

GDPR CHALLENGES

BY SULTAN SHIFFA

Governing General Data Protection Regulation Challenges with Enterprise Data Architecture

OVERVIEW

Today, we live in a digitalized economy where globalization is driving businesses across borders and data management needs more attention than ever.

The European Union's General Data Protection Regulation (GDPR) becomes effective on 25 May 2018. In contrast to older directives and data protection acts, the GDPR will bring new accountability obligations, increased data protection rights for EU citizens and restrictions on data flows across borders. Organizations that process EU citizens' personal data must comply with the regulations, and this applies to all data owners, who say why and how data is processed, and to data processors, who perform actions on the data.

It introduces also obligations to data breach notification, with stricter accountabilities that personal data information is sufficiently managed and protected.

In this solution brief, we discuss the most important facts that data management teams need to consider to comply with the new requirements and how to tackle these challenges with an enterprise data architecture solution, IDERA ER/Studio Enterprise Team Edition (ETE). Diagram 1 shows the requirements and how ER/Studio ETE addresses these challenges.

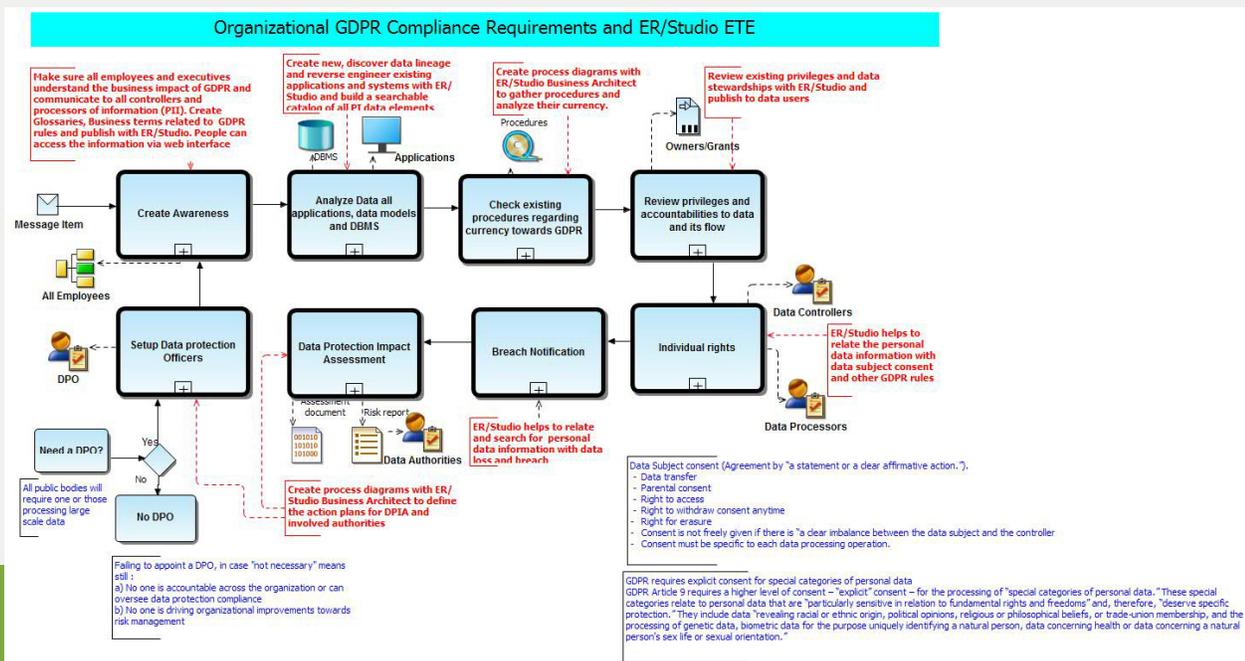


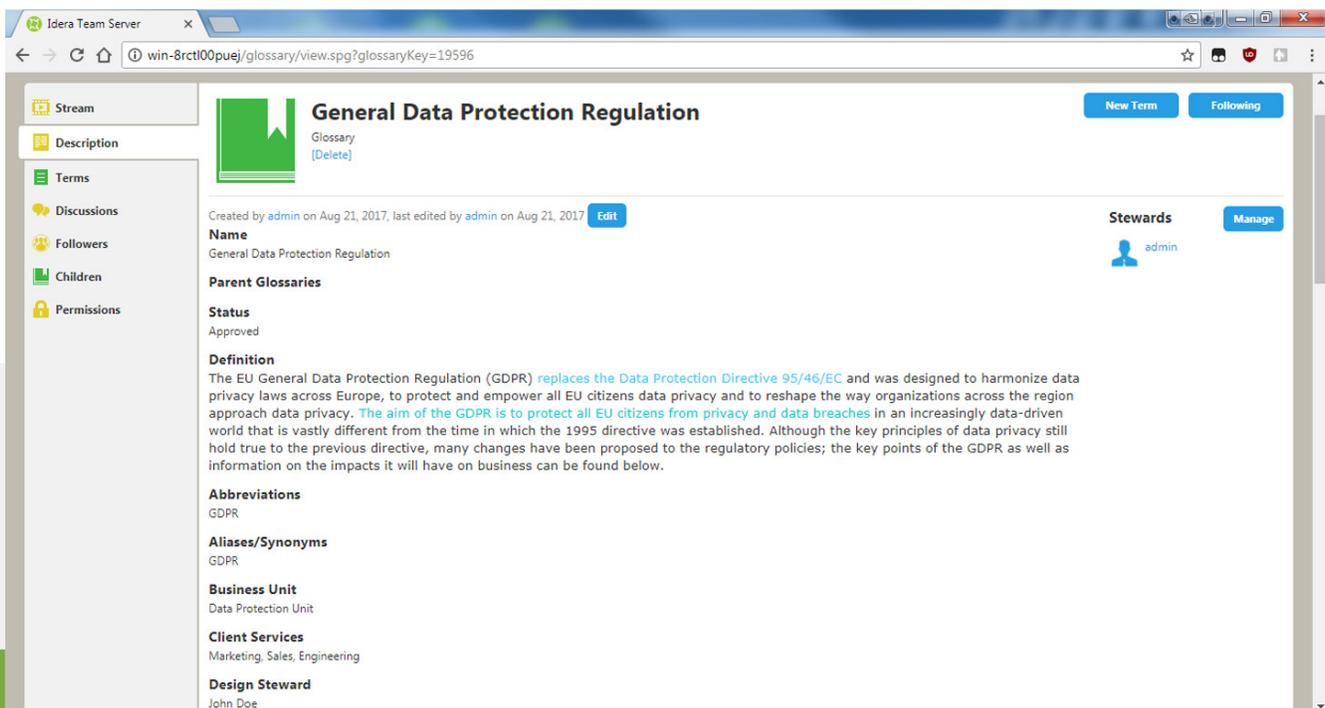
Diagram 1 Organizational requirements for GDPR compliance and ER/Studio Enterprise Team Edition

CREATE AWARENESS FOR GDPR COMPLIANCE ACROSS THE ORGANIZATION

One of the first key tasks of the data management team and the Data Protection Officer (DPO) should be to create awareness regarding the impact of GDPR on the business among executives, data controllers, data processors and data leaders across the organization. In order to generate awareness organizations need to have clearly defined documentation defining the policies, rules, requirements and the impact of the non-compliance to the whole organization. This can be achieved with web-based centrally accessible documentation of the applications, processes, business rules, data sources, business terms, stewardship, roles, and obligations used across the organization.

With ER/Studio Enterprise Team Edition, organizations can establish a foundation for data governance using the Team Server metadata repository and collaboration platform to share a glossary for GDPR regulations, business terms and rules. Diagram 2 depicts how GDPR is documented and planned to be used, and the policy each user has to follow. Users are able to track changes and get notified when changes occur to GDPR regulations and organization-specific policies. It shows also the level of compliance necessary for data elements.

