appgate

WHITEPAPER

# ADDRESSING ARTICLE 32 OF GDPR

Data sovereignty and privacy regulations differ significantly worldwide. The most noteworthy privacy regulation in the news today is the European Union General Data Protection Regulation (GDPR), a set of regulations adopted by the European Commission to strengthen and unify data protection standards for citizens of the EU.

Scheduled to take effect in May 2018, GDPR's purpose is to strengthen and unify data protection standards for all EU individuals by:

- Empowering EU citizens by giving them control of their personal information.
- Classifying how EU citizens' personal data should be protected and exported outside EU member states.
- Simplifying the regulatory environment for international businesses by unifying the data privacy regulations.

Organizations need to understand the data they have access to, how they use it, and track and monitor the controls they have in place as part of their overall GDPR compliance requirements.

Appgate SDP secures networks with a Software-Defined Perimeter—a network security model that dynamically creates one-to-one network connections between the user and the resources they access. Appgate SDP addresses article 32 of GDPR.

## ARTICLE 32: "SECURITY OF PROCESSING"

GDPR consists of 99 articles, divided into 11 chapters. The subject ranges by chapter and article from general provisions to responsibilities of the controller and processor to cooperation with the supervisory authority, and more.

Article 32 describes technical procedures and methodologies. The other 98 articles talk about internal requirements, establishing the GDPR committee and organization, etc. From a technical aspect, Article 32 is the most relevant. It read:

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 organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
   - the pseudonymisation and encryption of personal data;
   - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
   - a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

## APPGATE SDP ADDRESSES ARTICLE 32

Article 32 does not specify solutions, but instead requirements. In this case, Appgate SDP aids in two ways:

> **"Appropriate level of security account shall be taken… [to] …access to personal data transmitted, stored or otherwise processed."**

Appgate SDP is the ideal tool to address network access security for specific workloads. As the Article suggests, Appgate SDP can provide granular (and "appropriate level") identity-centric security, granting access to workloads only to those users that are specifically authorized to access them.

> **"…Take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them…"**

Appgate SDP prohibits unauthorized users from accessing workloads or databases for which they are not authorized to access. Put simply, in an Appgate SDP secured environment, the user would not be able to see, much less access any workload containing personal data that they were not specifically authorized to access.

Appgate SDP ensures compliance with Article 32 of GDPR. It offers an adaptive and context-aware Software-Defined Perimeter model that only grants access based on identity by dynamically managing access based on the person, environment and infrastructure.

Learn more about Appgate SDP at
www.appgate.com

appgate