SAS Solution for Personal Data Protection

Enabling compliance with new regulation

Will you be ready to comply with new EU Data Protection Regulation in time?

Soon you will have to find, evaluate and categorize your company's stored Personal Data (PD) in what may be thousands of databases, and create new processes in order to comply with the new regulation.

Protecting personal information and consumer integrity has become a high priority for the EU. Under the EU's new General Data Protection Regulation (GDPR), every consumer and citizen have the right to know how PD is being used – as well as the right to have his or her data completely erased upon demand. Naturally, this means that organizations that store and/or process EU consumer data must be vigilant and rigorous in protecting such data, regardless of where they are located. The EU values consumer integrity to such a degree that companies that do not comply with GDPR may be fined up to 20 million EUR or 4% of their annual global turnover.

The GDPR is a new regulation that will become effective within the EU countries as of May 2018. Its ambition is to secure privacy and integrity of the data that is collected from EU consumers (Personal Data or PD) in various ways.

To comply with the GDPR, you must have people, processes and tools in place that allow you to instantly know which data you have about your customers, where that data is stored (including the data in all your backup systems), and that you are lawfully keeping and processing the data.

The protection of personal data required by the GDPR is far-reaching, including any information relating to "an identifiable natural person" such as name, identification number, location data, economic, social or cultural identity. Individuals also have the right to know how, where and for what purpose their data is being processed. In addition, consumers also have the right to restrict further processing and to request the erasure of all their data.

Challenge – internally and towards authorities

Responding to these demands can be complicated since data may be stored in duplicate throughout various systems, and erasing data in one system does not necessarily mean that all data is erased in other systems or databases.

Data may also be handled in different ways, depending on how it is used and why it has been collected. There are various de-identification techniques that enable compliance with data protection requirements but at the same time complicate the discovery of personal data within an organization:

- Anonymization – removing PD
- Pseudonymization – replacing PD
- Encryption – encoding PD

New compliance requirements

To ensure compliance with the new GDPR, organizations will need to review the collection and handling of personal data, processes and routines. This includes, for instance:

- Data Protection Impact Assessments based on a questionnaire
- Complete list of systems and related risk rating based on ISO27001 risk rating (Confidentiality, Integrity and Availability)
- Predefined list of controls and options to add additional controls
- Support for policy management and life cycle tracking on all policies in order to ensure monitoring of policies and communication across organizations
- Creation of a standard process for incident management including related actions, responsibility/owner, documentation and reporting
- Easily find Personal Data, even where data is mixed and messy
- Get a clear overview of roles and responsibilities
- Link systems, processes and business owners in data flows

With less than two years to implement, there are a number of challenges on the way to full GDPR compliance. You have to face both internal and external challenges.

How SAS can help

In view of the new requirements, each organization will need to design or update its data protection compliance practices. Several functions in the organization will need to work together and, in some cases, entirely new functions may need to be created. One such function is the Data Protection Officer, who reports directly to the company's board, follows legislation and other news, and who independently monitors the company's GDPR compliance. Other functions that will need to be involved in GDPR are IT, IT Security, Legal, Compliance, CTOs, Marketing, Privacy Compliance Officers and Information Security Officers.

SAS, with its industry-leading analytics including strong solutions for data management and data quality, is well placed to support data protection compliance and to help your company meet evolving data protection compliance demands, particularly in five areas:

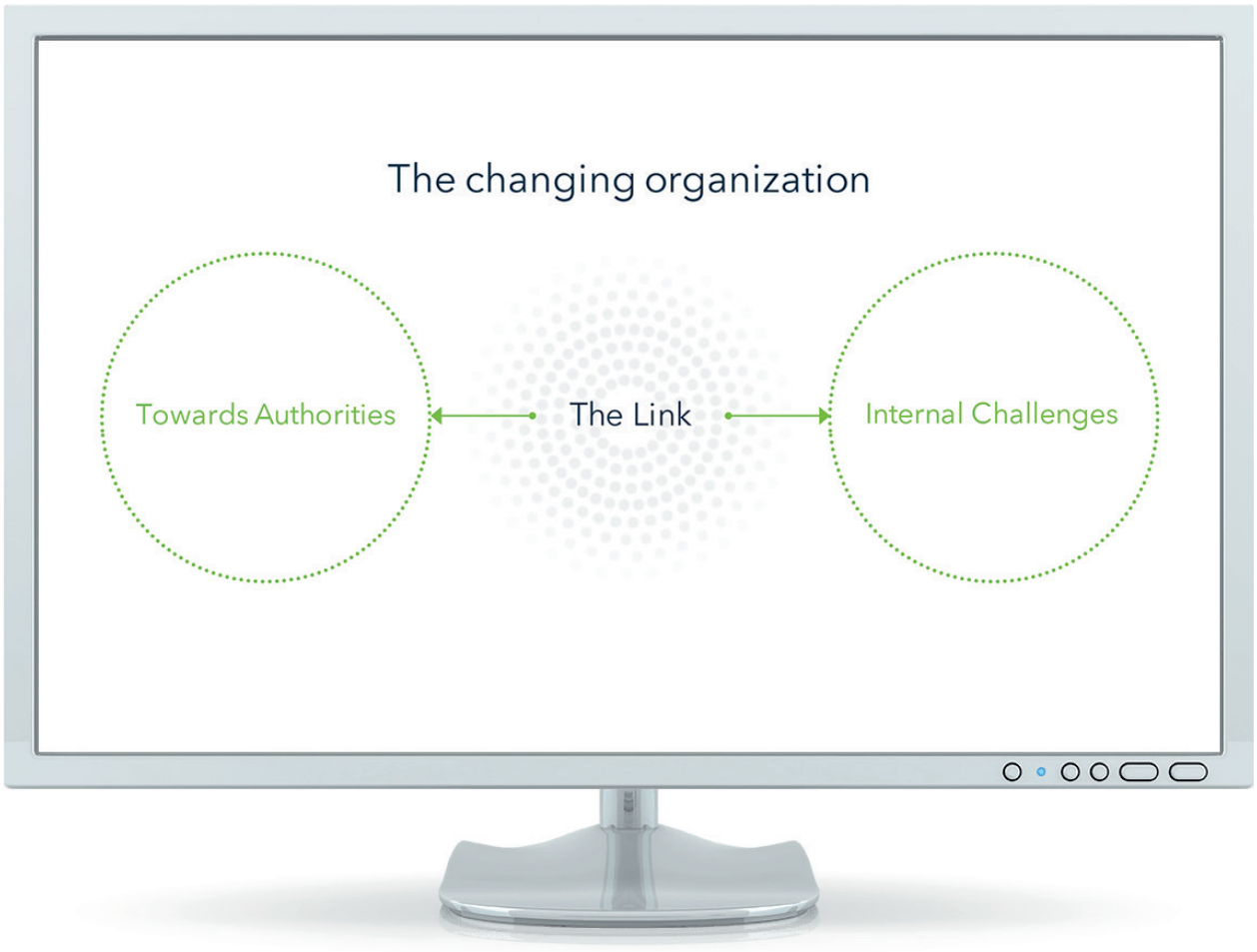
1. Identification (classification, catalogue) – Identification and extraction of PD from both structured and unstructured data sources, no matter where it resides throughout the organization. Incorporate sophisticated algorithms that go beyond traditional sampling methods and manual processes to enable improved Personal Data detection. Reduce false positives by using automated data quality filters and techniques that regularly search files for Personal Data content.

2. Data Flow Analysis – Monitoring and charting storage and processing of PD in order to conduct and document analyses and assessment of the risk involved in all PD collection, use and processing activities, Data Protection Impact Assessment (DPIA). This involves monitoring large amounts of actions, processes and plans, as well as documenting each such step. In addition, companies must in certain cases of high-risk processing for the individual conduct DPIAs and if needed consult with supervisory authorities before processing takes place.

3. Logging – Documenting how all systems are used, and ensuring that no "rogue" users are accessing personal data.

4. User Access Rights – Processes for ensuring exactly who should be allowed to use systems/data, and ensuring that access rights are enforced, even when an employee is transferred to another department, quits a job, etc.

5. Incident Management – Under GDPR, a company must report to authorities within 72 hours if data is lost or a breach in personal data is detected. The company must also show which procedures have been initiated to fix the problem.



SAS solution: a unified view of how your data is handled

For the functions within the organization that oversee how data is handled, normally over a wide range of platforms such as Mobile, Cloud, Social Media, proprietary databases and systems as well as commercial systems, SAS Institute's capabilities enable you to you handle all your data through a unified view. This means that you can seamlessly manage logging, user access and encryption of data to ensure Enterprise Governance and Data Compliance. It also means that individuals can easily find the necessary data – even if that data is "hidden" in "wrong" columns, text strings, mislabeled or identified only by context.

Only SAS delivers proven data management capabilities.

With SAS, you get superior detection capabilities that enable you to search your entire network, regardless of operating system, and locate personal data within varying file formats and both traditional and emerging data sources like Hadoop.

To contact your local SAS office, please visit: sas.com/offices

THE POWER TO KNOW.