VECTRA
SECURITY THAT THINKS.®

COMPLIANCE BRIEF

How Cognito enables compliance with the General Data Protection Regulation

GDPR
General Data Protection Regulation
European Commission

Within the European Union (EU), individuals have a fundamental right to protect their personal data. Ensuring that those rights are protected while enabling the free flow of data between EU member states is the impetus behind the creation of the General Data Protection Regulation (GDPR).

Globalisation and rapid technological developments – from cloud computing to location services to social networking – have led to a significant increase in the scale of personal data that private companies and public authorities collect and share.

These trends are key drivers behind GDPR, which goes into effect May 25, 2018, replacing the EU Data Protection Directive enacted in 1995.

GDPR modernises EU data protection rules and establishes a single, harmonised EU law, replacing the patchwork of national laws currently in effect across the 28 EU member countries.

It is estimated that the GDPR will result in €2.3 billion in economic benefits per year as a result of reducing legal complexity and making it easier for businesses to expand operations throughout the EU, according to the Justice and Consumers Department of the European Commission.

The GDPR will be implemented locally, with each EU member state appointing a managing supervisory authority. Its impact will also be felt beyond EU borders as the legislation applies to any organisation that holds or processes EU citizen data in relation to offering goods and services, or that monitors individuals within the EU, regardless of where that organisation is based.

Cognito augments cybersecurity teams and provides key technical capabilities needed to comply with the GDPR.

GDPR overview

Key features of the GDPR include:

- The personal data of EU residents is protected, no matter where it is sent, processed or stored, even outside the EU. "Personal data" means any information relating to an identified or identifiable natural person.

  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.

- Organisations need to obtain explicit, informed consent from an individual to collect and process their personal data.

- Individuals gain the right to data portability from one provider to another; to have their personal data erased; and to object to their data being used for the purposes of profiling.

- Individuals have the right to know when their data is hacked; in high-risk cases (for example, where identify theft is a concern), companies and organisations must notify individuals of a data breach within 72 hours.

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

- Under the "one-stop-shop" principle, a company with subsidiaries in several EU member states will only have to deal with the supervisory authority in the country where it is headquartered or locates its principle establishment.

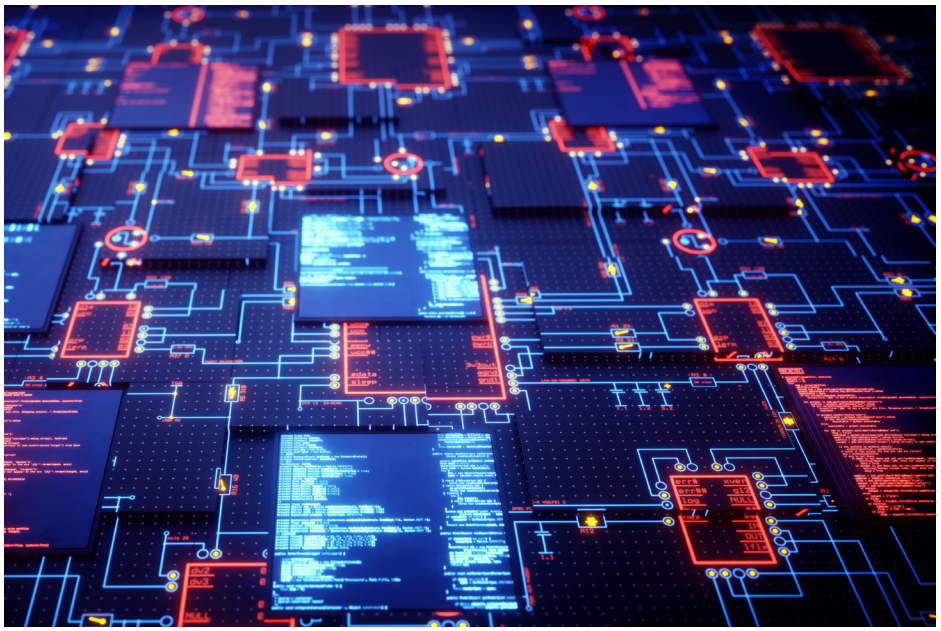
- Any organisation, whether or not it is established in the EU, will have to apply the EU data protection law if they want to offer goods and services in the EU or monitor the behavior of EU residents.