This helps to set up the compliance by default criteria of the GDPR in establishing reusable standards, transparency, and accountabilities to improve products, data movement chains, and processes, and minimize risks.



The screenshot displays the Idera Team Server web interface for a glossary entry titled "General Data Protection Regulation". The interface includes a left-hand navigation menu with options like Stream, Description, Terms, Discussions, Followers, Children, and Permissions. The main content area shows the following details for the glossary entry:

- Name:** General Data Protection Regulation
- Parent Glossaries:** (None listed)
- Status:** Approved
- Definition:** The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was 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. 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. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR as well as information on the impacts it will have on business can be found below.
- Abbreviations:** GDPR
- Aliases/Synonyms:** GDPR
- Business Unit:** Data Protection Unit
- Client Services:** Marketing, Sales, Engineering
- Design Steward:** John Doe

Additional interface elements include buttons for "New Term", "Following", "Edit", "Stewards", and "Manage". The "Stewards" section shows a user named "admin".

Diagram 2 General Data Protection Regulation Documentation in Team Server

CHECK EXISTING PROCEDURES REGARDING CURRENCY TOWARDS GDPR

Most of the larger organizations do have procedures and processes to demonstrate compliance due to prior data protection laws or they have a manual documentation of the rules and policies. It is the right time to look into those existing procedures and contracts with partners and suppliers and to analyze their currency and applicability towards the new GDPR regulations.

ER/Studio Business Architect can be used to define and graphically represent the necessary processes and actions to take. These processes show which data is accessed, which documents need a review, and which parties are involved in each process.

Diagram 4 below shows an example for establishing the necessary processes, tasks and people involved to attain that goal. This information can be maintained, kept alive and shared across the organization. As processes are reviewed, they can be optimized to eliminate any redundancies.

