Columbus® Once you know how...

GDPR: The Compliance Journey

Contents

GDPR: The Compliance Journey

Mitigate risks, ensure compliance and build trust

The General Data Protection Regulation (GDPR) imposes new rules on organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents, no matter where they are located. The GDPR not only applies to organizations located within the EU but it will also apply to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. GDPR will ensure that individuals (Data subjects) have full visibility on how their data is controlled and processed. In short, it aims to make data subjects the real masters.

GDPR compliance can be a very challenging goal if the organization's data landscape is highly diversified and fragmented. To achieve GDPR compliance and have full control of the data assets, organizations should have a comprehensive governance, risk management, and compliance (GRC) strategy in place. This gives a direction for evolving an effective data privacy regime that helps mitigate risks, ensure compliance, build trust and protect organization's brand value.

Five phases to a successful GDPR compliance

Lay the groundwork for a successful compliance journey early on, when you define the project goals. At that time, you also should review your existing business processes and data landscape, identify organization's exposure, key focus areas and activate a project governance structure to help meet the goals. You define and document the top-priority as-is and to-be processes and map organization's capabilities to them.

Columbus suggests a phased approach to the GDPR compliance journey. Five phases of this journey are:

Understanding the five phases of GDPR compliance journey

1 Discover

Understand the GDPR requirements and the rights of data subjects. Identify the complete organization-wide data inventory and processing. Prepare a complete inventory of data subjects PII Data. Prepare an inventory of all information and processing flows across the organization including third party and different member states operations. Identify high-risk areas so that you are able to prioritize the compliance activities.

Data Discovery : Any PII or PHI (Name , Email Address , Social media posts , Criminal, Physical, physiological, or genetic information, Medical information, Biometrics, Location, Bank details, IP address, Cookies, Cultural identity).

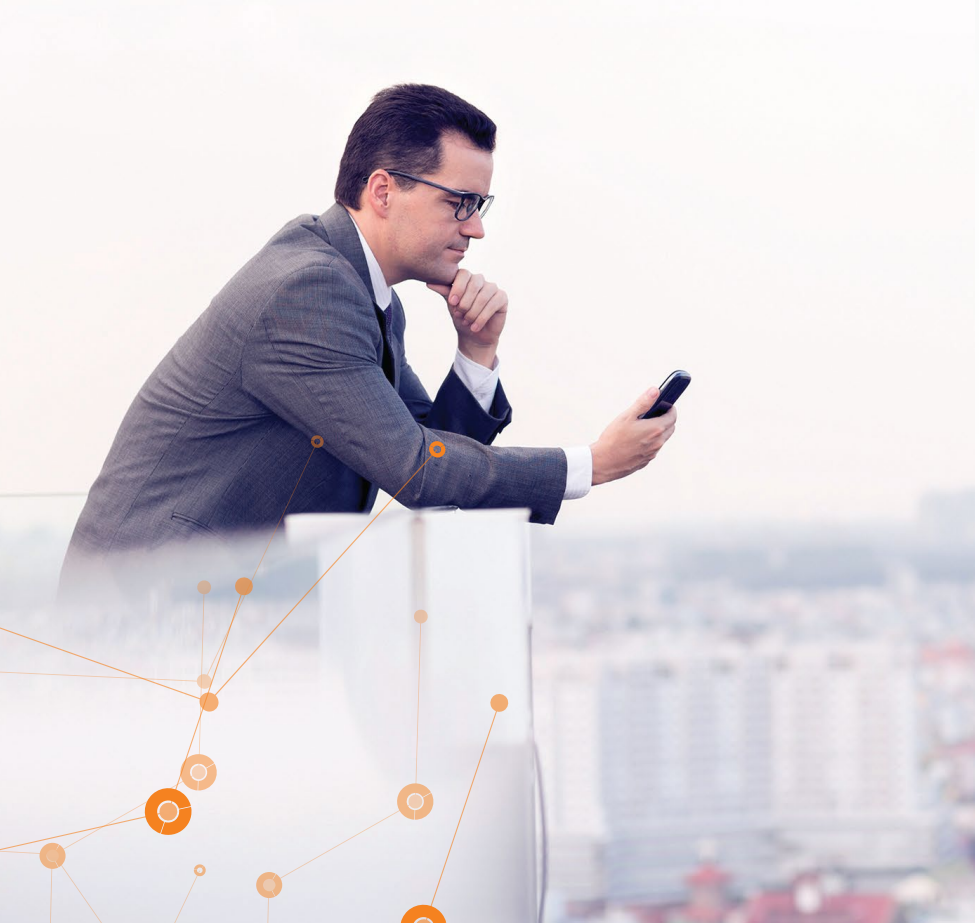
Data Sources: All places where personal data is captured and stored (Emails, Documents, Databases, Digital (Removable media), Metadata, Log files, External (data sharing), Backups)

2 Define

Define the compliance program charter, organization exposure and prioritize the activities. Map and analyze complete details of data collection, storage, and processing. List down the existing data protection capabilities within the organization. Analyze existing risk management and security policies and list down the gaps with respect to GDPR requirements. By the end of this phase organization should reach out to executive management for the project funding and support.

