DARKTRACE

WHITE PAPER

# General Data Protection Regulation (GDPR)

## Real-time Cyber Defense and Early Threat Detection

## Overview

On April 27th 2016 the European Council, Commission, and Parliament published the final version of the General Data Protection Regulation (GDPR), which became legally binding in all EU member states on May 25th 2018.

In material terms, GDPR defines a person and their personal data as:

> 'An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.'

In territorial terms, the law regulates any entity established or proactively offering goods and services within the European Economic Area (EEA). This will include international and cloud based offerings targeting customers in the EEA.

Additionally, the GDPR specifies that a data breach must be reported to the Data Protection Authority (and in some cases the individuals impacted) within 72 hours of becoming aware of the breach. For processors (those which, alone or jointly with others, process personal data on behalf of the controller) this means they will need to notify the controllers (those which, alone or jointly with others, determine the purpose and means of the processing of personal data) well within the 72 hour window.

> "Darktrace uses AI to spot patterns and prevent cybercrimes before they occur."
>
> **Gartner**

This requirement does mean that companies will need to adopt internal procedures to identify breaches and assess the risk in a timely manner, in order to determine if a breach is reportable.

The implementation of GDPR represents one of the most significant events in data protection regulatory history. The regulation is a game changer not only in terms of scope and ambition, but also the significant penalties for non-compliance: the fine for non-compliance can be up to 4% of global annual turnover (sales).

Darktrace is applicable to a range of requirements under GDPR. Darktrace provides the real-time visibility required to make intelligence-based decisions in live situations, while enabling in-depth investigations into historical activity.

Based on important advances in Bayesian probability theory and powered by cutting-edge machine learning, Darktrace ingests communications and creates a unique behavioral understanding of 'self' for each user and device in the organization. Like a biological immune system, it detects threats that cannot be defined in advance by identifying even subtle shifts in expected behavior.

This technology is ideally suited to detecting cyber attacks in their earliest stages before they become data breaches; even previously unknown threats that are novel or tailored. By identifying unexpected anomalies, controllers and processors are able to investigate compromises and insider risks as they emerge and throughout the stages of an attack's lifecycle.

bsi. ISO/IEC 27001 Information Security Management

Darktrace has successfully been certified with ISO 27001:2013. This internationally-recognized, third-party validation demonstrates how seriously Darktrace takes its internal security and validates the information security management system that it has in place.

CYBER ESSENTIALS

Darktrace's compliance with the UK Government-backed and industry-supported Cyber Essentials scheme further validates our approach to security. The Cyber Essentials scheme provides guidance on good cyber security practices to organizations, to ensure they are protected against the most common cyber-threats.

## A New Era in Automation

Darktrace was founded with a vision to change the way we think about cyber security. This vision is to provide an immune system for cyber security, providing organizations with evolving, internal protection and the ability to fight back against threats that penetrate the network.

Automation is central in keeping up with the quickening speed and sophistication of cyber-attacks, as humans alone are increasingly struggling to defend their networks from attackers. Machine learning is critical to how we deliver automated cyber security solutions.

Advanced machine learning can be used to analyze large data sets, and extract 'meaning', helping us to make sense of overwhelming volumes of information.

Darktrace's approach to cyber defense is based on some of these fundamental advances in probabilistic mathematics and machine learning developed by mathematicians from the University of Cambridge, the core of our technology.

This probabilistic mathematical approach is critical to Darktrace's unique ability to understand important information, amid the noise of the network – even when faced with unfamiliar activity, making it the de facto approach to address today's fast-evolving threat landscape.

> "We like the 'immune system' approach because it doesn't assume what 'bad' behavior looks like. So we don't need to have experienced a threat before, in order to be protected against it."
>
> **Stuart Berman,**
> **Information Security Architect, Steelcase**

### Enterprise Immune System

Darktrace's underlying technology is known as the Enterprise Immune System, and is now recognized as the de facto approach to address today's fast-evolving threat landscape of potential attackers or insiders.

Darktrace's Enterprise Immune System delivers this style of 'immune system' defense to the enterprise, for the first time. Based on proprietary, unsupervised machine learning and AI algorithms, Enterprise Immune System technology learns 'self' for an organization, its users and its devices, by continually calculating probabilities in the light of ever-changing evidence. As such, it has become the only technology capable of defending against 'unknown unknown' threats and insiders that start going awry.

