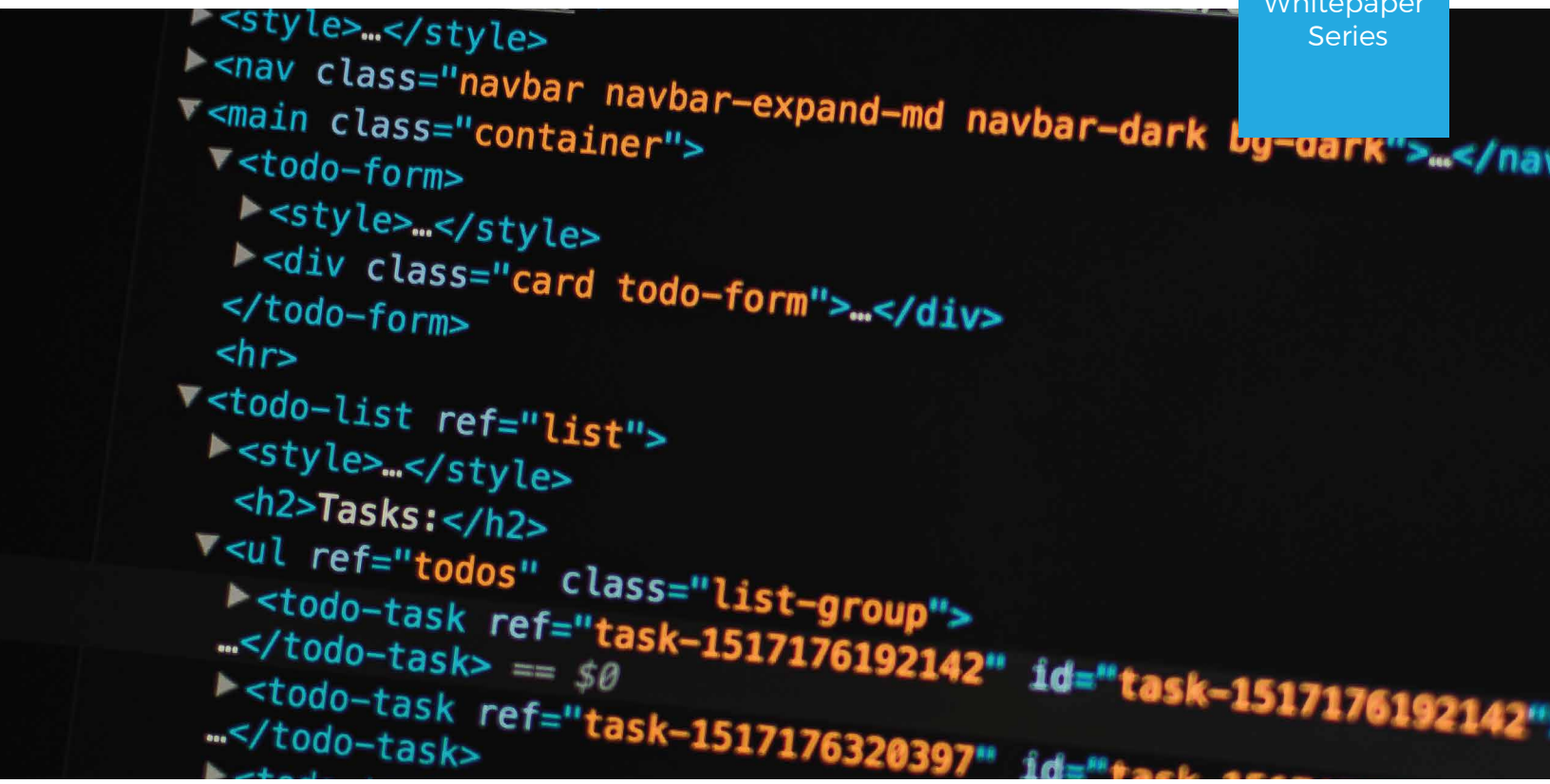
Whitepaper Series



Navigating GDPR:
SECURING THE FUTURE OF DATA PROTECTION
with Gensuite

EU

Gensuite

INTRODUCTION
What is GDPR?