- Data processors and controllers may only transfer data outside the EU if they put in place appropriate safeguards and if individuals have enforceable rights and legal remedies.

  The processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

  A controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- GDPR supervisory authorities have a range of sanctions at their disposal, including written warnings, audits, and punitive fines of up to the greater of €20,000,000 or 4% of annual worldwide revenues.



The following sections highlight the data protection and impact assessment aspects of the GDPR and detail how the Cognito™ automated threat detection and response platform from Vectra® contributes to GDPR compliance and helps protect personal data by providing continuous, automated threat surveillance and detection across an organisation's network.

By automating the hunt for hidden cyber attackers inside networks and enabling faster incident response to stop active threats, Cognito condenses weeks and months of work into minutes so security teams to act quickly to prevent data theft or damage.

Key data protection requirements of the GDPR

The GDPR is a robust set of regulations that covers rights and responsibilities, which include a broad requirement that organisations provide "data protection by design and by default."

That is, organisations are expected to design security into their operations and utilise technologies and services that have built-in data protection safeguards and privacy-friendly default settings, such as on social networks or mobile apps.

The GDPR provides specific suggestions for what kinds of security actions might be considered appropriate to the risk, including:

- Encrypting personal data and/or making it anonymous or using a numeric or another identifier as a pseudonym for an individual's name.
- Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- Restoring availability and access to personal data in a timely manner in the event of a physical or technical incident.
- Regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In addition, the GDPR calls for the designation of a data protection officer (DPO). The individual in this role is responsible for data protection implementation, compliance and reporting within an organisation. The DPO may fulfil other tasks and duties. For example, a chief information security officer can also be a DPO.

Cognito helps organisations address the GDPR

Complying with the GDPR requires putting appropriate technologies and processes in place. Cognito augments cybersecurity teams and provides key technical capabilities needed to comply with the GDPR.

Cognito supports data protection by providing continuous, nonstop network traffic monitoring, real-time threat detection, triage, and incident reporting. Using artificial intelligence and attacker behaviour analytics, Cognito automatically hunts down active cyber threats across the enterprise network, from cloud and data centre workloads to user and IoT devices.

Cognito automates many of the labour-intensive tasks that are typically the responsibility of Tier 1 cybersecurity analysts and incident response teams. By automating these tasks, Cognito dramatically reduces the time spent on threat investigations by up to 90%, enabling security teams to focus on data loss prevention and mitigation.

Key capabilities of the Cognito platform include:

- Continuous monitoring and analysis of all network traffic, including Internet-bound traffic and internal network traffic between physical and virtual hosts with an IP address – such as laptops, servers, printers, BYOD, and IoT devices – regardless of the device type, operating system or application.

- Real-time visibility into network traffic by extracting metadata from packets rather than performing deep packet inspection allows protection without prying into personal or sensitive payload information.