The technology works by analyzing network traffic and learning a 'pattern of life' for every network, device and user, modeling them as they go about their normal, day-to-day activity. It then employs powerful correlation techniques to classify and cross-reference these models, in order to establish a highly accurate understanding of 'normal' activity within that particular environment, and identify deviations from this 'norm' that are deemed significant.

Like the human immune system, Darktrace's Enterprise Immune System does not require previous experience of the threat, or pattern of activity, in order to understand that it is potentially threatening. No rules or signatures are needed. Instead, its sense of 'self' means that it can dynamically spot anomalies as they emerge, and even take measured action to curb the threat.

### Key Benefits

Darktrace is the only cyber defense technology that is capable of detecting anomalous behaviors without any prior knowledge of what it is looking for.

- **Adaptive** – evolves with your organization
- **Self-learning** – constantly refines its understanding of normal
- **Probabilistic** – works out likelihood of serious threat
- **Real-time** – spots threats as they emerge
- **Works from day one** – delivers instant value
- **Low false positives** – correlation of weak indicators
- **Data agnostic** – ingests all data sources
- **Highly accurate** – models human, device and enterprise behavior

## Breach Notification within 72 Hours

The GDPR introduced a duty for all organizations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected. If the breach is sufficiently serious to warrant notification to the public, the organization responsible must do so without undue delay.

> **A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stores or otherwise processed.**

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organization becoming aware of it. For processors this means they will need to notify the controllers well within the 72 hour window.

The Ponemon Institute found that the average time to identify a data breach is 201 days and the average time to contain a data breach is 70 days. This requirement does mean that companies will need to adopt internal procedures to identify breaches and assess the risk in a timely manner, in order to determine if a breach is reportable.

The ability to detect unusual behaviors or anomalous activity early, as it emerges, is therefore critical. Darktrace's threat detection capability uses a self-learning approach, and it can accurately pinpoint genuinely suspicious behaviors, against its evolving sense of 'normal' behavior.

> **Darktrace analyzes 100% of network traffic, allowing a full overview of all machine and user activity within an organization's infrastructure in real time.**

Real-time visualization of your environment and potential threats helps the process of understanding threat within the context of your day-to-day business activities, and improves analysts' ability to uncover vulnerabilities before they are exploited.

The ability to monitor and investigate the network in an intuitive and digestible way lies at the heart of Darktrace's user interface. Visualization technology gives an unprecedented view into your organization.

Darktrace's fully interactive visualization tool not only provides a high-level oversight of threat levels, but also allows you to dive deep into granular details, such as specific connections of particular devices, or the pace of data transfers outside the organization.

Darktrace is uniquely capable of mitigating threats by facilitating their discovery and limiting their spread. Key to this is that an unknown threat does not go unseen. Darktrace does not use signatures or patterns in the same way as a firewall or antivirus.

Designed to work in all sizes of organizations, from small businesses to large and complex networks with tens of thousands of users, Darktrace's technology filters out the noise in your network, automatically finding the threats that routinely bypass legacy security tools.

> "Darktrace is the clear leader in anomaly detection."
>
> **451 Research**

## International Data Transfers

The GDPR require that protection of personal data should not be undermined when transferred to countries outside the EEA, and should be carried out in compliance with the regulation.

Given that GDPR applies to all EU citizens, and not just data processed in the EU, the rules around international transfers will become more relevant.

The increasing use of cloud services blurs the picture further as it breaks down geographical barriers, but EU regulation retains very strong geographical boundaries.

Darktrace's ability to identify anomalous behaviors includes data transfers both within a company's network, and to external sources.

Across our customer base, Darktrace has detected a wide range of different anomalies. For example, Darktrace identified that one of the company's database servers was repeatedly allowing unencrypted connections from various internet locations. These machines were using a range of IP addresses allocated to a telecoms company in the Far East. Darktrace's processing of these connections suggested that the data being transferred was financial information. Attackers often target database servers for the high-value information that they hold.

The direct, unencrypted communications from the internet to this server that Darktrace observed were extremely risky. The potential for leaking or changing vital financial information through this server represented a serious risk to the company's operations and reputation.

## Privacy & Compliance

Darktrace's Enterprise Immune System uses technology that collects and inspects data from within the enterprise's network. This collection and analysis is fundamental to the Enterprise Immune System approach to cyber defense, and its ability to detect novel threats in today's complex business environments. This process has been designed with data protection and controls in place.

