SOLIX®
Empowering the Data-driven Enterprise

GDPR essentials and how a common data platform approach can help accelerate compliance

Issue 2

Executive Summary

On 25 May 2018, the European Union (EU) will bring into force the General Data Protection Regulation (GDPR). It replaces the Data Protection Directive (95/46/EC of 1995) and was designed to harmonize data privacy laws across Europe, to protect and empower all EU residents' data privacy and to reshape the way organizations across the region approach data privacy.

At its core, the regulation aims to put EU residents in control of their personal information. It regulates how their information is collected, stored, used, processed, transferred and deleted by an organization. Any organization, local and international, that holds any personally identifiable information (PII) on any EU resident will have to manage that information in accordance with GDPR regulations. Non-compliance can result in fines of up to 4% of the company's global annual turnover or €20 million, whichever is higher. This makes developing a holistic plan to comply with GDPR very critical for all organizations.

Major provisions under GDPR include requirements that companies get specific written consent from the data subjects for any uses beyond the initial reason for collecting the data, the right to be forgotten, data security, data portability and specific notification and other actions in the event of a data breach. EU citizens will have the power to register complaints that will trigger regulatory investigations if they believe their data is being misused.

GDPR applies to existing and historical data too and not just to data gathered after May 25. This includes structured and unstructured data from production and non-production alike. The non-production data copies including archives, backups and data marts often do not have the same security as production databases and have become a major cause of concern. Therefore, the first thing a company needs to do is determine what PII data they have and where it is located, both logically and physically. It then will need to determine what permissions it has for processing of that data at the individual level, and going forward it will need to track and manage the data usage and the associated permissions specifically. Some levels of permission are presumed. For instance, a contractor who provides banking information is presumed to have given permission for the company to use that information to pay him. But other uses may require separate permissions, and the requests for those permissions have to be worded so they are easily understood. No complex legal speak is allowed.

For many organizations, compliance to GDPR will require major changes to their data management and usage practices. Only if organizations plan their compliance strategy and update their personal data processing practices, from consent, collection to deletion, can the GDPR become an opportunity to streamline the value chain and identify innovative ways to provide customers with value added services.

To help organizations achieve GDPR compliance, Solix offers comprehensive GDPR readiness assessment services and a data management platform, namely the Solix Common Data Platform (Solix CDP). While the assessment services review the organizations data practices and provides comprehensive recommendations, the Solix CDP provides organizations with the capabilities needed to implement and sustain GDPR compliance.

Source: Solix Technologies

Ready or Not, GDPR is Coming

The European General Data Protection Regulation (GDPR) is a comprehensive privacy regulation that defines how personally identifiable information (PII) of residents of the European Union needs to be handled. It goes into effect on 25 May 2018, so companies need to start work now, if they have not already, to comply. And it comes with hefty fines for non-compliance, up to the amount of 4% of the organization's global annual revenue or €20 million, whichever is higher. Companies are also worried about the impact non-compliance could have on their brand image, especially if and when a compliance failure is made public. This makes it vital that all companies make GDPR compliance a high priority starting now.

Companies located outside the EU should not presume that the GDPR does not apply to them simply because their headquarters are not in Europe. The regulation applies to every organization that holds any PII on any EU resident (data subject), regardless of where the holder of that data is located. This means that if an organization has any offices, remote employees, contractors, or customers in the EU and therefore keeps personal records of those individuals such as their names, addresses, ages, financial information as in credit histories or bank data, health information, or anything else, must comply with the GDPR or face serious fines.

ENFORCED FROM
May 25, 2018

NON-COMPLIANCE
Fines up to 4% of annual turnover or €20Mn. Whichever is higher.