The European Union's **General Data Protection Regulation** (GDPR) is a new set of rules developed to give residents of the EU more control over personal information. GDPR extends the reach of the 1995 EU Data Protection Directive to further protect citizens' rights to personal data protection and implement stricter policies for the organizations collecting and storing data.

The GDPR was ratified in 2016 and will be enforced starting on **May 25, 2018.** Once enforced, this legislation will shift the burden of responsibility from consumers granting access to personal data, to the entities collecting, processing and controlling personal data.

DEFINING KEY TERMS
Understanding the Basics

To best understand the General Data Protection Regulation as it relates to your company and the protection of personal data, it is vital to understand the basic terminology used in the GDPR legislature.

Personal Data

Any information related to a natural person or "data subject" that can be used to directly or indirectly identify an individual [1]

Personal data can include: name, photograph, email address, bank details, social media posts, medical information or computer IP address

Data Subject

Any natural person whose personal data is being collected, held or processed; consent of the data subject is required for personal data use under GDPR [2]

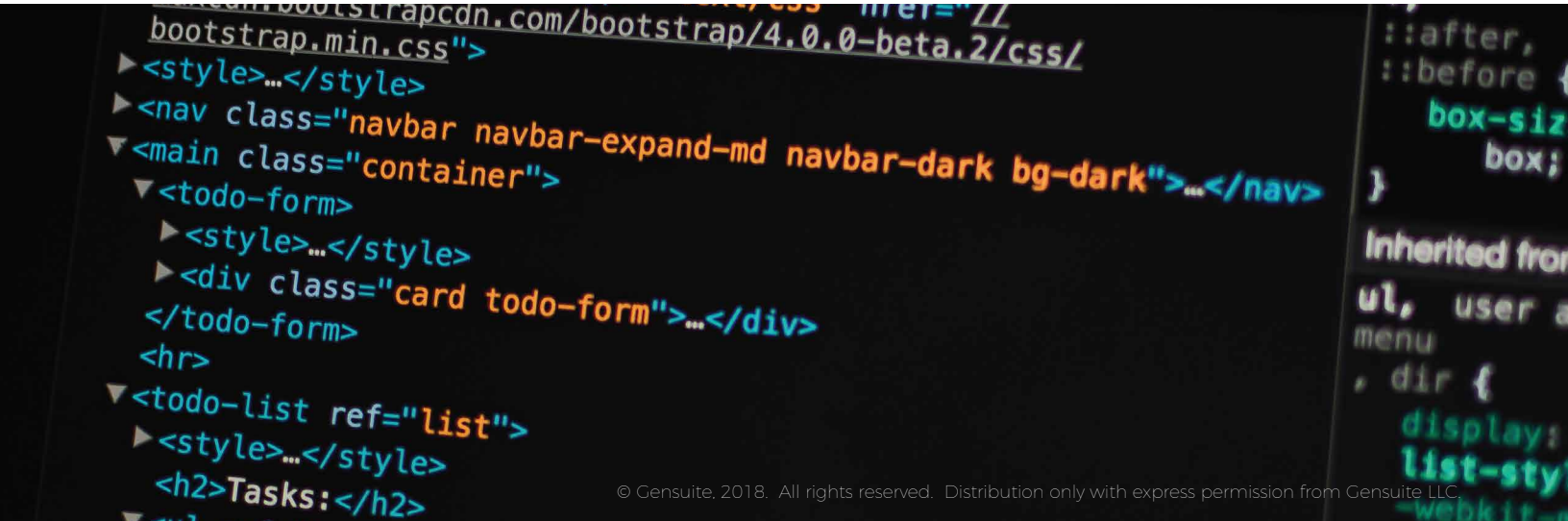
Data Controller

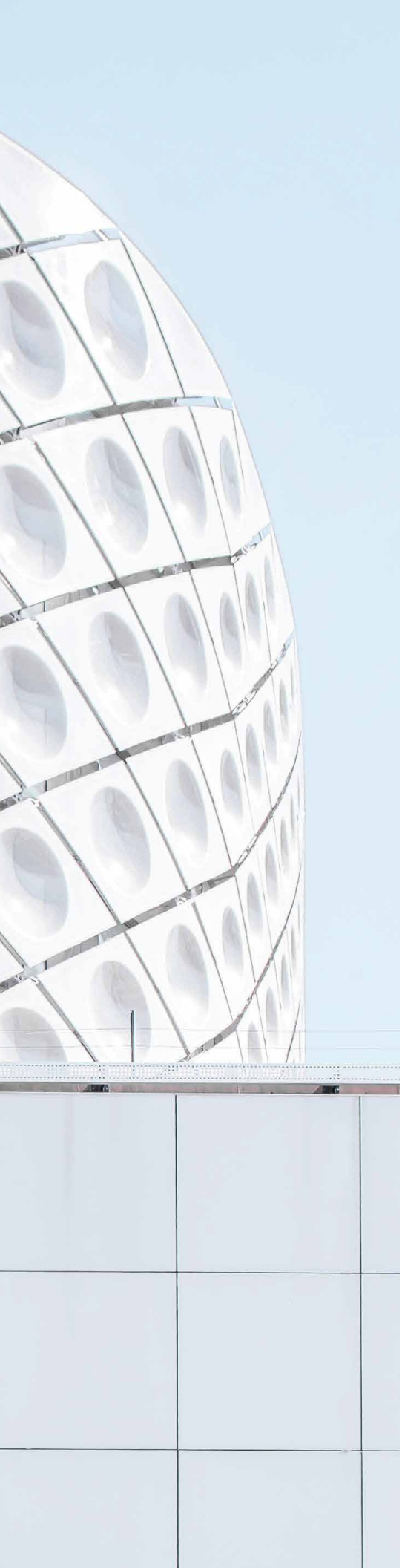
The entity that determines the purposes, conditions and means of the processing of personal data; the principal party responsible for collecting, managing and enabling consent [3]

Data Processor

The entity that processes data on behalf of the data controller; responsible for collecting, recording, organizing, storing, adapting, disclosing, restricting or destroying personal data [4]