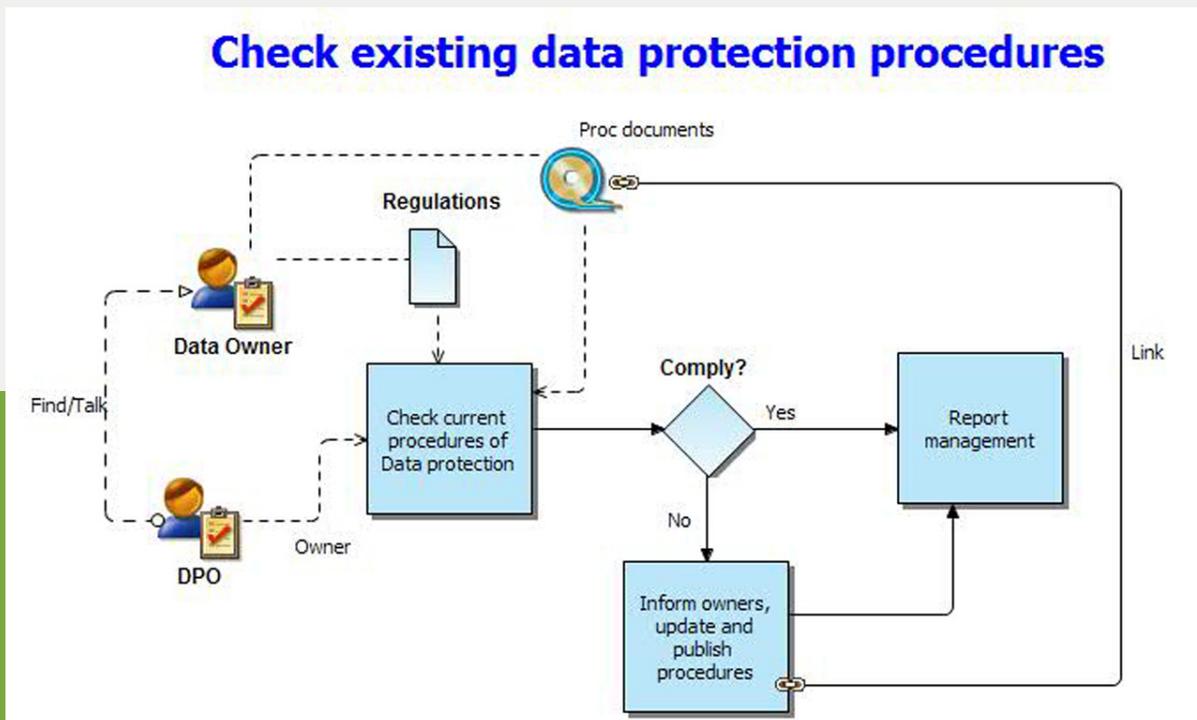


Diagram 4 ER/Studio Business Architect process diagrams show procedures and action plans

REVIEW PRIVILEGES AND ACCOUNTABILITIES TO DATA AND ITS FLOW

One of the key issues in terms of data management and maintenance is ownership. We keep always asking: Who is the owner the data? Who is able to create, read, update, and delete that data? Or can I send this data to a third party person? For GDPR compliance, we need first to understand who is responsible for the data objects, who has access to it and how this data is used across different departments.

ER/Studio Enterprise Team Edition consists of different components to define, maintain and understand the ownership and the flow of digitized data. It helps data owners also to identify and protect the data relating to identifiable individuals. Diagram 5 below shows how data stewardship can be assigned and managed in ER/Studio Enterprise Team Edition. Diagram 6 displays a data lineage diagram that supports data flows and data ownership documentation.

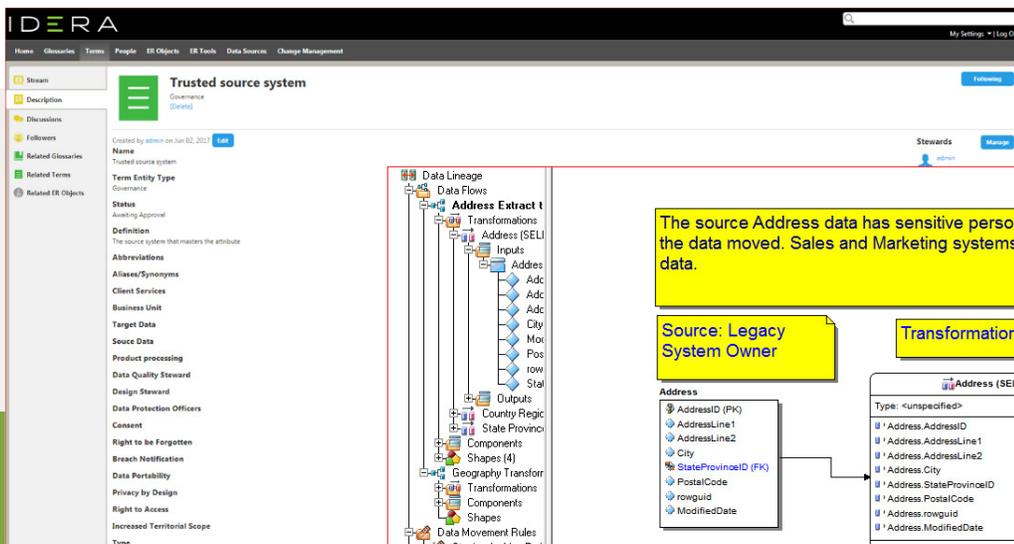


Diagram 5 Stewards assigned to business terms and additional custom ownerships defined