GLOBAL IMPACT
Impacts every company that does business with EU citizens

Source: Solix Technologies

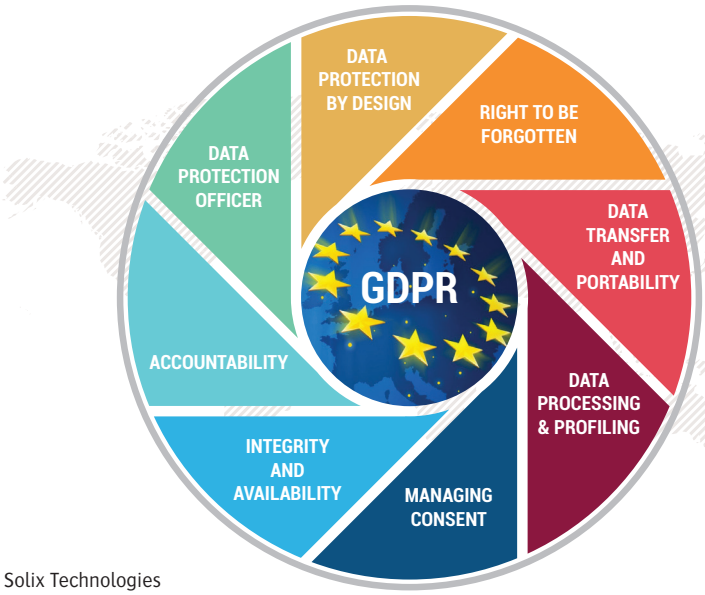
"A recent report on GDPR compliance says that, 86% of organizations worldwide are concerned that a failure to adhere to the GDPR could have a major negative impact on their business."

(Reference: Veritas 2017 GDPR report)

Key obligations under GDPR

Before any action can be taken to move towards full GDPR compliance, it is important that organizations understand the key legal obligations under GDPR and risks that could affect their business, so they can provide the necessary leadership to navigate the company towards compliance.

FIGURE 1 Key obligations under GDPR



Source: Solix Technologies

- **Data protection by design:** Personal data must be protected from misuse and unauthorized access at every stage in its lifecycle.
- **The right to be forgotten:** Individuals have the right to request for deletion of all their PII data. Organizations need to comply with such requests within a reasonable time.
- **Data transfer and portability:** Individuals have the right to move their data to another provider on request. The data should be made available in industry acceptable format in a safe and secure way, without hindrance to usability. Additionally, organizations need to restrict transfer of PII data outside of EU.

"The GDPR is the EU's latest mechanism to mitigate privacy risk where the impact on an individual is highest. The GDPR stresses the importance of a data subject's rights, the manner in which data breaches are dealt with, and general control over personal data."

(Reference: Gartner G00333107 "GDPR Clarity: 19 Frequently Asked Questions Answered" Bart Willemsen)

- **Data processing and profiling:** Processing of personal data is limited to explicit permissions given by the individual. Profiling should be explanatory and should avoid any bias.

- **Consent:** Define specific uses cases when obtaining consent and retain proof of consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it. Explicit consent is only required when processing PII data.

- **Integrity and availability:** Organizations must maintain data accuracy and restore access to personal data quickly following an outage or failure.

- **Accountability:** Log and provide audit trails for all data consents, collection, updates, processing and deletion.

- **Data Protection Officer (DPO):** DPOs must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data (Article 37). If your organization doesn't fall into one of these categories, then you do not need to appoint a DPO.

In addition to the above mentioned key obligations, GDPR also has rules for what happens during and after a data breach. A breach by itself is not prima facia evidence that the company has violated the GDPR. However, the organization will need to demonstrate that it has effective data security in place, in terms of company policies, actions, and technology. And it needs to take fairly specific actions in terms of notifying and helping impacted individuals within 72 hours after a breach is discovered.

GDPR applies not just to new data that may be collected after May 2018, but also to existing data where PII is present. Structured and unstructured data in active production environments and copies of data made for dev/test, data warehouse, backups, archives and ad-hoc analytics are all relevant. Non-production copies like backups and archives alone present a major challenge to many companies that have accumulated years of old, often inactive data. Many companies do not really know what they have in those back files or where all database and file copies, including old copies that are no longer in use, are. Just locating all the data that will come under the GDPR will be a major challenge in many cases.

Additionally, many companies are looking to leverage data for their analytics. More often than not, the data being processed for analytics includes PII. This invariably brings focus on how companies can leverage analytics without violating GDPR's automatic processing and profiling requirements.

GDPR has its share of complexity. For a start, it defines separate roles for the data subject, the data controller, and the data processor. It is important to assess whether the organization operates as a controller or a processor or both and those roles may be different for different business processes. For instance, if the sales department uses Salesforce.com, then the service provider becomes the data processor, But the organization is still the data controller, determining what the data is used for. In this case, for instance, Salesforce would be responsible for data security but the controller would still be responsible for gaining specific authorization from the data subject for any uses of the data beyond the original intended application.

While the GDPR has major implications for data management and security, it does not focus on technology as such. Further complicating this situation is that this is a new regulation Inevitably some issues will be amorphous, and a major challenge for organizations is determining how much they need to do to comply without going too far and incurring unneeded disruption and cost.

Source: Solix Technologies

"One of Gartner's strategic assumption is, by the end of 2018, over 50% of companies affected by the GDPR will not be in full compliance with its requirements."

Reference: G00311301
"Focus on Five High-Priority Changes to Tackle the EU GDPR" Bart Willemsen,

GDPR's Impact on Big Data Initiatives

Organizations embracing digital transformation are collecting, transforming, and analyzing tremendous volumes of structured, unstructured and semi-structured data often referred to as Big Data. Big Data goes beyond data in traditional databases. It includes emails, instant messages, spreadsheets, text documents, PDFs, images, videos, data from social media and more. This data is being used for profiling, spotting market trends, performance analysis and forecasting future outcomes and is becoming central to competitive success.

However, Article **22** of the GDPR prohibits automatic processing, including profiling, where such processing has a legal effect on a data subject or significantly affects the data subject. In this regard, profiling is defined as: "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements; ".

However, GDPR provides that sensitive personal data can be automatically processed based on explicit consent from data subject, irrespective of the effect of such processing, and that data subjects must be informed of the use of automatic processing and given information on the logic used, as well as the potential consequences. Data subjects should also have the option to challenge a decision which was based on automatic profiling and request for human evaluation.

In multi-national corporations, many a times data is moved to a central location for analysis. This practice also warrants a thorough review of data transfer practices as GDPR explicitly refrains organizations from moving personal data out of the jurisdiction of the EU.

It is imperative that businesses review their current use of data for profiling and automatic processing. Use of techniques like pseudonymization will greatly help mitigate risks associated with use of Big Data. Reviewing and updating privacy contracts and consent forms where necessary is also key.

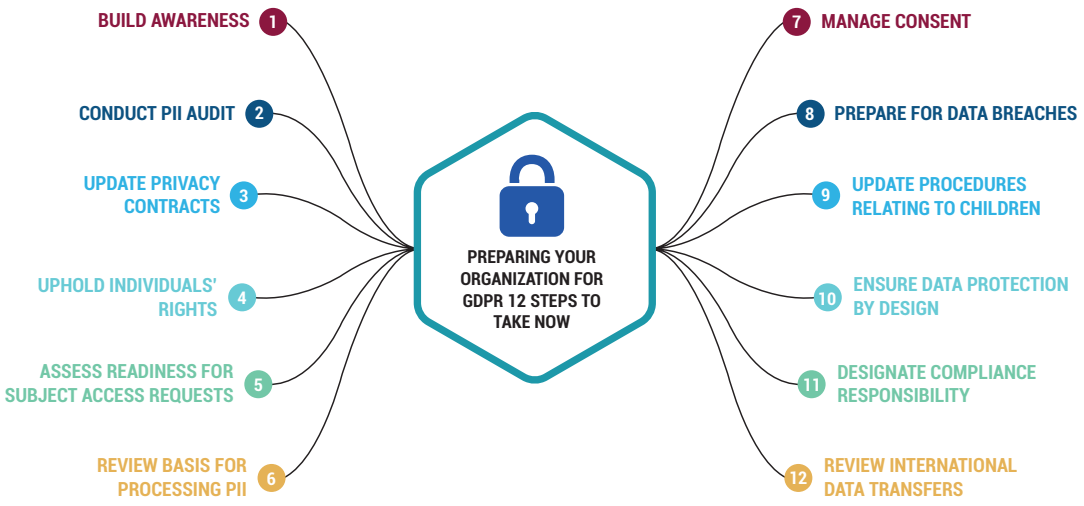
Source: Solix Technologies

Some of the risks particularly pronounced in the context of Big Data include:

- Processing of personal data outside of the purpose for which it was collected;
- Discrimination against certain individuals or groups resulting from profiling; and,
- Use of outdated or incorrect information

Preparing your organization for GDPR

FIGURE 2 12 steps towards GDPR compliance



Source: Solix Technologies

12 steps towards GDPR compliance

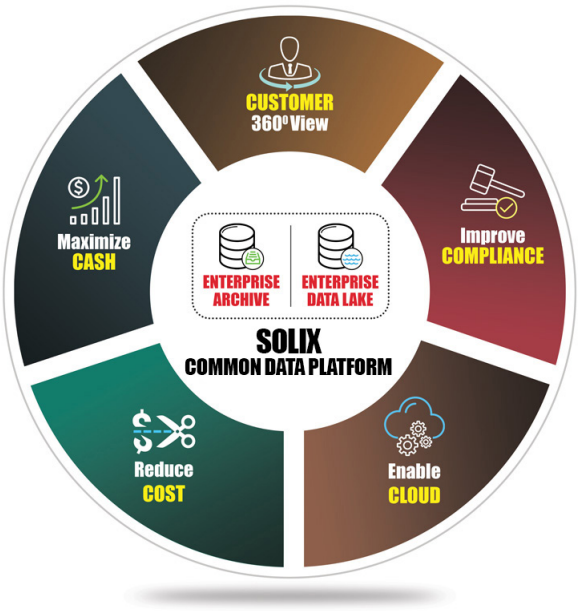
- **Build awareness:** Make sure everyone in your organization including the decision makers are aware of GDPR, its requirements and its impact on your company.
- **Identify PII data:** Identify the existence of PII across your organization, production and non-production alike. Then document it - where it came from, where it is located physically, and who you share it with and what they use it for.
- **Review and update privacy contracts and communication:** Review your current privacy notices and contracts, and put a plan in place for making any necessary changes in time for GDPR implementation.
- **Uphold individuals' rights:** Ensure your current data practices do not violate rights provided to individual under GDPR, including how you delete personal data or provide data electronically and in a commonly used format for easy data portability.
- **Review process for subject access requests:** Update your procedures and plan how you will handle requests within the new timescales and provide any additional information.
- **Identity lawful basis for processing personal data:** Identify the lawful basis for your processing activity in the GDPR, document it, update your privacy notice to explain it and seek consent where necessary.
- **Manage consent:** Review how you seek, record and manage consent. Make sure it explicitly covers all your data collection, retention and processing requirements. Refresh existing consents where necessary.

- **Update procedures relating to data breaches:** Have the right mechanism in place to detect and investigate a personal data breach. Have the required procedures in place to report data breaches within 72 hours.
- **Update procedures concerning children:** If your organization deals with children, then put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.
- **Plan for data protection by design:** You should familiarize yourself with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organization.
- **Assess the need for Data Protection Officer:** Assign the responsibility for data protection compliance to someone in your organization and assess where this role will sit within your organization's structure and governance arrangements. Designate a Data Protection Officer formally if necessary.
- **Review International Data Transfers:** If your organization operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority.

Source: Solix Technologies

Solix can Help

Thanks to digital transformation initiatives, even traditional organizations have begun to experience an explosion of data in various forms and frequency. This has exposed many organizations to data breaches and compliance nightmares. However, organizations need to take advantage of the treasure trove of insights available in this data to not only defend themselves in this highly transformative and competitive environment but actually thrive in it. Data-driven companies are the ones that will survive the ongoing digital disruption. Specifically, those that use data to optimize their five Cs: cash, cost, compliance, cloud and customer.



Solix is a leader in empowering data-driven enterprises. For over a decade, Solix has been helping global businesses from across industry verticals better organize their enterprise information for optimized infrastructure, data security, advanced analytics and compliance. Solix understands the complexity involved in complying with GDPR and has the required expertise and

software to help organizations design and implement a sustainable GDPR compliance strategy. Solix does this through two mutually independent offerings

1. Solix GDPR Readiness Assessment

2. Solix Common Data Platform

FIGURE 3 Accelerate GDPR Compliance

Source: Solix Technologies

Solix GDPR Readiness Assessment

The Solix GDPR Readiness Assessment provides an in-depth assessment of your organization's data practices including data collection, access, usage, processing, retention, protection and deletion. It provides risk and remediation-focused insights, and actionable guidance for your data policies, procedures and practices. This deep dive into your organizations data environment will provide an action plan to not only address GDPR, but strengthen your overall Information Governance approach.

Key Assessment Outputs:

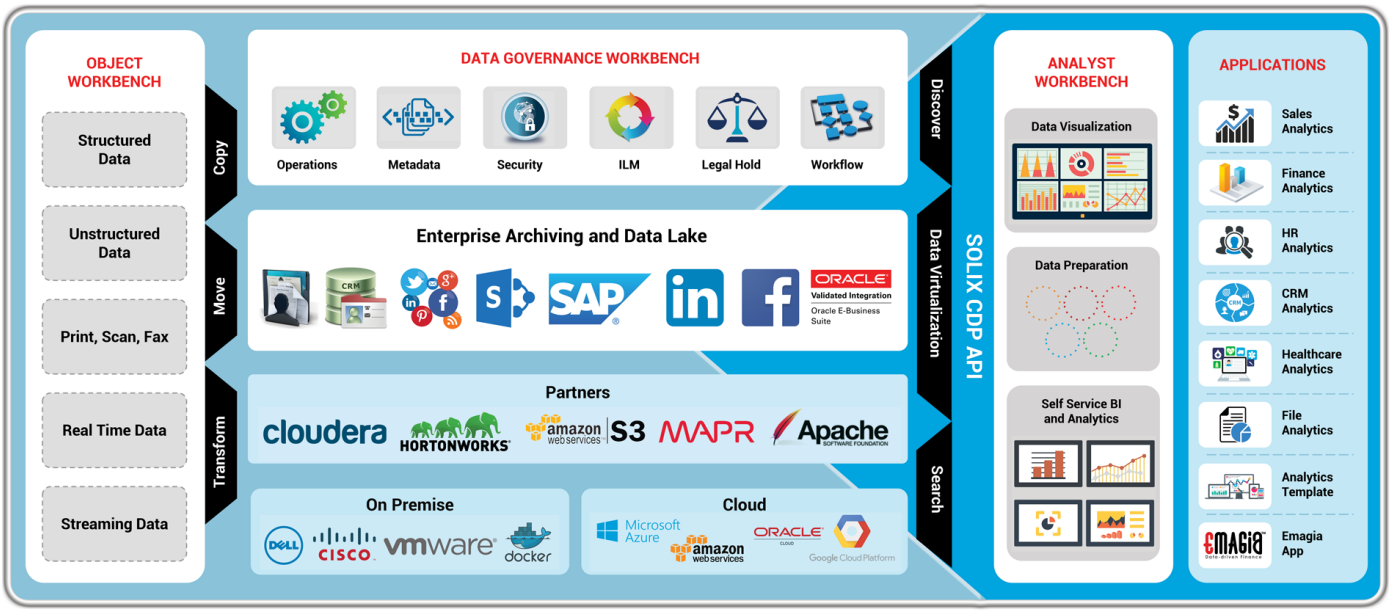
- Information Governance Maturity Rating
- GDPR-Specific Evaluation and Recommendations
- Inputs into the GDPR Business Case / ROI Model
- Approach to enabling GDPR compliance

Solix Common Data Platform

The Solix Common Data Platform (CDP) is a highly scalable and robust next-generation Big Data management platform that features uniform data collection, metadata management, data governance, ILM, data security, data discovery, and a full set of interfaces to support plug-and-play stack creation and modernization. It leverages

the high-performance and low-cost characteristics of the open source Apache Hadoop framework to allow economical storage and real-time processing of petabytes of structured and unstructured data.

FIGURE 4 Solix Common Data Platform



Source: Solix Technologies

With a built-in enterprise data lake, enterprise archiving, application retirement, and eDiscovery solutions, Solix CDP provides organizations with an unparalleled enterprise data management and governance framework. Now with its enhanced capabilities for GDPR compliance, Solix CDP accelerates GDPR compliance and helps sustain it even in the most complex and demanding data environments.