Data categorization: Structuring and classifying data to ensure proper handling (Types, Sensitivity, Context / use, Ownership, Custodians, Administrators, and Users).

Data sources: All locations where personal data is captured, stored and processed (Emails, Hard copies, Databases, Digital (Removable media), Metadata, Log files, External (data sharing), Backups).



3 Develop

Develop phase should start with the setting of a GDPR compliance Program Management Office and data governance policies. Develop specific compliance strategies to fill in the gaps. Develop corrective actions to fill the gap and confirm buy- in from the stakeholders for any additional investment.

Develop data governance: Defining policies, roles and responsibilities for the management and use of personal data (At rest, In process, In transit, Storing, Recovery, Archiving, Retaining, and Disposal).

Develop project governance: Overall governance within the key stakeholders (CIO, Head Compliance, Corporate Governance group, Information Risk group, Head Legal, Data protection officer. Human resources).

4 Deploy

Validate the new compliant processes and implement the monitoring and processes and applications. Data breach reporting, in particular, should be thoroughly tested based on the industry KPIs like MTTI (Mean time to identify) and MTTR (Mean time to response).This phase involves deploying the new systems, processes, and changes to existing data protection policies. By the end of this phase acceptance from the GRC team and sign off from the GDPR Compliance PMO should be taken.

Deploy data attacks prevention strategies: Protecting your data (Physical datacenter protection, Network security, Storage security, Compute security, Identity management, Access control, Encryption, Risk mitigation).

Identifying & reporting breaches: Monitoring for and detecting system intrusions (System monitoring, Breach detection, assessing impact, planned response, Disaster recovery, Notifying DPA & Data subjects).

5 Sustain

Ensure perennial support for the new GDPR compliant setup by institutionalizing accountability and DPO Compliance Analytics. This can be ensured by having a dedicated GRC team supporting the ongoing compliance. DPO dashboards and other monitoring tools processes need to be updated to be in sync with the GDPR requirements.

In case of a change in GDPR requirement, an initiative should be launched to realign with the new requirements. A key capability in this sustenance phase is an ongoing capability to provide evidence of accountability and compliance.

Ongoing compliance and record keeping: Enterprises will need to record the: (Purposes of processing, Classifications of personal data, Third-parties with access to the data, Organizational and technical security measures, Data retention times).

Reporting solutions: Implement reporting capabilities:(Cloud services (processor) documentation, Audit logs, Breach notifications, Handling Data Subject Requests, Risk management reporting, Governance reporting, Compliance reviews).

Align business processes with the ERP system

In managing the security of business roles, ERP system, and data, your organization needs to remain accountable to all the compliance mandates that affect your operations. Because roles, ERP, and data cannot be separated from the business processes that structure all activities within your organization, and you also need to include all the workflows and processes in planning compliance and security.

Columbus RapidValue BPM suite, a business process management tool at use in many different organizations, provides the means to sync business processes with the ERP system and align both business activities and ERP with your company's objectives and strategy. All organization specific GRC (governance, risk management, and compliance) and GDPR business processes and flows can be mapped as a solution in RapidValue BPM Suite.

Achieving GDPR compliance with RapidValue BPM Suite

- RapidValue BPM suite helps you in creating the data model, application model, process model, and business process model for your organization.
- All GDPR related vision, mission, goals, and metrics (example MTTI-Mean Time to Identify, MTTR-Mean Time to Resolve in case of a breach) can be mapped in RapidValue BPM Suite.
- RapidValue BPM suite can also be linked to your process model. This helps you identify the applications that have a touch point with personal data (PII).
- RapidValue BPM Implementation Work Space provides your GDPR team a perfect tool to gather evidence; tracking compliance of those applications across functional groups and provide a complete a project orientation across your GDPR compliance journey.