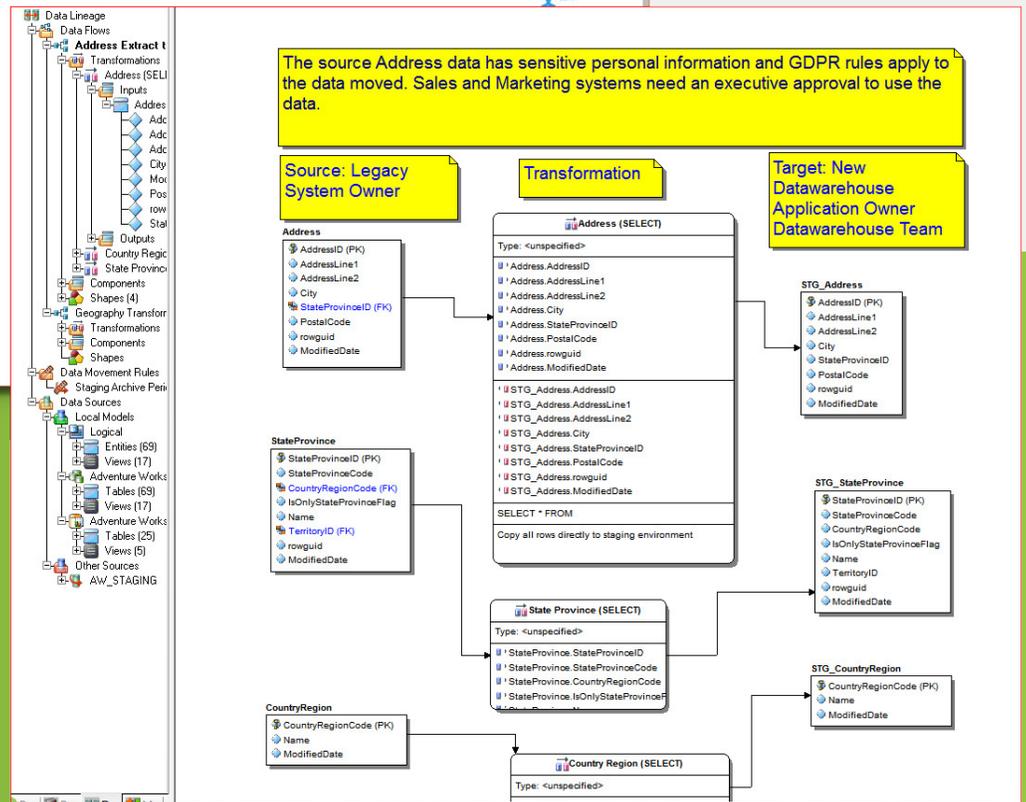


Diagram 6 ER/Studio's data lineage supports data flows and data ownership documentation

DOCUMENT AND MANAGE INDIVIDUAL RIGHTS

The new GDPR law strengthens the data protection rights for EU citizens and they will have more rights regarding their personal data information than any previous data protection directives.

According to the new law:

- Personal data must be erased if individuals do not want their data to be processed.
- They have to opt-in instead of opt-out. In order to process personal data information, organizations need an active consent from individuals, which applies only for the purpose the consent was given.
- Data must be transparent and users have the right to know which data is stored and how it is processed by organizations and their partners located in the European Union or elsewhere.
- Data must be portable. That means organizations have to ensure that data can easily be transferred from one service provider to another.

That means organizations should keep records of what customers consented to and make it accessible in case they are asked to provide proof. On the other side, organizations should know what data they have received from other suppliers and how long to keep them. Most business applications today and their existing data models do not currently include these additional GDPR-related PII fields. With ER/Studio Data Architect, organizations can model, tag, capture permissions, and relate critical data elements, business data objects, and attributes defined across the organization with customizable metadata information and rules like data erasure, access, portability and usage, as seen in Diagram 7.

