COMCAST BUSINESS | MASERGY

WHITE PAPER

GDPR: how Masergy's Managed Detection and Response Service helps enterprises detect, report, and respond to security threats

The European General Data Protection Regulation (GDPR) became applicable on May 25, 2018. In addition to applying to entities within the European Union (EU), the GDPR has a broad territorial scope and may apply to entities outside the EU that offer goods or services to individuals in the EU or monitor their behaviour.

The GDPR and Masergy

The GDPR introduces a personal data breach notification obligation. Under the GDPR, data controllers (i.e., entities that decide the "why" and "how" personal data is processed) are required to notify a personal data breach to (i) a supervisory authority within 72 hours after becoming aware that personal data has been compromised, and (ii) where the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, they must notify affected individuals without undue delay. In addition, data processors (i.e., entities that process personal data on behalf of data controllers) are required by the GDPR to notify a personal data breach to the data controller without undue delay. These notification obligations are highly connected to an organisation's ability to detect, address and mitigate a personal data breach in a timely manner.

Masergy's Managed Detection and Response (MDR) service delivers continuous monitoring and security incident response to minimize the risk from advanced threats for an organisation.

Combined with 24/7 analysis by security professionals, Masergy's MDR service helps expel attackers before they can find and exfiltrate company information including personal data. Among others, but particularly relevant to the GDPR, Masergy MDR helps companies with:

- Breach detection and reporting;
- Breach forensics; and
- Data Protection by Design (taking data protection into account at an early stage).

What is a personal data breach?

It is important to understand what a personal data breach actually is. Under the GDPR, a personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Examples of personal data breaches, security risks, and threats that Masergy's MDR service helps organisations detect and/or mitigate include but are not limited to:

- A compromise of an organisation's network that results in a third party obtaining access to personal data or exfiltrating such data from the network;
- A compromise of a user's credentials for accessing an organisation's system that maintains personal data;
- A cybersecurity vulnerability or configuration issue associated with an organisation's products or equipment that may reasonably result in a compromise to the confidentiality, integrity, or availability of personal data processed in connection with those products or equipment;
- A security incident that leads to unauthorized use, disclosure or transmission of personal data;
- Unauthorized access to a customer account that results from a password replay attack or other method of compromise involving account credentials obtained from third-party sources;
- Phishing scams that result in unauthorized access to or disclosure of personal data;
- Installation or execution of malicious software, code, viruses or other malware that infects an organisation's systems and results in personal data being accidentally or intentionally accessed, altered or deleted; and
- Denial of service attacks that prevent or impair the normal authorized functionality of an organisation's networks, systems or applications to the extent the issue renders personal data unavailable, either permanently or temporarily.

What are the legal and practical implications of a personal data breach?

Suffering a personal data breach due to lack of appropriate security measures and not notifying it to the relevant supervisory authority or affected individuals, when required, can result in substantial fines.

In addition, a personal data breach may result in significant direct and indirect business costs for an organisation, including:

- Post-breach cleanup costs that will increase the longer it takes to detect a breach;
- Legal and forensic investigation fees;
- Public relations costs and reputational-loss-driven costs;
- Increased insurance premiums;
- Negative impact on credit ratings;
- Losses resulting from damage to client relationships; and
- Defending litigation and regulatory enforcement actions.

When a personal data breach must be notified to the relevant supervisory authority and in some cases to affected individuals, additional notification-related costs will be incurred, including:

- Preparation and transmission of notifications;
- Establishment of a call center and other communications procedures; and
- Fraud monitoring services.

Masergy integrates and unifies your disparate corporate IT security systems to deliver advanced managed detection and response solutions unique to your business

Breaches: how to be prepared

It is therefore important to understand, among other things, your business processes, who your customers are, what, how, and where personal data is being transmitted and stored, all the different personal data breach possibilities, and the resulting potential impact. Subsequently, it is important to determine how a personal data breach should be handled to learn how to reduce business risk. Once achieved, these processes must be tested and reviewed on a regular basis, and revised where necessary.