Features in Solix CDP that help accelerate and sustain GDPR compliance

Discover and Report PII: Solix CDP's enhanced metadata management and discovery features provide Data protection officers (DPO) with a single pane of glass view into data across production and non-production environments. This greatly enhances the ability to identify the presence of PII for the DPOs and enables them to quickly put in measures and processes to comply with GDPR.

Data as a Service: Solix CDP through its central data lake repository provides authorized data consumers with a singular point of access to structured and unstructured data from a wide range of enterprise data sources. This centralized provisioning and singular point of data access for data analytics, data warehouse and other downstream applications provides great control over which applications can have or continue to have access to PII data. This can help prevent unapproved processing of PII data as data can be provisioned only after thorough review of usecases and consent. Additionally, the centralized repository, data quality and provisioning tools make data portability an easy task.

Govern PII Usage and Access: With granular role based access control, Solix CDP enables only authorized users to access data from its centralized repository. It can be used to restrict access to PII data only to authorized users.

Archives and Backups: With built in enterprise archiving and application retirement solutions, Solix CDP is an ideal platform to house all the enterprise archives and backups. This brings otherwise difficult to access offline data under a governance framework, making it easy to discover PII and implement the necessary mechanisms to support GDPR compliance.

Protect PII data: Solix CDP provides multiple data protection options including role based access, data encryption in transit, data encryption at rest and data masking. Access controls and data encryption capabilities help prevent unauthorized access to sensitive data present in the Solix CDP. Data masking can help provision data for downstream analytics or test data environments with structurally similar but unauthentic version of PII.

Retention and Deletion: Solix CDP captures metadata and lineage of all the data present in its central repository. This when coupled with search and discovery features of CDP makes it easy to identify and delete PII data of an individual user. The ILM capabilities also enable automated deletion of data past consent expiration thereby minimizing unnecessary storage of sensitive data. The lineage information also helps CDP purge data from the source systems as necessary.

Full Audit Trail: Solix CDP logs every action performed within its platform including data ingestion, access, deletion, updates and export to provide a comprehensive audit report for DPO. This helps DPO manage the compliance program effectively and show proof of compliance.

Process Configurator and Notifications: The process configurator helps automate PII discovery, PII retention, PII deletion and PII encryption while notifications provide timely updates to DPO on all actions performed on PII data.

Source: Solix Technologies

Conclusion

It is time now for organizations to implement a comprehensive strategy to comply with GDPR. Failure to do so will lead to significant monetary damages and potential loss of customer trust. With data breaches at an all-time high, GDPR is no more a compliance challenge alone. It is a business issue that requires board-level engagement and a well crafted strategy. It is bound to transform the ways in which organizations collect, process, store, share, and destroy personal data. Successful adherence to GDPR can help gain and retain more customers as it demonstrates an organizations investment and commitment to protecting customer data and privacy. Penalties associated with failure to comply and the gains associated with successful compliance provide enough reasons for a company to invest in the right people, processes and technologies. Solix with its comprehensive GDPR Readiness Assessment Program and the Solix Common Data Platform provides the right mix of expertise and technology to help companies accelerate and sustain GDPR compliance.

Source: Solix Technologies

About Solix Technologies

Solix Technologies, Inc. is a leading big data application provider that empowers data-driven enterprises with optimized infrastructure, data security and advanced analytics by achieving Information Lifecycle Management (ILM) goals. Solix Big Data Suite offers an ILM framework for Enterprise Archiving and Enterprise Data Lake applications with Apache Hadoop as an enterprise data repository. The Solix Enterprise Data Management Suite (Solix EDMS) enables organizations to implement Database Archiving, Test Data Management (Data Subsetting), Data Masking and Application Retirement across all enterprise data. Solix Technologies, Inc. is headquartered in Santa Clara, California and operates worldwide through an established network of value added resellers (VARs) and systems integrators. To learn more, please visit http://www.solix.com.

SOLIX®
Empowering the Data-driven Enterprise