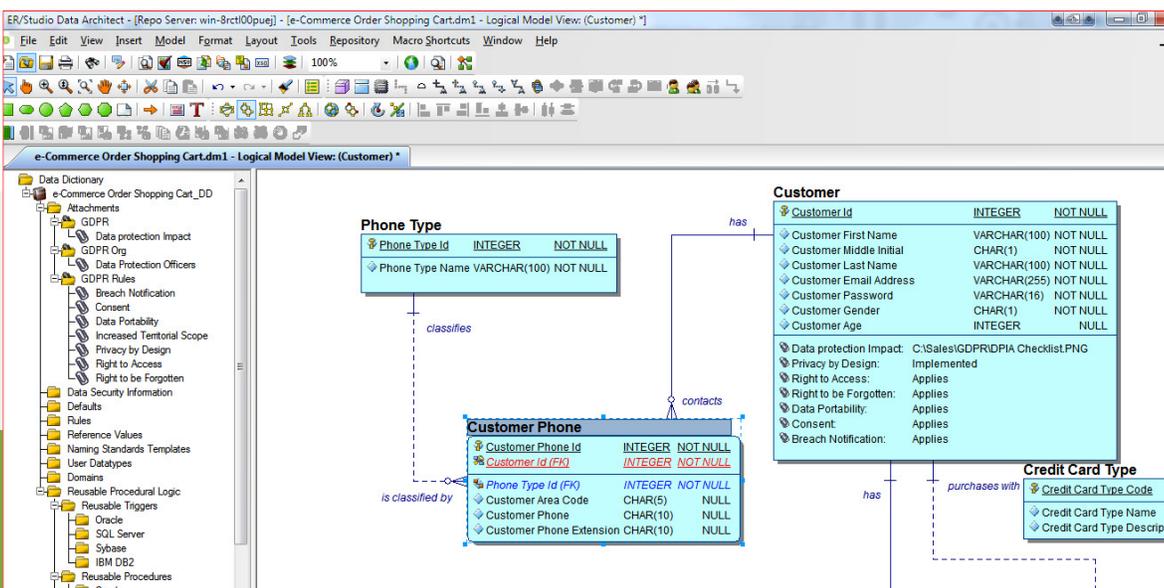


Diagram 7 Data Architects can define the rules for sensitive information within the model

This information gets published into ER/Studio Team Server where users can view relevant data objects, as seen in Diagram 8. This allows, for example, a search for all data elements which need “data access or erasure” across all applications and a report to be generated for analysis and auditing. As shown in Diagram 9 below, ER/Studio Team Server comes with an interactive diagram viewer, providing users with a visual and interactive representation of data objects, rules and related parent objects. Diagram 10 displays search results on critical and sensitive data objects tagged with GDPR rules and annotations.

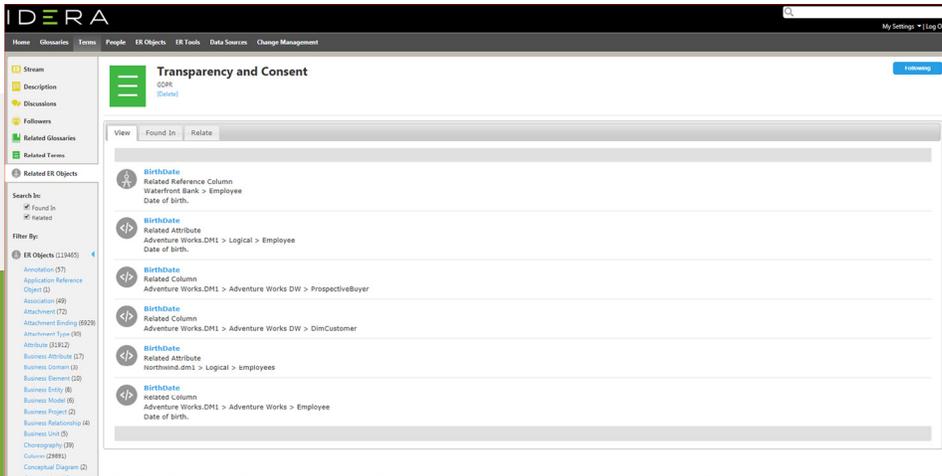


Diagram 8 Business analysts can search all data objects across applications related to data subject “transparency and consent”

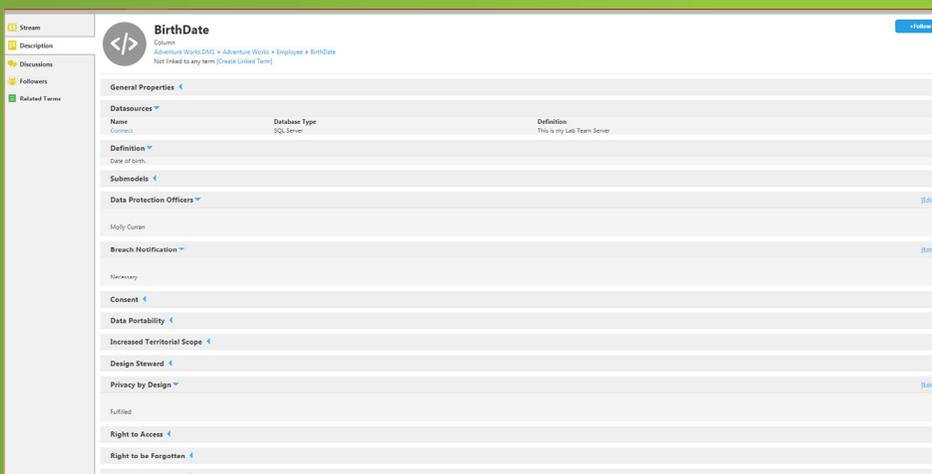
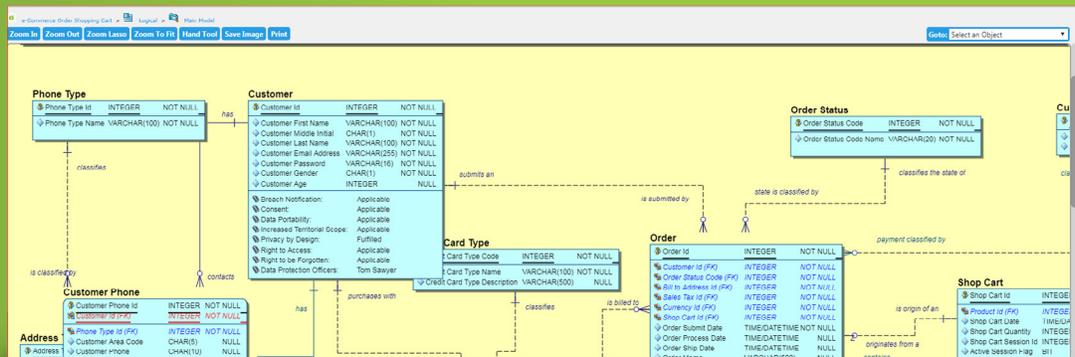