[1-4] https://www.eugdpr.org/glossary-of-terms.html





BACKGROUND
Security in the Information Age

By 2025, an average person anywhere in the world will interact with connected devices nearly 4,800 times per day — one interaction every 18 seconds. 90% of the data exchanged will have the potential to negatively impact individual citizens if unsecure, meaning that the majority of data will require additional security measures.[5]

Personal data can take many forms: biometric figures tracked by wearable devices, financial information collected from eCommerce sites, personal images and life experiences amalgamated from social media platforms. Organizations are collecting this personal data as quickly as it is being produced, building virtual consumer profiles, predicting behavior and more efficiently catering to individual needs.

One of today's greatest security risks lies at the intersection of big data and the individual's right to data protection. Because of the rapid rate at which technology has advanced, there are very few regulations written to address data protection adequately. As a result, personal data is not always secured by the organizations controlling it, which increases personal vulnerability to hackers, identity theft and more.

[5] https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf

SECURING THE FUTURE OF PRIVACY
Data Protection as a Fundamental Right

The European Union considers the protection of natural persons in relation to the processing of personal data a fundamental right. (6)

Until the General Data Protection Regulation was ratified in 2016, established regulations were not written to encompass the rapid technological growth of the past two decades. The GDPR is an extension of preexisting legislation, acting to define the legal rights of EU citizens while regulating the responsibility organizations have to secure personal data.

