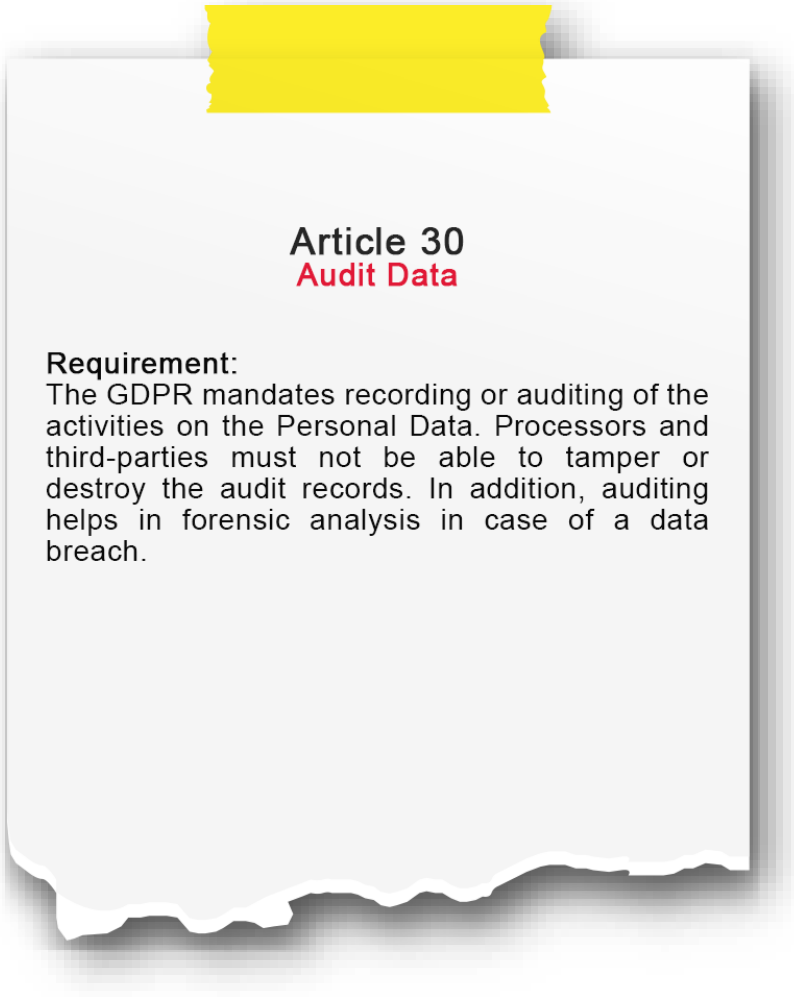
ODYSSEY™

How MSS/MDR can help You meet GDPR compliance

ClearSkies™ Big Data Security Analytics Platform helps you meet these requirements by leveraging the following capabilities:

- **Privileged user monitoring**: Monitor privileged user access and activities throughout the enterprise by utilizing UEBA (User Entity Behavioral Activity)
- **User rights monitoring**: Identify excessive, inappropriate, and unused privileges
- **VIP data privacy**: Monitor strict access controls on highly sensitive data, including data stored in enterprise applications (i.e SAP and PeopleSoft)
- **Data masking**: Mask sensitive/confidential data found within log data collected for safeguarding confidentiality
- **Assets Inventory**: Create a group/inventory of critical assets that store or process sensitive data, for reporting purposes
- **Vulnerability assessment**: Import VA scan reports for more accurate correlation
- **Compliance status**: Use ServiceModule that contains report templates for PCI DSS, ISO27001, FISMA, HIPPA, GDPR as well as custom reporting

How MSS/MDR can help You meet GDPR compliance



Help your organization to constantly monitor activities on the Personal Data and provide records of security events and Threat Intelligence, documenting the **who**, **what**, **when**, **where**, **why**, **how** and **how much data**, thus facilitating the whole forensic investigation.

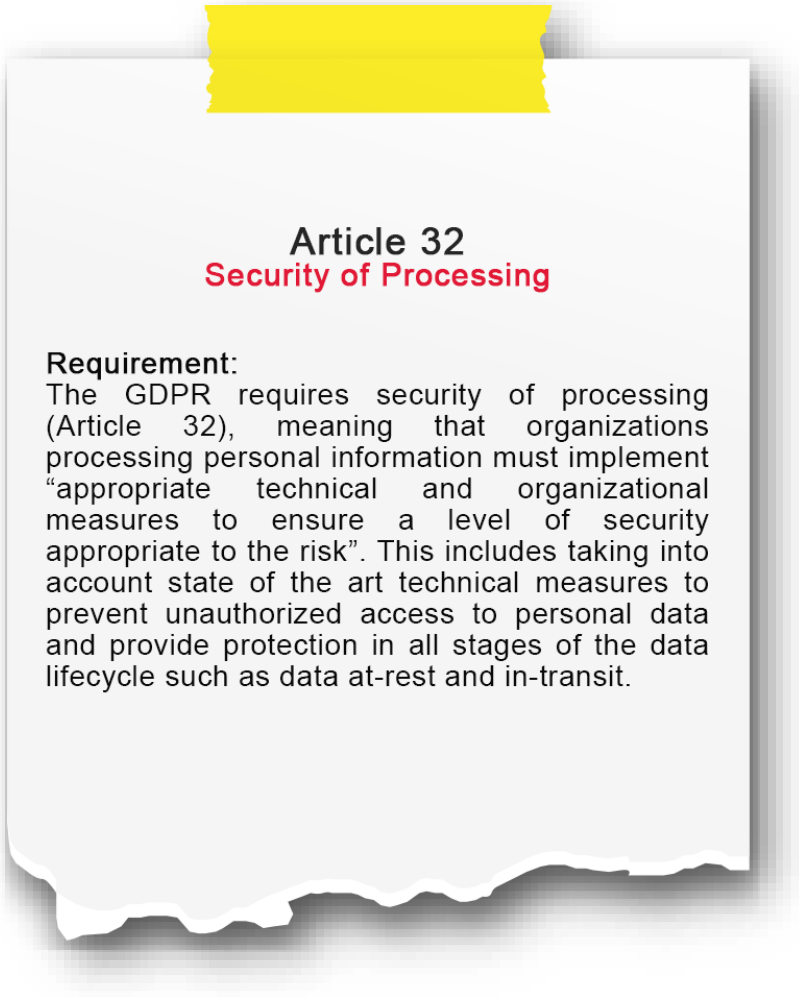
ODYSSEY™

How MSS/MDR can help You meet GDPR compliance

ClearSkies™ Big Data Security Analytics Platform helps you meet these requirements by leveraging the following capabilities:

- **Asset discovery**: Detect unknown systems on the network
- **File integrity monitoring (FIM):** Detect changes in critical files and suspicious user activity
- **Threat Intelligence**: Integrate with Odyssey's IthacaLabs™ for Threat Intelligence feeds and Incident Response assistance for emergency threats
- **Advanced Correlation**: Apply dynamic, evidence-based correlation through security/networking/applications, from across the network
- **Digital signing and encryption**: Utilize raw log data for forensic investigation purposes and/or legal evidence should the need arise
- **Assets Inventory**
- **Privileged user monitoring**

How MSS/MDR can help You meet GDPR compliance



Help your organization generate insights from the machine data **to provide early warning of threats to your IT infrastructure.**

Your environment produces massive volumes of activity logs that can be used to **identify anomalies in user behavior and detect unauthorized access**.

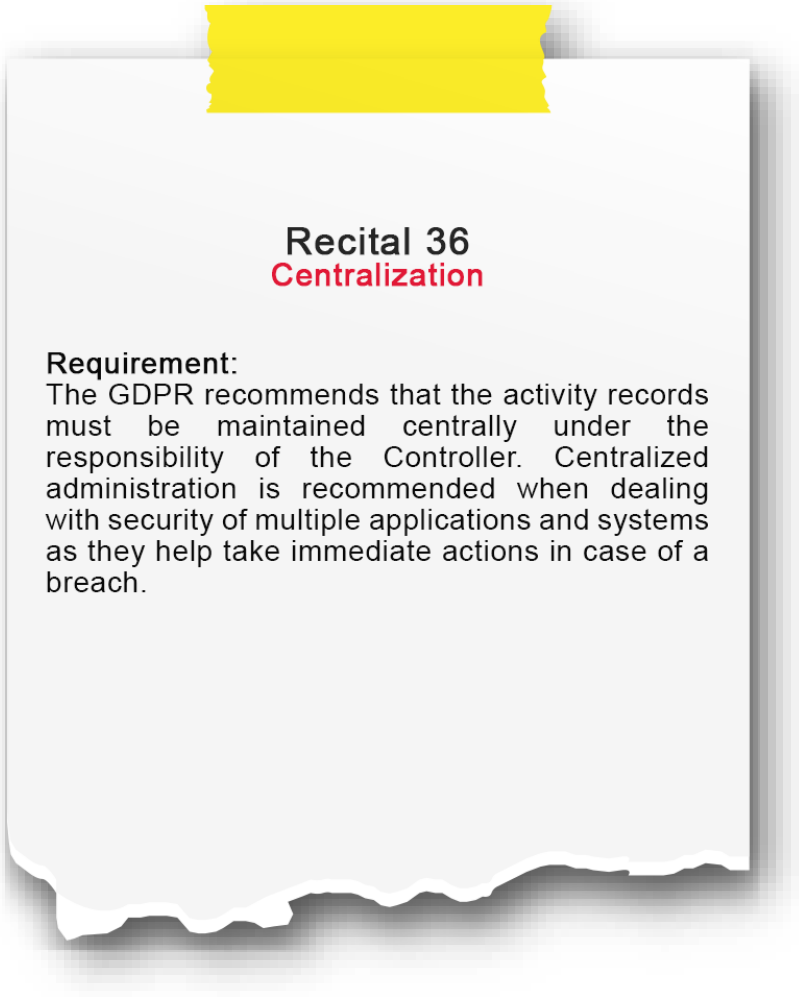
ODYSSEY™

How MSS/MDR can help You meet GDPR compliance

ClearSkies™ Big Data Security Analytics Platform helps you meet these requirements by leveraging the following capabilities:

- **Network activity monitoring**: Detect unauthorized activity, identify threats as they appear and assist in mitigating them by leveraging Supervised and Unsupervised UEBA, Behavioral and Predictive/Machine Learning as well as Artificial Intelligence Analytic Models
- **Asset discovery**
- **Assets Inventory**
- **Vulnerability assessment**
- **Threat Intelligence**
- **Digital signing and encryption**

How MSS/MDR can help You meet GDPR compliance



Serve as a **centralized control** which also:

- enforces **uniformity** across multiple environments of your organization (external, internal, unique operational environments)
- **reduces the chances of false positives** on individual environments
- leverages the **best practices** across your enterprise

ODYSSEY™

How MSS/MDR can help You meet GDPR compliance

Article 33 & 34 and
Recitals 85 & 86
Notification obligation

Requirement:
The GDPR requires breach notification and communication. This means that organizations must notify supervisory authorities within 72 hours of becoming aware of a personal data breach that could harm the rights and freedoms of EU citizens (Article 33) and must notify the affected individuals without undue delay (Article 34).

Help your organization generate insights from the machine data to allow organizations **to quickly detect, investigate and scope breaches.**

Analytics allow your organization to track **how** and **when** the attacker came into the environment, **which** systems and data were accessed and **when, how many people/records** were affected and **what** remedial measures need to be taken, all of which help you meet your notification requirements.

ODYSSEY™

How MSS/MDR can help You meet GDPR compliance

Article 58
Supervisory Investigative Powers

Requirement:
The GDPR grants each supervisory authority the power to carry out investigations in the form of data protection audits and issue warnings, reprimands or bans on data processing (Article 58) and assess fines of up to €20 million or four percent of an organization's total worldwide annual turnover - whichever is greater. Additionally, Article 82 gives any person who has suffered material or nonmaterial damages the right to receive compensation. Fines can only be avoided if a party can show that it was not in any way responsible for the event giving rise to the damage.

Help your organization to find **current** and **historical information** they need to demonstrate to controllers and supervisory authorities that they had

- appropriate security controls in place and
- proactively worked to mitigate the risk

ODYSSEY™

How MSS/MDR can help You meet GDPR compliance

Article 15, 17, 18 and 28
Data Subject Rights

Requirement:
The GDPR grants EU citizens the right to know what personal data is being processed about them, with whom it is shared and where it is processed (Article 15). Data subjects can also ask that their personal data be corrected (Article 16) or deleted (Article 17). Processors are required to ensure that only authorized persons process the personal data and when the processing is complete and the contract terminated, the controller can request that all personal data be deleted or returned, including in some cases any existing backup copies.

Help your organization achieve **end-to-end visibility** into your **processing activities** – critical information for GDPR compliance.

ODYSSEY™

Conclusion

Conclusion

With the **MSS/Managed Detection and Response (MDR)** services, organizations of any size, complexity or industry, **enhance** their detection and response capabilities to "**Targeted Attacks and Data Breaches**" and **accelerate their compliance with the GDPR requirements** before it is too late.

Impossible Challenges, Possible Solutions

ODYSSEY™
Impossible Challenges, Possible Solutions

HEADQUARTERS

CYPRUS
1 Lefkos Anastasiades Str.,
2012 Strovolos, Nicosia
Tel.: +357 22463600
Fax: +357 22463563
Email: info@odysseycs.com
www.odysseycs.com

OFFICES

CYPRUS | GREECE | USA

Contact details
Mr. Angelos Printezis
aprintezis@odysseycs.com