Steps to GDPR compliance

1. Define your organization's GDPR vision, strategy, goal and maps in RapidValue BPM Suite.
2. Create a GDPR Compliance Journey solution in RapidValue BPM Suite.
3. Import GDPR requirements and description and map your Policies in RapidValue BPM Suite. This includes all Data subject requirements and Privacy requirements as well.
4. Map third party and different member state governance.
5. Map Enterprise Risk, remediation, compliance and resiliency process in RapidValue BPM Suite.
6. Capture specific Audit requirements in RapidValue BPM Suite. For D365 for FOE, To-increase Security and Compliance Studio helps you track close to 40 different event types.
7. Personally Identifiable Information (PII) mapping across your organization flows. Highlight all Business processes, flows, and activities with PII or PHI data.
8. Identify the key data elements as PII or PHI Data Objects in RapidValue Data Objects. This includes- Data items (Name, email address, health data, credit card info, bio metrics, location data, and criminal records), Data formats (paper records, database, and digital like USB etc.), Data Locations (on premise, cloud, and third party. different member state) and Data Transfer methods (Internal, external, social media, mobile, posts etc.)
9. Scope and phase out your GDPR compliance project. Phase the separate compliance project activities into Discover, Define, Develop, Deploy and Sustain milestones in RapidValue BPM Suite.
10. Do a Fit-Gap analysis so that there are no gaps in your compliance efforts to meet the deadlines

Business strategy

Mission statement

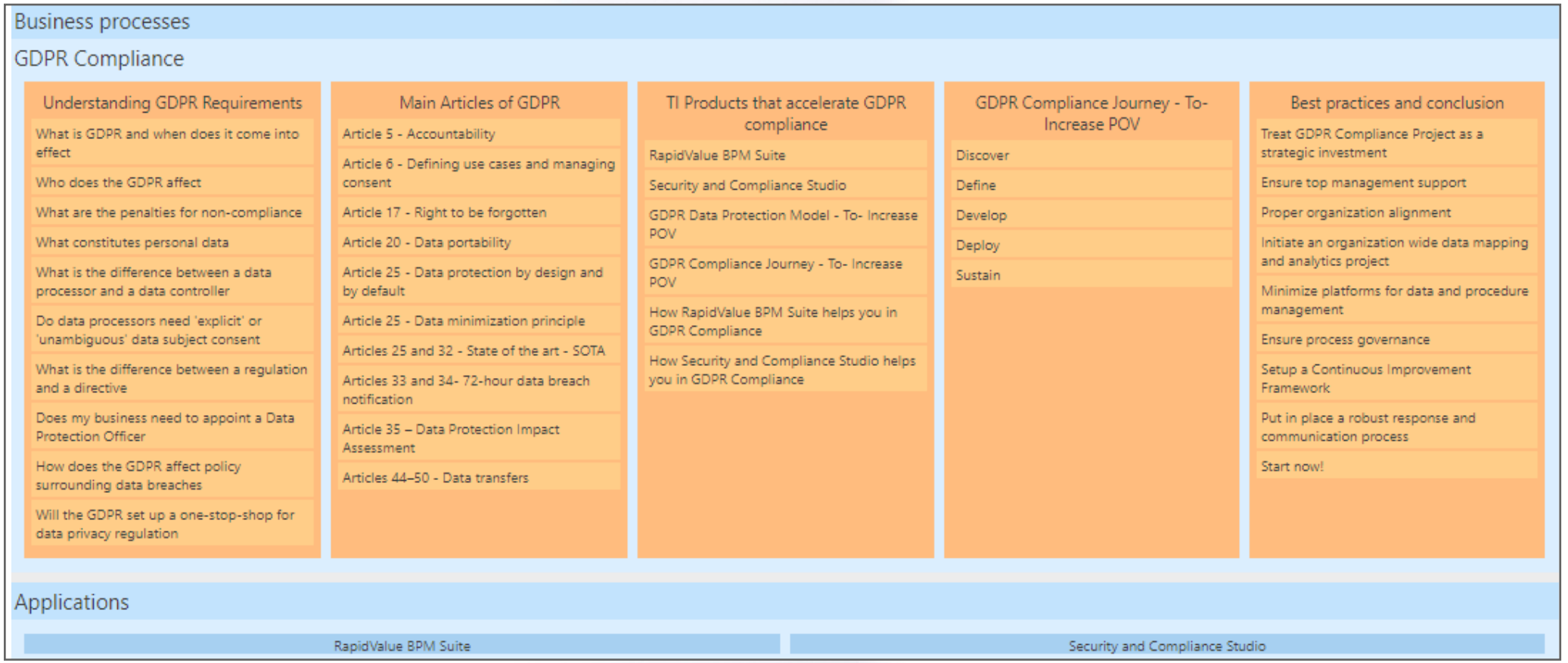
To be GDPR compliant before the 25th, May 2018. The General Data Protection Regulation (GDPR) will come into force on the 25th May 2018, replacing the existing data protection frameworks for member states under the EU Data Protection Directive.