"The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established." (7)

In 1995, when the European Union adopted The Data Protection Directive to protect the fundamental rights and freedoms of natural persons, less than 1% of the world's population were using the internet. When the General Data Protection Regulation was approved and adopted by the EU Parliament in 2016, that percentage had risen to nearly 50%. (8)

GDPR provides increased regulatory accountability for organizations processing and controlling personal data in the Information Age, and ensures that adequate data protection is incorporated into the process of collecting personal data "by default and by design" (9), securing personal data throughout its entire lifecycle by minimizing data collection and deleting data once it is no longer necessary.

[6] https://gdpr-info.eu/recitals/no-1/
[7] https://www.eugdpr.org/the-regulation.html
[8] https://data.worldbank.org/indicator/IT.NET.USER.ZS
[9] https://gdpr-info.eu/art-25-gdpr/

WHO WILL GDPR AFFECT?
Pay Attention to Your Territorial Scope

The GDPR will impact any organization collecting and storing the personal data of data subjects residing in the European Union – meaning that any international organization can be held responsible for data breaches involving EU data. GDPR will broadly affect software companies, cloud-based service providers and companies offering services to individuals globally. Affected organizations can be categorized as data controllers, data processors, or in some scenarios, both.

To better understand the difference between data controllers and data processors, consider a hypothetical situation:

> If a hospital in the EU outsources payroll activities to a company outside of the EU, there will necessarily be an exchange of information, but the payroll management company would not exercise any control or responsibility over that personal data.

In this example, the EU hospital would be classified as the data controller and the company managing payroll, the data processor. Because the personal data in question ultimately belongs to data subjects in the EU, both the hospital and the payroll management company must adhere to GDPR requirements – and could face penalties in the event of a breach.

KEY CHANGES
What Can You Expect?

The General Data Protection Regulation is more broadly enforceable to ensure that residents of the EU are better protected from data breaches and privacy violations. GDPR increases organizational accountability to combat the current evolution of cyber threats in an attempt to better protect personal data, including:

Increased Territorial Scope: Any organization collecting personal data of EU residents is required to comply with GDPR requirements, regardless of geographic location.

Penalties: Organizations in breach of GDPR can be fined up to 4% of annual global turnover, or €20 million (whichever is greater).

Privacy by Design: Under GDPR, companies are required to consider data protection from the onset of the design process - ensuring that security is not an afterthought.

Consent: Organizations are no longer permitted to use long, illegible terms and conditions. They must request consent clearly, intelligibly and accessibly – and it must be as easy to withdraw consent as it is to give it.

INDIVIDUAL RIGHTS PROTECTED BY GDPR
Digital Citizen Rights

Although companies are legally able to collect, store and even sell data, the objective of GDPR is to define the rights of the individual as they relate to data protection. These rights can be summarized as follows:

Breach Notification: In the event of a data breach, organizations will have 72 hours to notify any individuals whose personal information may have been affected.

Right to Access: Data subjects have the right to obtain detailed information from data controllers regarding organizational use of personal information, including: where it is being processed, and for what purpose.

Right to Be Forgotten: Data subjects have the right to demand the erasure, cessation of dissemination, and halt the third-party processing of any personal data.

Data Portability: Data subjects have the right to request personal data that they have previously provided, in an accessible format.

GENSUITE SOLUTIONS
Comprehensive, Global Data Protection

Gensuite is committed to maintaining a comprehensive data protection scheme that is compliant with the laws of all applicable jurisdictions. Gensuite employees can be found on four continents, with European offices in France and the United Kingdom. To address the upcoming EU GDPR requirements and continuously improve security measures, Gensuite teams have taken the following steps:

Privacy Shield

GDPR outlines very specific requirements relating to the transfer of data out of the EU – which the United States does not technically qualify for. To ensure free data transfer between U.S. and EU companies and citizens, Gensuite is committed to maintaining Privacy Shield certification– meaning that every Gensuite global location is certified to facilitate safe and secure information transfer in accordance with GDPR. [10]

Commitment to Personal Data Protection

Gensuite only handles subscriber data per contractual agreements and official subscriber requests. All sensitive data is encrypted to protect identifying information, including name, gender, incident details and other personal information.