Diagram 9 Data Analysts can view and print diagrams that show how data entities are tied to GDPR rules

Diagram 10 Data Elements can be tagged with GDPR rules and annotations

DEFINE PROCESSES FOR SECURITY MANAGEMENT AND DATA BREACH NOTIFICATION

GDPR will introduce data loss and breach notification requirements and requires security of processing personal information. That means organizations have to implement technical and organizational measures to meet these requirements.

ER/Studio Business Architect can be used to define, document, search and report on the processes, technology and people involved in case of a personal data breach and the actions organizations must take to comply with the data processing.

As shown in Diagram 11, data architects can define and attach metadata information to the customer data regarding data processing and GDPR compliance. The process diagram shown in Diagram 12 represents the supervisory authorities which must be informed, along with all information and data subjects which must be included in the notification. These data can also be shared with authorities if they might want to perform auditing of the data protection rules and technologies implemented to secure data processing activities.

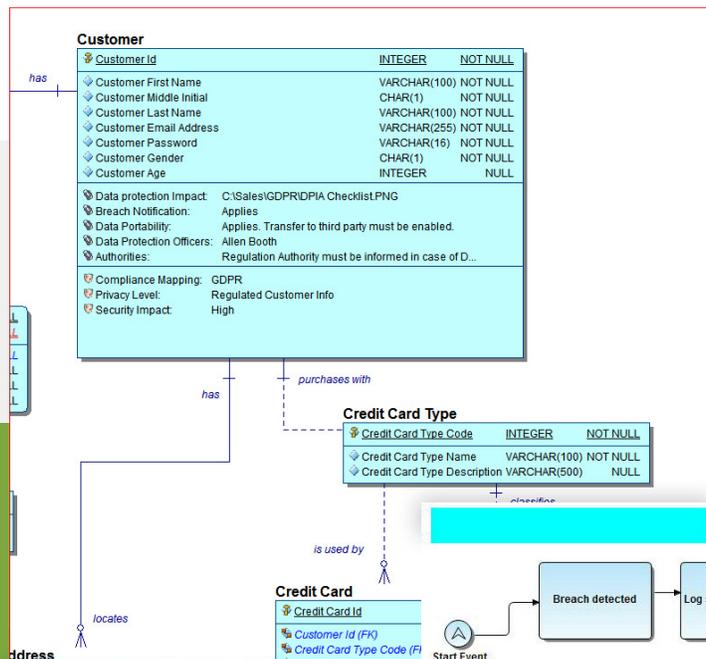


Diagram 11 Metadata for data security and GDPR-related rules for Customer

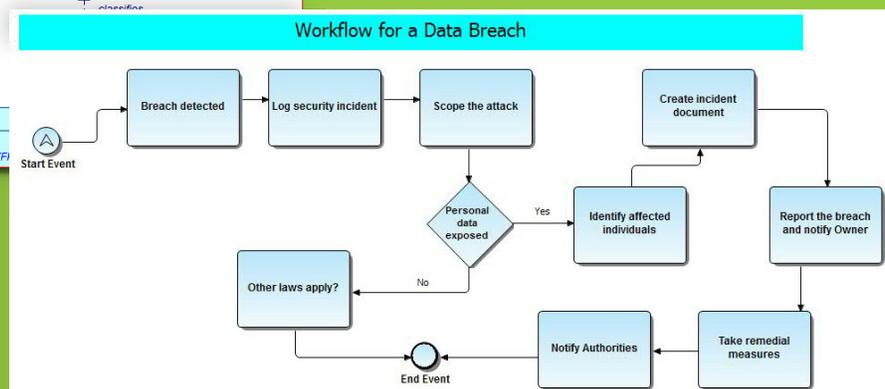


Diagram 12 ER/Studio Business Architect data breach workflow process diagram

DATA GOVERNANCE, COLLABORATION AND DATA PROTECTION IMPACT ASSESSMENT

The pillars of data quality, security and enhancement are data governance processes and organizational setups existing within an organization. The data governance team and the data architects play an important role to meet the regulatory compliance with GDPR. They need to develop a compliance plan to address all potential issues necessary to improve existing systems and to create standards for future systems, including products, data flows and processes where people are involved. This plan should involve and come from all departments as this encompasses the whole organization. A successful data governance program is also based on collaboration. Every business application project should involve not only the development or testing team but also the data owners, business analysts, subject matter experts and data leaders. Not considering those resources might require application re-design if the impact on data protection cannot be envisaged appropriately.

