GDPR and Scale Computing Frequently Asked Questions

What is GDPR?

The EU General Data Protection Regulation (GDPR) was put into law to establish a new framework for handling and protecting the personal data of EU citizens. In short, the GDPR aims to standardize data privacy laws across Europe while also addressing the export of personal data outside the EU, strengthen data protection and security protocols pertaining to personal data, give individuals greater control over their own data and how organizations use it, and reshape the way organizations approach privacy management.

When is the GDPR effective?

The GDPR becomes effective May 25, 2018, replacing the 1995 EU Data Protection Directive.

Who is affected?

As alluded to above, the GDPR aims to protect the fundamental rights to privacy and protection of personal data for every EU resident and empowers the individual to have greater say over what, how, why, where, and when their personal data is used, processed, or deleted. Any company or organization that works with the personal data of individuals located in the EU in any manner, regardless of location, has obligations to protect the data.

What sort of personal data is covered under the GDPR?

Personal data is any information relating to an identified or identifiable individual. Names, addresses, and social security numbers are some standard fields one would associate with personal data, but other information such as IP addresses, device unique IDs, and location data are also examples of personal data.

You may also hear the terms pseudonymized data and anonymous data. Pseudonymized data is data that cannot be attributed to an individual without the use of additional information. For example, a name or credit card number is replaced with a unique number or token on a company's list of transactions. In this case, we may not know the identity of a specific individual, but we could correlate entries with an individual if the same unique numbers or tokens appear multiple times on the list. Then, if we have access to look-up tables that connect these unique numbers back to a name or credit card number, we could get back to identifying that individual. Pseudonymized data is still personal data.

Anonymous data is data that cannot relate back to an identifiable person or personal data that is de-identified in such a manner that the individual is no longer identifiable. In our example above, instead of a unique number, "xxxxx" or "Anonymous" could be substituted for the name or credit card number for all transactions. We'd have no way of knowing whether one individual or a number of individuals made all of these purchases. However, even this might not be enough. If an individual has a habit of purchasing the same item from the same store every Saturday morning, his/her predictable behavior could allow us to indirectly re-identify him/her. In practice, it is very difficult to reach full anonymity.

Tell me more about the requirement to obtain consent from the individual for the usage of their data?

Consent is key to the GDPR. Quite simply, consent must be freely given, specific, informed, and unambiguous. Ahead of giving their approval, individuals must be informed of why each piece of data is being collected and how that data is being processed. Individuals must also be given the option to withdraw consent at any time. Silence, pre-ticked boxes, inactivity, or language buried in terms of conditions do not adequately confer consent. Note that there may be other legal bases to process personal data, such as a statutory obligation, or a legitimate interest that is balanced against the interests of individuals.

In addition to consent, what other rights do individuals have?

Individuals may request from controllers access to all of their personal data. They have the right to restrict or object to certain processing activities, make changes to the data currently in possession of the controller, or completely erase all data (the right to be forgotten). The information requested must be provided to the individual free of charge and in a portable, machine-readable format.

What role does Scale Computing play in all of this?

Under EU data protection law, an organization can either be a data controller or a data processor. A data controller is the organization that determines the purposes, conditions, and means of the processing of personal data. A data processor is the organization that processes data on behalf, and at the instruction, of the data controller.

Scale Computing as an organization, is a data controller for data flow processes and activities that it conducts for its own purposes, such as HR and marketing. When we process personal data for our customers, we act as a data processor on their behalf.

How will Scale Computing handle data in compliance with GDPR?

The GDPR outlines a number of key principles that organizations must abide by when processing personal data.

First and foremost, Scale Computing will process personal data lawfully, fairly and in a transparent manner in relation to the individual.

Next, purpose limitation states that personal data should be processed for specified, legitimate purposes. Further processing for any other purpose will generally require further consent or permission from the individual. Data minimization stresses that only data required to perform the specific processing activity should be collected. If a piece of data is not required to perform a processing activity, there is no reason for that data to be collected in the first place. Scale Computing will collect and process data with a legal basis, such as consent and only for specific, legitimate purposes.

Personal data must also be accurate and kept up to date through the best reasonable efforts of the controller. Going one step further, if data is no longer needed for its original intended purpose, it should be deleted unless the organization has other grounds for retaining it. Scale Computing will only retain data for the purpose it was collected and will keep it to date and accurate for that purpose.

Scale Computing will follow appropriate security measures when processing personal data to ensure protection from unauthorized access, unlawful processing, and accidental loss or destruction.

Are there penalties for organizations not in compliance?

Organizations that fail to comply with the GDPR may be subject to fines depending on the nature of the infraction. On the high end, organizations may be required to pay up to four percent of their global turnover, or 20 million Euros, whichever is highest.

What about data breaches?

Under the GDPR, data breaches likely to present a risk to individuals must be brought to the attention of the appropriate authorities without undue delay, and within 72 hours if feasible, upon becoming aware of the breach. Notifications must also be made without undue delay directly to affected individuals in the case of high-risk breaches.

What other actions has Scale Computing taken to comply with GDPR?

Here are just a few of the initiatives Scale is taking in order to satisfy GDPR requirements and ensure full compliance:

- Identifying and documenting the flow of all personal data throughout our organization through an extensive data mapping exercise.
- Development and refinement of data privacy and retention policies to ensure their full GDPR compliance.
- Confirming GDPR compliance with third parties who handle our data and revising agreements as needed.
- Updated data consent language and collection mechanisms while also simplifying subject access requests.
- Streamlined notification protocols and clear action plans in the event of a data breach.
- Engaging with internal teams to ensure privacy by design and privacy by default are both at the forefront of all processes and product roadmaps going forward.

How do Scale Computing products and solutions fit into a GDPR compliant solution?

Scale Computing creates secure and reliable IT infrastructure platforms on which organizations can build GDPR compliant IT environments. More information on the data security and protection features of Scale Computing HC3 Infrastructure platforms can be found in the following documents:

- *Information Security with HC3 Whitepaper*
- *Quick Guide to GDPR and Scale Computing Solutions*

Corporate Headquarters
525 S. Meridian Street
Suite 3E
Indianapolis, IN 46225

West Coast Office
360 Ritch Street
Suite 300
San Francisco, CA 94107

EMEA B.V.
Europalaan 28-D
5232BC Den Bosch
The Netherlands

www.scalecomputing.com

1-877-SCALE-59 (877-722-5359)

© 2018 Scale Computing, All rights reserved. Any and all other trademarks used are owned by their respective owners.