Gensuite customers may exercise the GDPR right to be forgotten by submitting requests for individual-specific data to be forgotten or deleted as necessary.

Data Protection Addendums are in place with EU/U.S. customers per the expansion of the scope of liability

Preparedness

Gensuite conducts Privacy Impact Assessments via the NIST Cybersecurity Risk Management Framework to ensure the protection of data and mitigation of security risks organization-wide.

In case of Disaster Recovery, Gensuite has back-up datacenters in place.

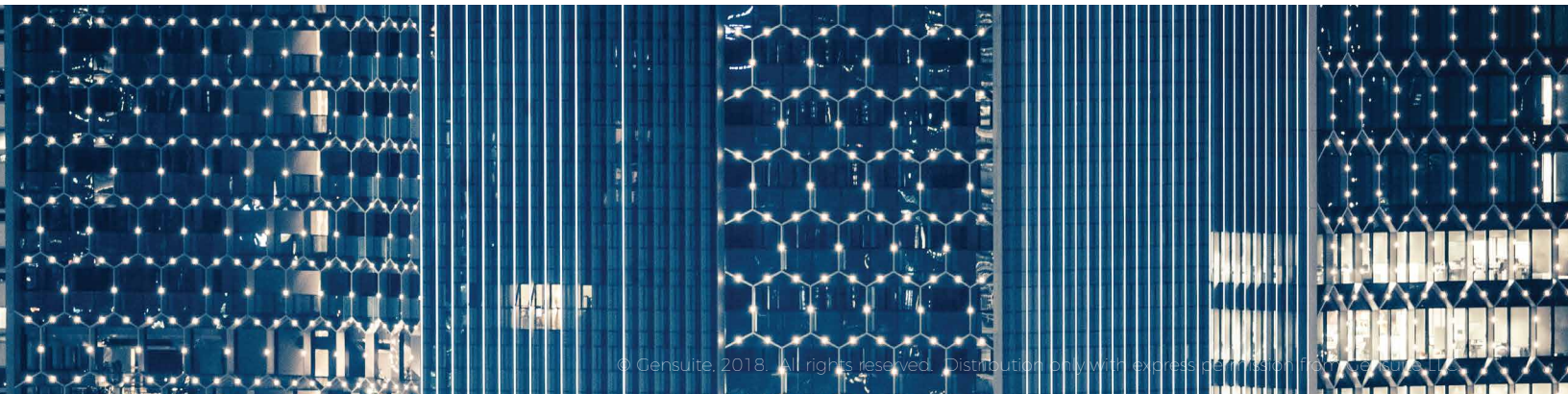
Monthly and bi-monthly penetration and vulnerability testing are in place to address potential security vulnerabilities both internally and externally.

A Security Breach Notification Policy is in place to address the process and communication strategies in the event that a breach were to occur, ensuring accurate communication within the 72 hour window mandated by GDPR.

Investing in the Future of Security

By end of 2018, Gensuite will take the next step in protecting subscriber data by implementing data masking across subscriber instances. By utilizing data masking, Gensuite teams will enhance database accessibility while encrypting sensitive data using random characters. In the event of a data breach, all information would be unreadable.

[10] https://www.privacyshield.gov/Program-Overview



VISUALIZING
The Future of Personal Data

How can companies better protect personal data?

"Pseudonymization" enables companies to make personal data anonymous through **data masking.**

What is Data Masking?

"Data masking replaces all stored information with fictitious data that functions normally and appears real in case of a data breach.

1,946,181,599
total records containing personal or sensitive data breached between January 1, 2017 and March 20, 2018 (11)

191 Days
average time needed to identify a breach (12)

66 Days
the average time needed to fully contain a data breach in 2017 (13)

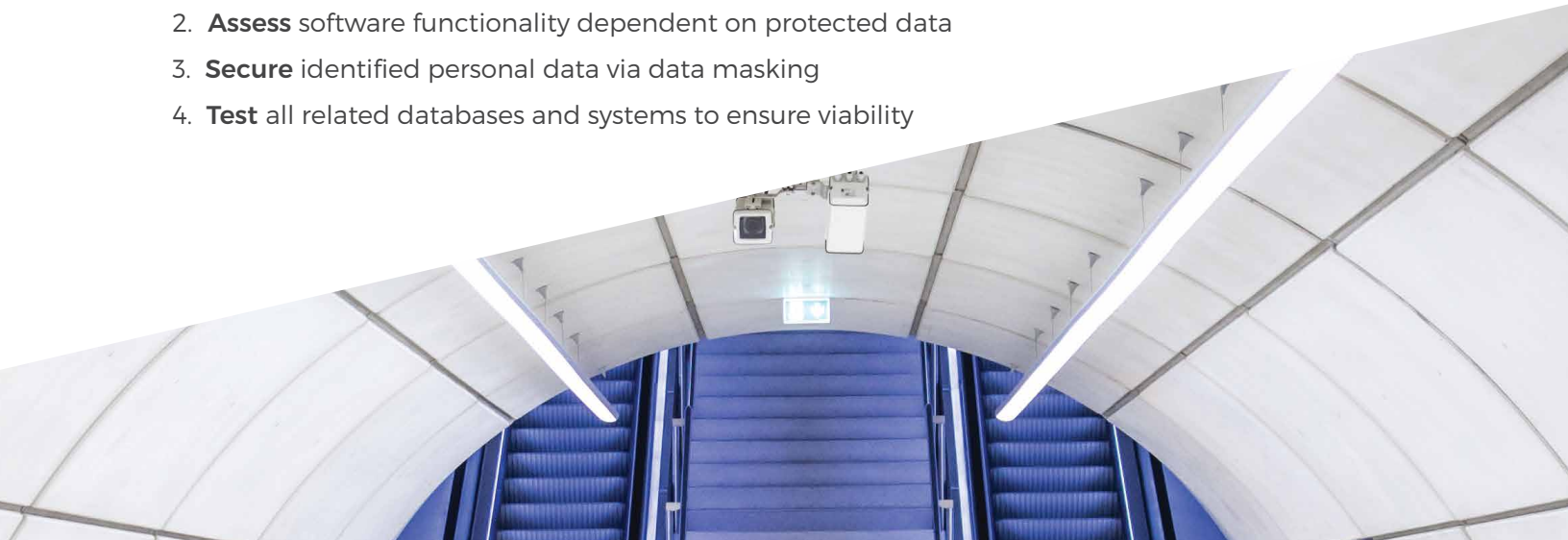
By 2025, almost **90%** of all global data created will require some level of security, but less than **50%** will be secured.

Smarter, more interconnected devices like wearables, virtual assistants and smartphones share data more today than ever before – most of it unprotected.

Masked data is secure and functional – and companies can choose which personal data to mask without affecting software programs or privacy.

4 Steps to Leverage Data Masking

1. **Identify** personal & sensitive data
2. **Assess** software functionality dependent on protected data
3. **Secure** identified personal data via data masking
4. **Test** all related databases and systems to ensure viability



CONCLUSION

The European Union's General Data Protection Regulation will go into effect on May 25, 2018. This legislation expands EU citizens' individual rights to data protection and increases the financial penalties associated with current data breaches. Because any global company using EU data is subject to these regulations, companies must systematically evaluate data use, communicate with current customers and ensure compliance with upcoming regulations.

For more information about Gensuite's GDPR compliance, visit https://www.gensuite.com/privacy-policy/.

Visit our website for a collection of whitepapers and resources:
www.gensuite.com/library

USA | Canada | Mexico | UK | France | India | China | Australia