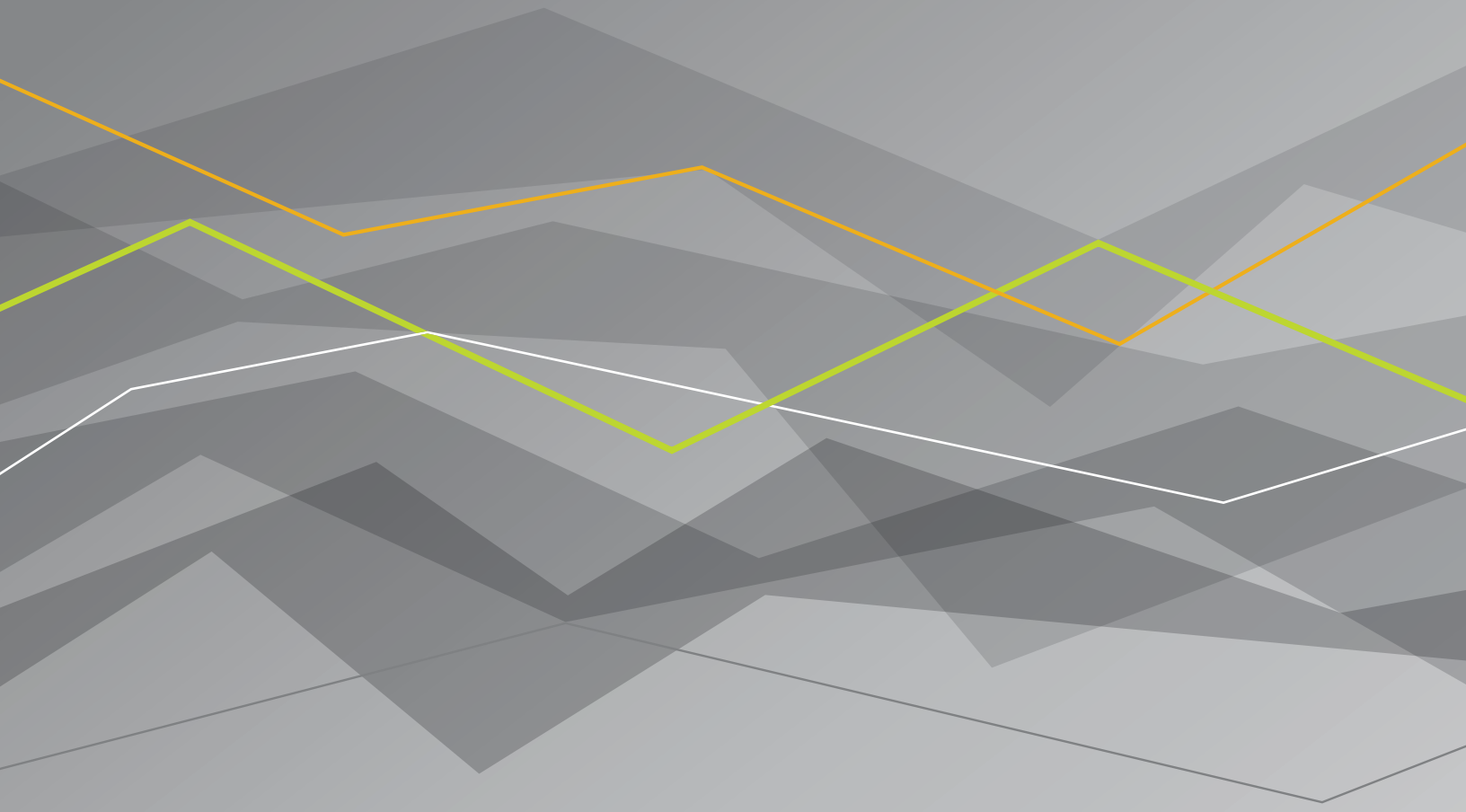
SignalFx



GDPR COMPLIANCE NOTICE

Get Real-Time Performance
with **ENTERPRISE-LEVEL SECURITY**

GDPR Overview

This whitepaper provides an overview of (i) the General Data Protection Regulation (GDPR), (ii) SignalFx's readiness for GDPR, and (iii) how SignalFx can help its customers with GDPR compliance.