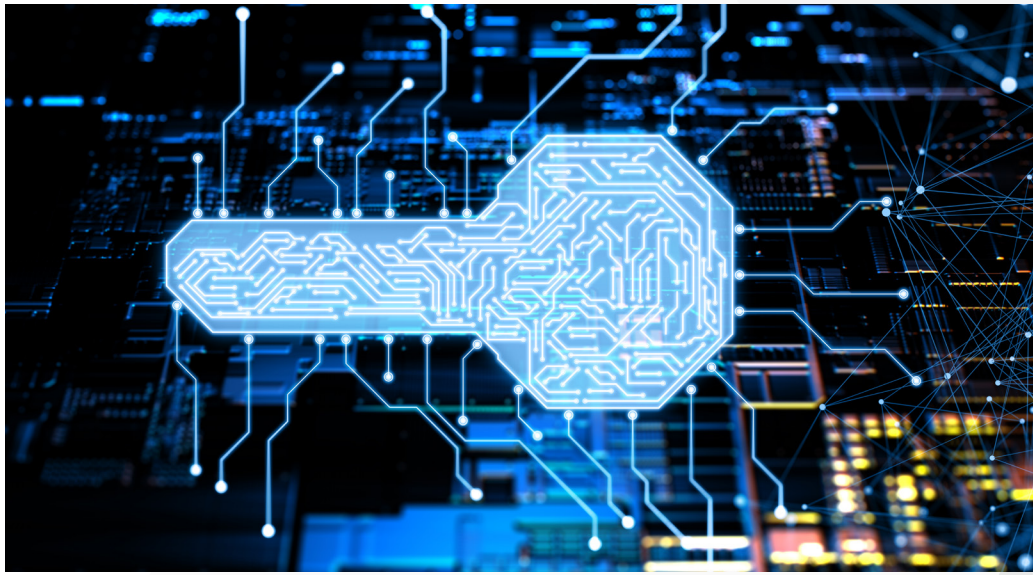
- Analysis of metadata from captured packets with behavioural detection algorithms that spot hidden and unknown attackers, whether traffic is encrypted or not.

- Deterministic identification of attack behaviors, including the use of remote access Trojans, encrypted tunnels, botnet behaviors, ransomware, insider attackers, and targeted advance threats.

  Cognito persistently tracks threats over time and across all phases of an attack, ranging from command and control (C&C), internal reconnaissance, lateral movement and, critically for GDPR, data exfiltration behaviors.

- Automatic correlation of threats with host devices under attack and threat detection details that include host context, packet captures, the seriousness of the threat, and certainty scores.

- Support for adaptive cybersecurity through an iterative process of improvement that leverages the work of the Vectra Threat Labs™, a group of highly-skilled security researchers, as well as behavioral detection algorithms that constantly learn from the local environment and from global trends.



How Cognito supports key GDPR requirements

The following table details the various ways in which Cognito helps organisations address specific elements of the GDPR requirements.

GDPR article	Cognito capability
Article 25: Data protection by design and by default 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this regulation and protect the rights of data subjects. 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.	Cognito assists in enforcing data handling standards by alerting cybersecurity staff when data is transferred between parties in a manner that violates or is not consistent with established practices. This is achieved by baselining standard network behaviors and then monitoring for any anomalous movement of data between hosts, including the volume or frequency of data movement. When anomalous movement is detected, Cognito provides insight into the host transmitting the data, where it is transmitting the data, the amount of data and the technique used to send it. In addition, Cognito supports the requirement for data encryption and pseudonymisation (data protection by design) by focusing on network packet headers and not the data payload, negating the need for any form of data decryption, data routing or intrusive data monitoring/processing techniques.

Cognito assists in enforcing data handling standards by alerting cybersecurity staff when data is transferred between parties in a manner that violates or is not consistent with established practices.

GDPR article	Cognito capability
Article 32: Security of processing 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: A. The pseudonymisation and encryption of personal data; 4.5.2016 L 119/51 Official Journal of the European Union EN; B. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; C. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; D. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	By constantly monitoring the network for indicators of compromise, Cognito helps organisations validate the efficacy of their defensive technical solutions as part of their GDPR measures. Cognito lets security staff see what is getting past their defences by providing alerts about precursor threat behaviours, such as C&C, internal reconnaissance, lateral movement, and data consolidation. Cognito provides multiple early-warning opportunities to detect ransomware, other malware variants, and targeted malicious activity that can precede data theft, manipulation or destruction attacks against any network device, including devices that do not run antivirus software. Likewise, Cognito tracks the internal Kerberos infrastructure and system administration tools to understand normal usage behaviours and detect when trusted user credentials are compromised by a rogue insider or external attackers. These behaviors include the misuse of administrative credentials and abuse of administrative protocols such as IPMI. As a result, security teams can identify and mitigate attacks in a timely manner. In addition, Cognito helps organisations demonstrate that they have appropriate technical measures in place. For example, Cognito automated detection, triage and threat prioritisation triggers real-time notifications to security teams. Notifications offer concise explanations of each attack detection, including underlying events and historical context that led to the detection, possible triggers, root causes, business impacts, and steps to verify.