It is also a good practice to have a data protection impact assessment (DPIA) to understand the impact of unintended data changes and the business risks associated with this change. According to GDPR, DPIA is a must for organizations dealing with “large scale data processing.”

ER/Studio Enterprise Team Edition helps also to identify where data elements are used across different applications and databases. Additionally, metadata attachments can be added to those personal data elements to investigate and document how such risks will be mitigated. Collaboration is intrinsic and a key functionality within the product with the ability to discuss and comment on all data elements. All the data is transparent and accessible across the organization via a web interface. As compliance must be continual, organizations need to have an end-to-end living documentation of their data governance compliance plan at their fingertips anytime. Diagram 13 below shows how visual metadata information like DPIA risks can be associated with customer personal data in ER/Studio Data Architect.

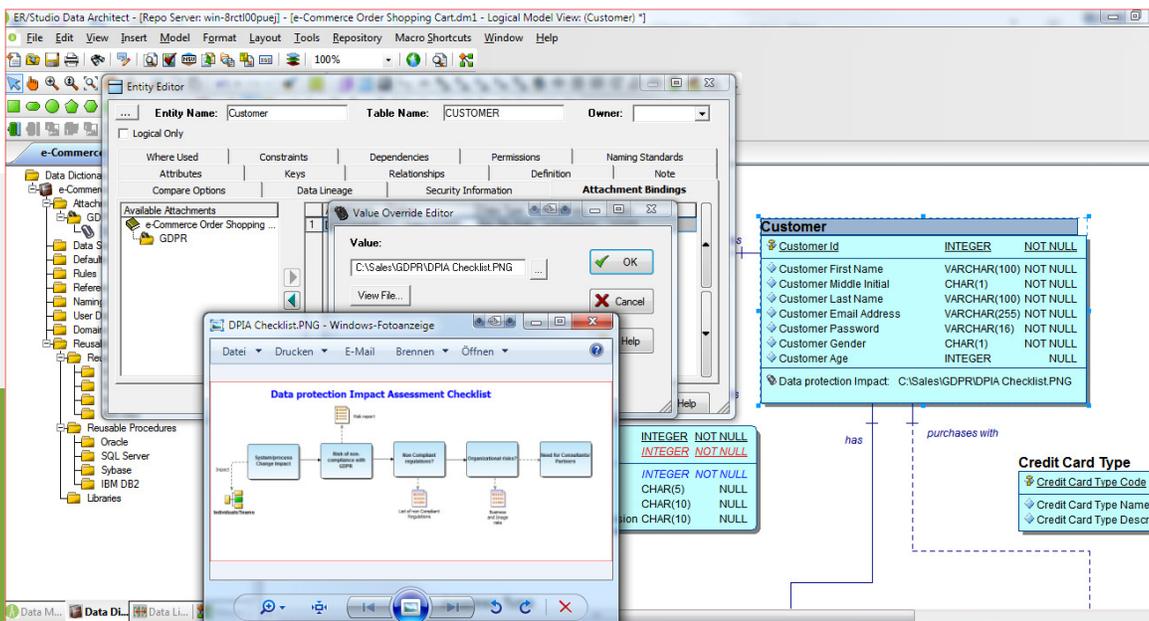


Diagram 13 This diagram depicts the checklists and risks associated with the customer data

Diagram 14 shows the related data objects associated with the specific entity, and Diagram 15 displays how the information is shared across the organization in ER/Studio Team Server.