> **The analysis of raw data flow does not include the content of data files, but the information collected is used to correlate data between the source and the receiver for a given traffic session.**

To do this, metadata is extracted from rich data flow and Darktrace's unique mathematical algorithms are applied to check for anomalous or suspicious behaviors inside the network.

Extracted metadata is stored in a rolling buffer on the appliance(s) within the customer site and is expired as disk space requires. The customer can back up this data elsewhere, if required. The amount of metadata (such as the amount of data in the transaction body of a packet) stored on the appliance is configurable.

Additional controls define who can access data on the appliance and what data they can access. For example, user accounts can be granted restricted access to subsets of the Darktrace functionality. Stringent access profiles and auditing are applied to all activity on the appliance, which can be recorded and reported to a data controller.

> “Darktrace shines a light onto our systems, giving us a visual overview of what's really happening 'under the hood'.”
>
> **Conor Claxton, COO,**
> **Macrosynergy Partners**

## Security

Darktrace maintains high security standards within the organization, demonstrated by our ISO certification and compliance with Cyber Essentials.

Darktrace has successfully been certified with ISO 27001:2013. This internationally-recognized, third-party validation demonstrates how seriously Darktrace takes its internal security and validates the information security management system that it has in place.

Darktrace's compliance with the UK Government-backed and industry-supported Cyber Essentials scheme further validates our approach to security. The Cyber Essentials scheme provides guidance on good cyber security practices to organizations, to ensure they are protected against the most common cyber-threats.

Connections to and from Darktrace are encrypted, using high-grade TLS encryption with perfect forward secrecy. User passwords are salted and one-way hashed for storage. Data in the system is protected from unauthorized deletion or modification by users.

## Anonymization Mode

Darktrace can be configured for enhanced anonymization, using Anonymization Mode. If set, this mode anonymizes various aspects of the data seen by Darktrace.

If an incident is identified in Anonymization Mode, the analyst can seek internal approval to conduct an in-depth investigation. Once approval is given, the analyst temporarily logs in as a user with additional privileges. This provides them with the visibility necessary to conduct a thorough investigation of the incident.

Anonymization Mode grants sufficient visibility for analysts to conduct initial triage and to identify incidents, while still protecting the privacy of employees and other users on a network.

## Investigative Tools

The ability to monitor and investigate the network in an intuitive and digestible way lies at the heart of Darktrace's user interface. Visualization technology gives an unprecedented view into your organization.

> **Darktrace's fully interactive visualization tool not only provides a high-level oversight of threat levels, but also allows you to dive deep into granular details.**

As cyber security has become a boardroom issue, the ability to visualize and demonstrate network activity to non-technical personnel, including board directors, is critical, and the Threat Visualizer is an excellent tool to help broaden engagement and encourage common understanding on this issue.

The Threat Visualizer supports collaborative work with its easy-to-use, drag-and-drop functionality, allowing analysts to add comments to incidents and generate threat reports, which may be shared and published. Report generation also facilitates investigation auditing.

As a fully customizable interface, users may include additional business context to enrich network traffic analyzed by Darktrace. For example, users may tag specific devices or prioritize models that are particularly pertinent to the organization.

One-click analysis allows users to visualize and correlate relevant information, and provides the context for a breach or incident. Concise summaries of overall behavior for devices and external IPs are provided, and can be easily integrated with existing dashboards or tools. This speeds up the analysis process, and allows the security team to take quicker decisions about investigations.

> "As opposed to retrospective approaches, Darktrace provides us with absolute visibility into what is happening in real time."
>
> **Louis Kangurs, IT Network Manager, Virgin Trains**

# GDPR Extract: Data Breach

## Recitals 85, 87, 88 & Articles 33, 34, 83

### Recitals

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

### Article 33: Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least: (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

### Article 34: Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. L 119/52 EN Official Journal of the European Union 4.5.2016

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

## About Darktrace

Darktrace is the world's leading AI company for cyber defense. With over 7,000 deployments worldwide, the Enterprise Immune System is relied on to detect and fight back against cyber-attacks in real time. The self-learning AI protects the cloud, SaaS, corporate networks, IoT and industrial systems against the full range of cyber-threats and vulnerabilities, from insider threats and ransomware, to stealthy and silent attacks. Darktrace has 800 employees and 39 offices worldwide. It is headquartered in San Francisco, and Cambridge, UK.



## Contact Us

North America: +1 415 229 9100

Latin America: +55 11 97242 2011

Europe: +44 (0) 1223 394 100

Asia-Pacific: +65 6804 5010

info@darktrace.com

darktrace.com