On May 25th, 2018 GDPR becomes enforceable. GDPR was created to homogenize data protection approaches across EU member states. GDPR's objective is to give EU citizens control over their information and to protect them from companies using their information irresponsibly. To achieve this objective, GDPR imposes new rules on companies that process personal information of EU residents. GDPR applies globally, no matter where you are located.

Complying with GDPR is non-negotiable. Penalties for non-compliance can be both monetary (up to the greater of 4% of annual revenue or €20 million), as well as the ability to suspend or permanently ban a company's operations within the EU.

SignalFx GDPR Readiness

At SignalFx, we take the security and privacy of our customer data seriously. In support of that commitment, we implemented procedural, technical, and contractual and policy measures to meet GDPR requirements.

Process and Policy

Security and Privacy by Design and by Default — A core component of GDPR is the concept of "Privacy by Design and by Default." SignalFx has supplemented that principle by adding the element of security. SignalFx considers privacy and security at every layer — in every phase of product development, and in all business processes.

Data Protection Policy (DPP) — SignalFx implemented DPP to provide a framework to achieve effective management of GDPR compliance requirements. DPP ensures that personal data is:

- Processed fairly and lawfully
- Processed for specified purposes only
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept longer than necessary
- Processed in accordance with data subjects' rights
- Not transferred outside the countries of the EU without adequate protection

Data Inventory — SignalFx, in preparation for GDPR, created a data inventory document which captures (i) all data processed by SignalFx, (ii) all data sources, (iii) the purposes for processing, (iv) the legal basis for processing, (v) the systems where data elements are collected, processed and stored, and (vi) applicable security controls.

Lawful Basis for Processing — SignalFx reviewed its data processing methodologies and determined that contractual assent (e.g. assent obtained via an MSA or Terms and Conditions) was the most effective means by which to ensure that SignalFx has established a lawful and transparent basis for processing customer data.

Data Subject Access Requests (DSAR) — SignalFx implemented a process to support individuals' right to (i) obtain confirmation from SignalFx that we process their personal data, and (ii) obtain a copy of their personal data (as well as other supplementary information). All DSARs should be sent to gdpr-compliance@signalfx.com.

Breach Notification — SignalFx implemented a breach notification process to ensure that all security events are assessed for the likely risk to Data Subjects and to ensure proper notice to the following: Information Commissioner's Office (ICO), Data Subjects, and anyone else that might have been affected.

Data Protection Impact Assessment (DPIA) — SignalFx created a DPIA to systematically and comprehensively analyze data processing to help identify and minimize data protection risks. SignalFx employees were trained to consider a DPIA at the early stages of any project involving personal data.

Data Processing Agreement (DPA)— SignalFx sends DPAs to all of its sub-processors to ensure that the sub processors comply with all rules set forth in the GDPR. Additionally, SignalFx provides a signed DPA to all its customers and prospects to convey SignalFx's compliance with GDPR.

Privacy Policy — SignalFx updated its privacy policy to in accordance to GDPR guidance.

Employee Training — SignalFx provided comprehensive training to its employees on GDPR requirements and its employees roles and responsibilities in meeting those requirements.

Technical

SignalFx implemented technical controls in support of the processes and policies set forth above to ensure compliance with GDPR requirements.

Recording Legal Basis for Data Collection — SignalFx updated all forms that accept and record user information to ensure that users can read, confirm understanding, and consent to our Term and Conditions and Privacy Policy. This confirmation is retained by SignalFx.

Security Controls — SignalFx validated its existing security controls and processes to ensure that they achieve data protection levels at least as robust as required by GDPR. For details on security controls please refer to SignaFx Security & Compliance whitepaper.

Contractual

Data Processing Agreement (DPA) — SignalFx provides its prospects and customers with a DPA to confirm SignalFx's compliance with GDPR and to enable the users to comply with GDPR.

Model Clauses — SignalFx provides its users with Model Clauses to facilitate data transfers outside of the EU.

GDPR and Data Localization Requirements

In summary

- GDPR allows data transfer outside of EU; however, individual countries and/or companies may implement stricter requirements for certain categories of data (e.g. financial data, geolocation data)
- Transfer ≠ Transit. Transit, routing data through a location outside of the EU, is allowed
- Data localization policies apply to (i) storage and processing and (ii) focus on content provided by customers

Data Localization and GDPR

GDPR restricts transfers of personal data outside the EEA, or the protection of the GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.