It is also important to be able to demonstrate that due diligence has been followed in regard to protecting personal data and be able to address a personal data breach in a timely manner. For instance, any missing documentation or third-party contracts may increase the impact and cost of a breach. Being able to demonstrate (through documented records) evidence of the measures taken to protect personal data should be an essential part of any organisation's GDPR journey. This could include, for instance:

- An up-to-date security incident response plan that is regularly reviewed
- An up-to-date personal data breach notification procedure and toolkit with template notifications
- Presence of security incident detection systems/ services
- Evidence that contracted third parties are taking GDPR seriously
- System event log collection to aid security incident detection and forensics
- Up-to-date company security policies
- Evidence of regular user security awareness training
- Evidence of following a data protection by design strategy

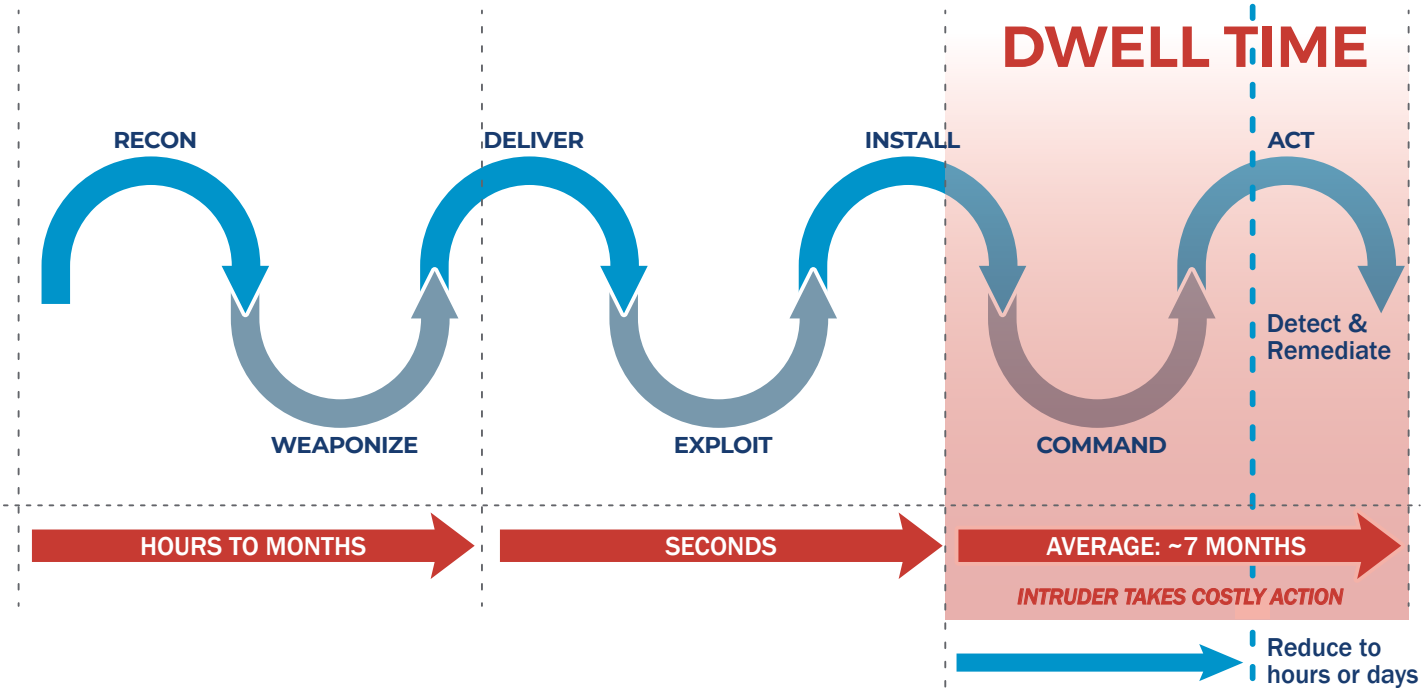
How does Masergy's MDR Service help address a personal data breach?

Breach detection and reporting

Masergy's MDR service provides early detection of security threats that could lead to a personal data breach. In addition, it helps reduce the time taken to detect actual security incidents, especially before they are detected outside of an organisation, which helps organisations promptly assess if a security incident has led to personal data being compromised. Proving due diligence and due care before, during, and after the breach detection, as well as implementing response and reporting processes are key to mitigating the risk to an organisation and affected individuals.

Expedited detection of personal data breaches requires effective technology integration to enable efficiencies and economies of scale. At Masergy, specific technologies are integrated with each other to provide these efficiencies. In addition, integration with your existing and future tools and services is key to providing further efficiencies in respect to automation, threat correlation, minimal false positives, actionable alerts and incident response. Masergy integrates and unifies your disparate corporate IT security systems to deliver advanced managed detection and response solutions unique to your business. Masergy Security Analysts assist with configuring and maintaining Masergy's MDR service in various environments to provide low false positives and actionable alerts, followed by professional remediation advice.

Although Masergy's MDR Service will detect security incidents at various stages during the Cyber Kill Chain® (see illustration below), Masergy's mission is to reduce "dwell time." Dwell time is the length of time it takes from penetration to threat detection and remediation. A reduced dwell time mitigates an organisation's risk by detection of security threats and personal data breaches at an early stage.



72-hour reporting timeline

The GDPR imposes a 72-hour breach reporting timeline. This means that once detected a personal data breach must be reported to the relevant supervisory authority within 72 hours. The breach reporting will need to include as much information as is available at the time, as well as steps that are being taken to further investigate and mitigate the breach.

To assist with the legal analysis and reporting, Masergy's MDR service can provide relevant information such as:

- When the security incident occurred;
- What type of security incident occurred;
- What personal data was affected, to the extent it is known at the time that the affected data is personal data; and
- If available within the 72-hour timeline, how the breach occurred.

HOURS

72

GDPR reporting time

Breach forensics

Masergy's MDR service can provide forensic capabilities to help organisations investigate a personal data breach by identifying the following:

- What types of personal data were impacted
- The approximate number of affected individuals and records
- The circumstances under which the personal data breach occurred
- What, if any, steps can be further implemented to prevent reoccurrence

The security analytics conducted by Masergy help identify the information listed above. They are set up during the implementation of Masergy's MDR service to support each organisation's specific circumstances and can be adjusted throughout the service contract at no additional cost.

Data protection by design

The GDPR introduces the principle of Data Protection by Design, which requires organisations to implement data protection and security measures at the time of the development or design of new products, services, and applications, and to implement measures that enable organisations to create and improve security features. The GDPR's principle of Data Protection by Design focuses on new systems and services that collect, store,

and transmit personal data. Its focus is to ensure new systems and services are designed, implemented, configured, and maintained with security front of mind. This includes securely architecting new services to withstand cyber attacks and other security incidents and the introduction of features to improve the security of the data processing.

Masergy's MDR service is aimed at fostering Data Protection by Design. It helps organisations integrate security safeguards into their data processing systems (and any systems that support them at any stage), track and report changes to critical security configurations, and improve the security posture through continuous monitoring, scanning, detection, alerting, incident response and reporting.

Masergy MDR overview

Masergy's MDR service combines its patented technology platform with continuous 24/7 security monitoring to thwart advanced persistent threats. The platform applies advanced machine learning and big data analytics across ingested data, from multiple sources, to generate a current prediction of normal behaviour for clients' unique networks. Then, Masergy's security professionals dissect all alerts and behavioural anomalies and deliver only actionable alerts to our clients. By combining the very best of machine and human intelligence, clients repeatedly confirm that Masergy becomes an extension of their team, delivering superior threat prediction, detection, and protection.

Intertrust

Legal and financial services company Intertrust Group uses Masergy's Unified Enterprise Security solution to tackle security risks and multi-country compliance demands. Explore how the IT team responds to regulations and buys back time.

VIEW CASE STUDY

Weightmans

Weightmans required more manpower and a comprehensive security strategy to make its security operations as strong as its legal team. See how Masergy's Managed Detection and Response platform delivers 24/7 monitoring and saves the IT team 144 hours each quarter.

VIEW CASE STUDY

DISCLAIMER

This whitepaper is made available for reference purposes only and does not provide legal advice. The information presented herein may not reflect all applicable legal requirements, legal developments, published guidance, prevailing market trends, regulatory actions or court decisions. These materials may be revised without notice, and Masergy Communications, Inc., Masergy Communications UK Ltd. and their affiliates are not responsible for any errors or omissions in the content of this whitepaper or for damages arising from the use of or reliance upon any information contained herein. You are encouraged to seek legal counsel for specific legal advice concerning compliance with the requirements of the GDPR or other legal requirements.

About Masergy

Masergy is the software-defined network and cloud platform for the digital enterprise. Recognized as the pioneer in software-defined networking, Masergy enables unrivaled application performance across the network and the cloud with Managed SD-WAN, UCaaS, CCaaS, and Managed Security solutions. Industry-leading SLAs coupled with an unparalleled customer experience enable global enterprises to achieve business outcomes with certainty.