INTEZER

# HOW INTEZER SUPPORTS GDPR ADHERENCE

The EU General Data Protection Regulation (GDPR) was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy[1].
Going into effect in May 2018, the regulation imposes multiple requirements on enterprises regarding personal data breaches. Intezer facilitates complying with some of the GDPR requirements in a manner that removes the burden from the enterprise.

## Stop Attacks Before the Breach Occurs

Just as enterprises invest resources to improve their security infrastructure, so do attackers invest in finding ways to bypass these security layers and successfully breach the enterprise.
It's been a while now since data breaches evolved into multi-staged, sophisticatedly planned and executed cyber-attacks. As such, organisations have "opportunities" to reveal attacks in the making before a breach actually occurs.
GDPR requires that organisations demonstrate a high level of security, to prove they are doing the necessary, to minimize the chances of a breach. Specifically, organizations are required to show they are regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the data processing (Article 32) [2].

The Intezer Compromise Assessment service conducts a, complete assessment of the enterprise network, to detect any existing malware or backdoors, within the organization's network.
Intezer's technology stands at the core of the Compromise Assessment service, ensuring detection of even the most sophisticated threats. From a stealthy code injection attempt to a full-blown Remote Administration Tool based attack, the service is designed to maximize resilience.
Intezer's Compromise Assessment service delivers a report of every suspicious, malicious or unknown file in the organization upon detection. This includes mitigation recommendations, to empower the SOC team to effectively address threats. The report also provides the information required to remediate threats across the entire organisation with vaccines.

## Detect the Hidden Cyber Attacks within Your Organization

1. Detect even the most sophisticated cyber-attack within the organization
2. Receive a report with detailed expert insights and recommendations
3. Remediate threats with effective vaccines to maximise resilience

[1] http://www.eugdpr.org/
[2] https://gdpr-info.eu/art-32-gdpr/

INTEZER

## Shorten Investigation and Speed Incident Response

It is too often that enterprises lack sufficient investigation tools, threat intelligence and human resources, to run an efficient investigation and response operation in a timely manner.
GDPR requires that organisations notify the authorities[3], as well as the data subject[4], about a data breach, within 72 hours of the breach discovery and include the following descriptions:

> The nature of the personal data breach including where possible, the categories and approximate number of data subjects and data records concerned.
> The likely consequences of the personal data breach.
> The measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Intezer Analyze™ integrates in the organisation's incident response plan and enables to quickly check and prioritize alerts, remove false-positives and keep only alerts that indicate a breach has occurred – facilitating and speeding investigation.
Based on its Code Intelligence technology™, Intezer Analyze dissects any given file or binary into thousands of small fragments, within seconds, comparing all analyzed code pieces to its Code Genome Database. Every alert is measured against the billions of code pieces in the Code Genome Database, enabling to immediately identify and classify attackers, and quickly vaccinate against specific attacks, even when only a tiny piece of code has been re-used.
The ability to classify threats and vaccinate the organisation, based on existing data, ensures fast response to threats and breaches, enabling organisations to meet the 72 hours requirement and to provide all the investigation data and attack details needed, to avoid being fined.

**Speed-Up Investigation with Intezer Analyze**

> Quickly check and prioritize alerts, and remove false-positives

> Classify threats and vaccinate the organisation, to meet the 72 hours GDPR requirement

## About Intezer

Intezer is replicating the concepts of the biological immune system into cyber security, offering enterprises unparalleled threat detection and accelerated incident response.
Intezer provides a fast, in-depth understanding of any file by mapping its code DNA at the 'gene' level -- offering the most advanced level of malware detection and analysis. By identifying the origins of every piece of code, Intezer is able to detect code reuse from known malware, as well as code that was seen in trusted applications.

www.intezer.com

[3] https://gdpr-info.eu/art-33-gdpr/
[4] https://gdpr-info.eu/art-34-gdpr/