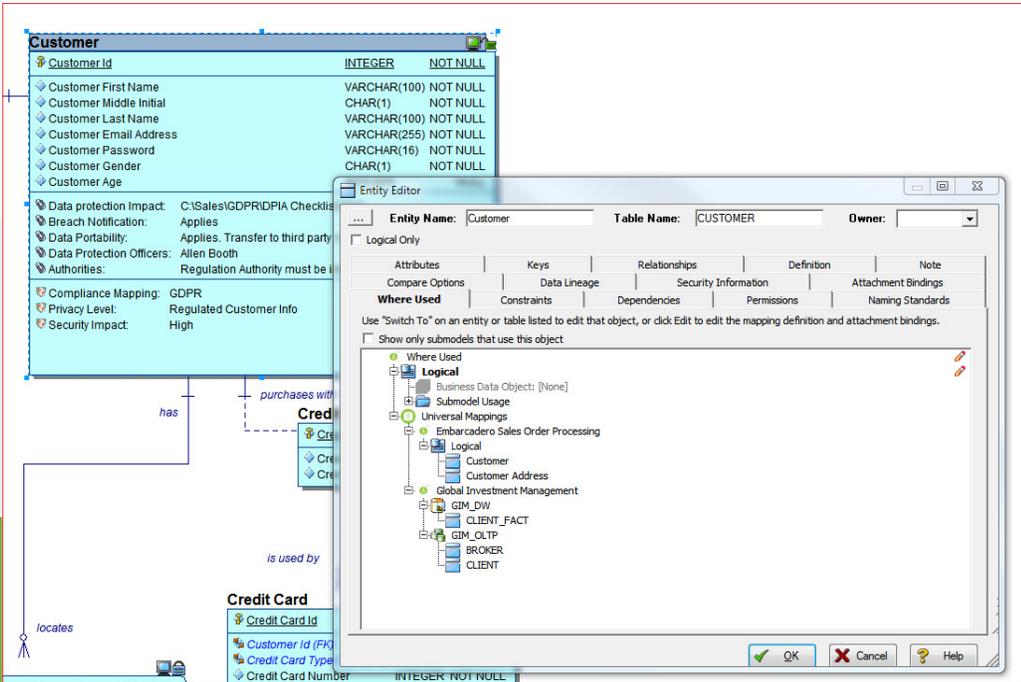


Diagram 14 The Universal Mapping facility in ER/Studio shows related data objects across different applications

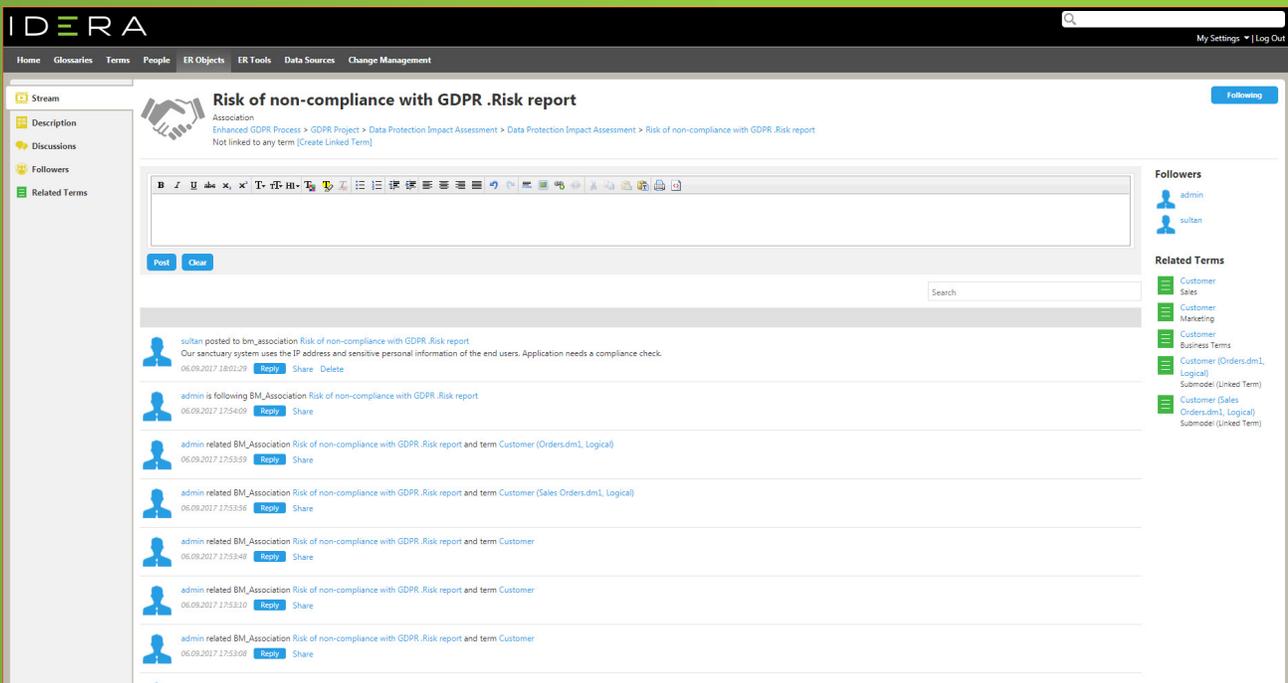


Diagram 15 The organization can run discussions and learn about data compliance and usage

SUMMARY

GDPR expects customer data privacy and industry compliance by design and default.

The first step to support data protection requirements would be to establish a robust data governance program and create awareness about the rules and impact of not being GDPR compliant, leveraging integrated process and data modeling tools.

Discovery is the second step to look into existing systems and processes. Whether we are working on new systems or looking into existing legacy systems, we need to store and maintain our data fields in line with the GDPR rules. ER/Studio Enterprise Team Edition gives organizations visibility into their applications, databases and processing activities holding critical information for GDPR compliance. It helps them to understand the data itself, the applications using it and how it is used across repositories and enables compliance by design.

Finally, ER/Studio serves as a collaboration platform for sharing information related to different applications and systems across the organization. It helps also to document and encourage discussions on data how organizations are complying with GDPR legislation within the organization and external regulators in case of an audit.

IDERA understands that IT doesn't run on the network – it runs on the data and databases that power your business. That's why we design our products with the database as the nucleus of your IT universe.

Our database lifecycle management solutions allow database and IT professionals to design, monitor and manage data systems with complete confidence, whether in the cloud or on-premises.

We offer a diverse portfolio of free tools and educational resources to help you do more with less while giving you the knowledge to deliver even more than you did yesterday.

Whatever your need, IDERA has a solution.

I D E R A