GDPR permits data transfer leveraging any of these approaches:

1. **Adequacy Decision**
   - This decision is a finding by the Commission that the legal framework in place in that country, territory or sector provides 'adequate' protection for individuals' rights and freedoms for their personal data.

2. **Privacy Shield**
   - The adequacy finding for the USA is only for personal data transfers covered by the EU-US Privacy Shield framework.
   - The Privacy Shield places requirements on US companies certified by the scheme to protect personal data and provides for redress mechanisms for individuals. US Government departments such as the Department of Commerce oversee certification under the scheme.

3. **Contractual Safeguards**
   - These appropriate safeguards ensure that both you and the receiver of the transfer are legally required to protect individuals' rights and freedoms for their personal data.
   - Model Clauses

In order to meet our customers data localization requirements SignalFx has a EU realm in Dublin. All data sent to SignalFx EU realm will be processed and stored in EU Dublin region. All backups will be stored in EU Dublin region as well.

How Can SignalFx Help Its Users Meet GDPR Compliance Requirements

SignalFx provides its customer with a signed DPA attesting SignalFx compliance with GDPR. Additionally, SignalFx supports its customers GDPR compliance by providing support for DSAR and performing your own Data Protection Impact Assessments.

Conclusion

At SignalFx, we are well equipped to ensure the security and privacy of our customers data. We have put in place procedural, technical, contractual, and policy measures to meet GDPR requirements.

FAQ

What is Personal Data?
For the purposes of GDPR 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); 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. Personal data and unique identifiers: legal definition of personal data now puts beyond any doubt that IP addresses, mobile device IDs and the like are all personal and must be protected accordingly.

Is Encryption Required by the GDPR?
No. GDPR requires reasonable protection of data and does not explicitly require encryption.

Is There an Overview of the Security Measures in Place for All the Services SignalFx Offers?
Yes. Please refer to SignalFx Security & Compliance whitepaper.
https://www.signalfx.com/wp-content/uploads/2018/11/Security_Privacy.Nov_.27.2018.pdf

Is Consent Required for Processing of Personal Data?
Consent is only one of the legal bases one can use for the processing of personal data (Article 6(1)(a)). The legal basis are: (i) consent, (ii) contract, (iii) legal obligation, (iv) vital interests, (v) public task, (vi) legitimated interests.

EU Data Subject have an absolute right to have their personal data deleted upon request. The right to erasure also referred to as the 'right to be forgotten' is not absolute. Data Subjects have the right to have their personal data erased when: (i) the personal data is no longer necessary for the purpose which it was originally collected or processed; (ii) consent was the lawful basis for holding the data and the data subject withdraw the consent; (iii) personal data is processed for marketing purposes and the data subject objects to that processing.

Key Definitions

Consent-freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data

Data Controller — the entity that determines the purposes, conditions and means of the processing of personal data

Data Erasure — also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

Data Portability — the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller

Data Processor — the entity that processes data on behalf of the Data Controller

Data Protection Authority — national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Subject — a natural person whose personal data is processed by a controller or processor

Encrypted Data — personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access

Personal Data — any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Personal Data Breach — a breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data

Privacy by Design — a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition

Privacy Impact Assessment — a tool used to identify and reduce the privacy risks of entities by analyzing the personal data that are processed and the policies in place to protect the data

Processing — any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Right to be Forgotten — also known as Data Erasure, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

Right to Access — also known as Subject Access Right, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

Subject Access Right — also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

Supervisory Authority — a public authority which is established by a member state in accordance with article 46

SignalFx is the only real-time cloud monitoring platform for infrastructure, microservices, and applications. The platform collects metrics and traces across every component in your cloud environment, replacing traditional point tools with a single integrated solution that works across the stack. SignalFx is built on a massively scalable streaming architecture that applies advanced predictive analytics for real-time problem detection. With its NoSample™ distributed tracing capabilities, SignalFx reliably monitors all transactions across microservices, accurately identifying all anomalies. Through data-science-powered directed troubleshooting, SignalFx guides the operator to find the root cause of issues in seconds. SignalFx is used by leading enterprises across high tech, financial services, consumer products, retail, communications, media, entertainment, and web-scale players like Yelp, HubSpot, Acquia, and Kayak. SignalFx is venture-funded by Andreessen Horowitz, Charles River Ventures, and General Catalyst.

signalfx.com **@signalfx**