Cognito lets security staff see what is getting past their defences by providing alerts about precursor threat behaviours.

GDPR article	Cognito capability

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.

Cognito leverages a combination of artificial intelligence techniques to automate the identification and documentation of attacks and ascertain which, if any, require reporting under GDPR. Security teams receive concise explanations of each detection, including possible triggers, root causes, business impacts, and steps to verify.

Cognito helps security teams by:

- Displaying detection information via a simple dashboard that prioritises the compromised hosts that pose the highest risk, changes in a host's threat and certainty scores, and any key assets that show signs of attack.
- Enabling security teams to easily share the same information on demand or on a set schedule using the highly customisable Cognito reporting engine.
- Leveraging the Vectra Threat Certainty Index™ to trigger real-time notifications so security teams know instantly which network hosts with attack indicators pose the biggest risk with the highest degree of certainty.
- Enabling timely reporting and notification of personal data breaches by identifying data exfiltration detections and providing evidence of attempted data breaches.

Cognito also supports these security response and remediation activities:

- Real-time alerts via email, syslog or other tools that have been integrated via a REST API.
- A precorrelated starting point for security investigations within security information and event management (SIEM) systems and forensic tools.
- Driving dynamic response rules or automatically triggering a response from existing security orchestration and enforcement solutions.

Security teams receive concise explanations of each detection, including possible triggers, root causes, business impacts, and steps to verify.

GDPR article	Cognito capability
Article 35: Data protection impact assessment 1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. [...] 7. The assessment shall contain at least: A. A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; B. An assessment of the necessity and proportionality of the processing operations in relation to the purposes; C. An assessment of the risks to the rights and freedoms of data subjects referred to in Paragraph 1; D. The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this regulation taking into account the rights and legitimate interests of data subjects and other persons concerned. 8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment. [...] 11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.	Cognito constantly monitors the communication between applications, tools and systems. When new technologies or platforms are connected to the network, they are instantly monitored by Cognito for signs of an attack. In addition, Cognito provides continual awareness of poor data-handing and system misconfigurations that could create data exposure and breach risk. Cognito contributes to the ability to perform a holistic impact assessment as it provides the evidence of suspect and real threat behaviors inside the network that are associated with data manipulation and loss, as well as precursor attack behaviors.

Cognito constantly monitors the communication between applications, tools and systems.

Protecting personal data with Cognito

The uniform application of the GDPR across EU member states should make it easier for organisations to establish compliant data security regimes and breach notification procedures. Having appropriate tools and technologies in place is key.

Unfortunately, detection and response to cyber attacks is often a slow affair. According to the M-Trends 2016 report, it takes an average of 146 days before a breach is detected. And 53% of those are only discovered after notification from an external party, the report states.

The Cognito platform reduces threat notification and response processes from weeks or days to minutes. Powered by artificial intelligence, Cognito identifies threats proactively and in real time.

By automating labour-intensive tasks that are typically the responsibility of Tier 1 cybersecurity analysts and incident response teams, Cognito dramatically reduces the time spent on threat investigations by up to 90%, enabling security teams to focus on data loss prevention and mitigation.

Efficient and economical, Cognito gives IT security teams realtime visibility into all network traffic, spots hidden and unknown attackers, and puts security event context at their fingertips.

By giving cybersecurity teams the ability to identify and intervene against the early stages of an attack, well before a data breach occurs, Cognito reduces the risk of GDPR reportable data breaches.

Likewise, these same Cognito detections and alerting capabilities contribute to assessment, and form part of an appropriate technical cybersecurity architecture that supports GDPR compliance.

By giving cybersecurity teams the ability to identify and intervene against the early stages of an attack, well before a data breach occurs, Cognito reduces the risk of GDPR reportable data breaches.

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai