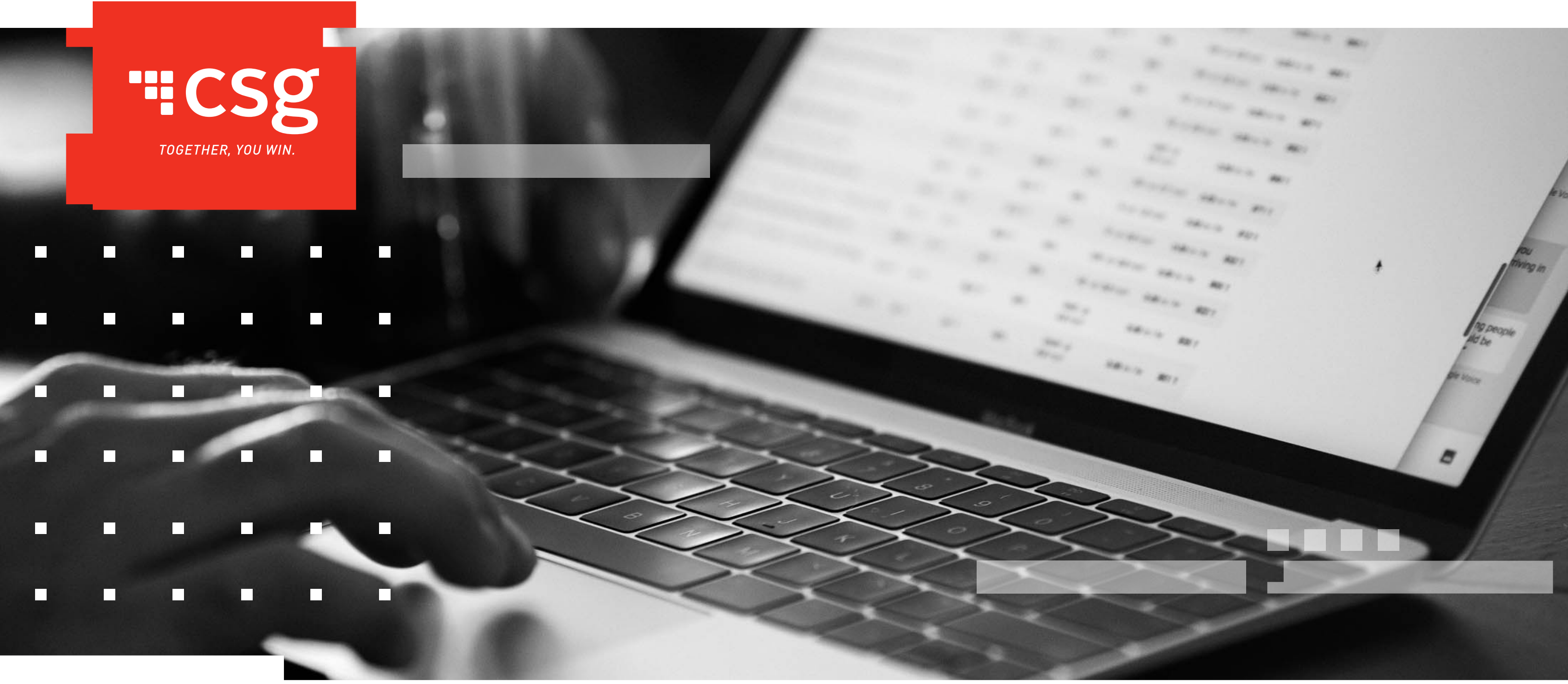
CSG

TOGETHER, YOU WIN.

STREAMLINING ONGOING COMPLIANCE TO GDPR

A BRIEFING PAPER



THE GENERAL DATA PROTECTION REGULATION (GDPR) (REGULATION (EU) 2016/679) IS A REGULATION DESIGNED TO HARMONIZE DATA PRIVACY LAWS ACROSS EUROPE, TO PROTECT AND EMPOWER ALL EU CITIZENS' DATA PRIVACY AND TO RESHAPE THE WAY ORGANIZATIONS ACROSS THE REGION APPROACH DATA PRIVACY. GDPR WILL REPLACE THE CURRENT DATA PROTECTION DIRECTIVE FROM 1995 AND APPLIES FROM MAY 25, 2018.

INTRODUCTION

Across the EU, privacy is a fundamental human right. GDPR governs the **processing of personal data** and grants rights to individuals.

Under GDPR, both the data controller (organizations like services providers that collect data from EU residents) and the data processor (organizations that process data on behalf of data controller e.g. cloud service providers) are responsible for ensuring compliance and will be held directly accountable. Specifically, both will be held accountable for their own level of appropriate security, must document their processing to the same extent and must obtain prior consent to use sub-processors.

Organizations in breach of GDPR can be fined up to 4 percent of annual global turnover or 20 million euros (whichever is greater), for the most serious infringements such as violating privacy by design concepts or not having sufficient customer consent to process data. Lesser infringements, like not notifying the supervising authority and data subject about a data breach or not conducting an impact assessment, can result in fines of up to 10 million euros or 2 percent of worldwide annual turnover.

Communication service providers must consider many additional aspects for end-to-end compliance, like the protection of personal data from breaches with solutions like encryption. Given this larger scope service providers need to evaluate how to not only achieve fast compliance, but also approaches that are cost-effective over the longer term.

THINGS TO KNOW

It is important to the understand the terminology of the regulation. **"Processing"** is a broad term covering all operations performed on personal data including collecting, accessing, recording, storing, organizing, altering, retrieving, using, transmitting, combining, blocking or erasing. And **"personal data"** is not limited to obvious identifiers, such as name but includes "any information relating to an identified or identifiable natural person." The GDPR definition makes it clear that information such as an online identifier, like an IP address, can be personal data. This definition also includes data not considered Personally Identifiable Information (PII) under U.S. law. Personal data that has been pseudonymized—key-coded, for example—can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to an individual.

In the context of data contained within event detail records (EDRs) which capture information about a customer's data, call or content usage (who/what used a service, where, how and when), it is more commonly defined as metadata under existing legislation like the UK Investigatory Powers Act. However, in the context of GDPR, the data held in EDRs is considered personal data.

One of the biggest changes with GDPR is the extended jurisdiction, as it applies to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location. For the purposes of data protection law, a "transfer" is any movement of personal data across an international border. The method is irrelevant. Merely viewing personal data from a non-EEA jurisdiction is a transfer—even if said data isn't modifiable. Transfers outside the EEA (European Economic Area) are prohibited unless certain conditions are met:

→ Adequate contractual obligations governing data processor's obligations to comply

→ Controllers and processors must provide sufficient guarantees to implement appropriate technical and organizational measures protecting the rights and freedoms of data subjects, and must be able to demonstrate compliance

For service providers that use systems integrators for operations with remote or offshore staff, or for multinational groups with operations across many countries, the extended jurisdiction of data transfers can increase the need for demonstrable compliance.

ARE YOU COMPLIANT?

ORGANIZATIONS IN BREACH OF GDPR CAN BE FINED UP TO 4 PERCENT OF ANNUAL GLOBAL TURNOVER, OR €20 MILLION, FOR INFRINGEMENTS.

DEMONSTRABLE COMPLIANCE

GDPR requires a detailed record of data processing activities, which may need to be shared with regulators. Service providers must document the types of data collected, the purposes for which it is being processed, how it was obtained, and the parties that it is being shared with. Consequently, auditing processes need to consider the following activities:

- Privacy impact assessments
- Data flows and maps
- Processing activity registers
- Data breach registers
- Stress testing and regular assessments of security effectiveness
- Risk mitigation steps

At the highest level, the software application must support three capabilities: firstly, logging for operations on personal data (when it is created, read, updated or deleted). Secondly, comprehensive application user security for controlling access to such logs and personal data. And lastly, application user monitoring for tracking access to personal data and to the application.

DO YOUR SOFTWARE APPLICATIONS SUPPORT THESE 3 CAPABILITIES?

DATA BREACH AND PRIVACY BY DESIGN

GDPR requires that data controllers notify the supervisory authority with 72 hours of a data breach, and individual data subjects must be notified if the impact is deemed adverse. However, controllers do not have to notify data subjects if they have implemented “pseudonymization” techniques like data encryption, and implemented adequate internal policies and security measures. Example measures include pseudonymizing personal data as soon as possible, encrypting the data locally, and keeping the decryption keys separately from the encrypted data.

Appropriate security measures now include a legal requirement to implement “privacy by design” and “privacy by default”: service providers must now take a proactive approach to ensure that an appropriate standard of data protection is the default position taken when designing systems and processes, rather than an addition. Further, GDPR requires service providers to only store and process the data strictly necessary for the completion of its business obligations, and to strictly limit the access to personal data to only staff needing it.

The implications of data breach notifications and privacy by design are that the systems need to support pseudonymization capabilities. Not only do software applications need to support encryption of data, but exceptionally high-performance encryption in order to deliver cost-effective scalability when processing tens of billions of records a day.

ENCRYPTION APPROACHES

There are many approaches to encryption of data ranging from encryption at SAN level with firmware accelerators to field-level and application-level encryption of software application data payloads.

SAN-level encryption has advantages of speed and efficiencies, but downsides in terms of protecting against unauthorized viewing of data, since users who can log into the underlying application server can view files on disk, unencrypted, using simple shell utilities. Field- and application-level encryption provide stronger protection against such vulnerabilities, because only users with sufficient privileges can view the data unencrypted and only using application provided interfaces, and usage data cannot be viewed unencrypted outside the application.

Application-level encryption has several advantages over field-level encryption, particularly for offline processing. Firstly, it is more efficient from a processing perspective, since the expensive operation of encryption is only called once for many records and no record or field framing is required. Secondly, when application-level encryption uses a different key for every file it significantly reduces the security vulnerabilities of field encryption. If applications use field-level encryption they typically must either decrypt fields to perform these functions and re-encrypt them resulting in a heavy performance penalty, or they must perform these functions on unencrypted data before the encryption steps.

CONCLUSION

GDPR is a new regulation that comes into force in May 2018 and carries heavy financial penalties for non-compliance, for service providers both inside and outside the EU. Products like CSG Intermediate, CSG Interactivate, CSG Singleview, CSG Interconnect, CSG Route and Ascendon offer proven, industry-standard capabilities that support the key requirements for maintaining GDPR compliance. And with capabilities like application-level encryption and security logging for securing personal data from source to destination, CSG is helping operators around the world to quickly enable GDPR compliance, and deliver a secure solution that is cost-effective over the long term as operators maintain their ongoing compliance obligations.

ABOUT CSG

CSG simplifies the complexity of business transformation in the digital age for the most respected communications, media and entertainment service providers worldwide. With over 35 years of experience, CSG delivers revenue management, customer experience and digital monetization solutions for every stage of the customer lifecycle. The company is the trusted partner driving digital transformation for leading global brands, including Arrow, AT&T, Bharti Airtel, Charter Communications, Comcast, DISH, Eastlink, iFlix, MTN, TalkTalk, Telefonica, Telstra and Verizon.

At CSG, we have one vision: flexible, seamless, limitless communications, information and content services for everyone. For more information, visit our website at csgi.com and follow us on LinkedIn, Twitter and Facebook.