It is essential that our organisation starts immediately to prepare for the implementation of GDPR by carrying out a analysis of all our current or envisioned information processing in line with GDPR. This will allow time to ensure that we have adequate procedures in place to deal with the improved transparency, accountability and individuals' rights provisions, as well as optimizing our approach to governance and how to manage data protection as a corporate issue. It is essential to start planning our approach to GDPR compliance early , and to ensure a cohesive approach among the key data protection stakeholders in the organisation.

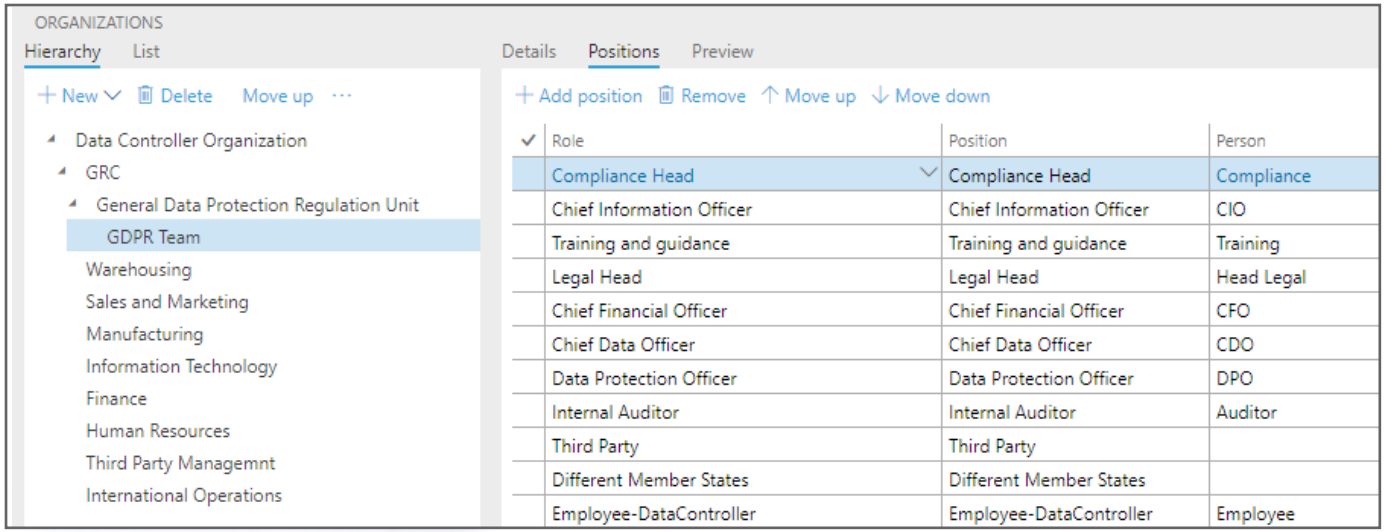
Business goals

Goal	Importance
Always use customer consent as ground to process	Very high
Comply with privacy by design within organization	Very high
Comply with processing children's data.	Very high
Become ready for mandatory breach reporting.	Very high
Have a Data subject communication strategy	Very high
Comply with Data subject privacy rights	Very high
Become GDPR Aware	Very high
Establish an internal GDPR governance team	Very high
Become GDPR Accountable	Very high
Implement Data Protection Impact Assessment	Very high
Implement Data protection by Design and default	Very high
Ensure different state compliance	High
Ensure Third party compliance	High

1.0 GDPR Organization strategy model mapped in RapidValue to detail GDPR Mission, Goals and KPIs.



1.1 GDPR Organization process and application model mapped in RapidValue. Organizations may need investment in ISV or other applications to meet GDPR data subject rights as mentioned in Chapter-3 (Article 12-23) Rights of the data subject



1.2 GDPR Organization model mapped in RapidValue to detail GDPR governance structure, departments, roles and positions.

11. Analyze gaps to create System requirements. Push these requirements to VSTS for subsequent development work.

12. Conduct Data Protection Impact Assessments (DPIAs) using RapidValue as the base.

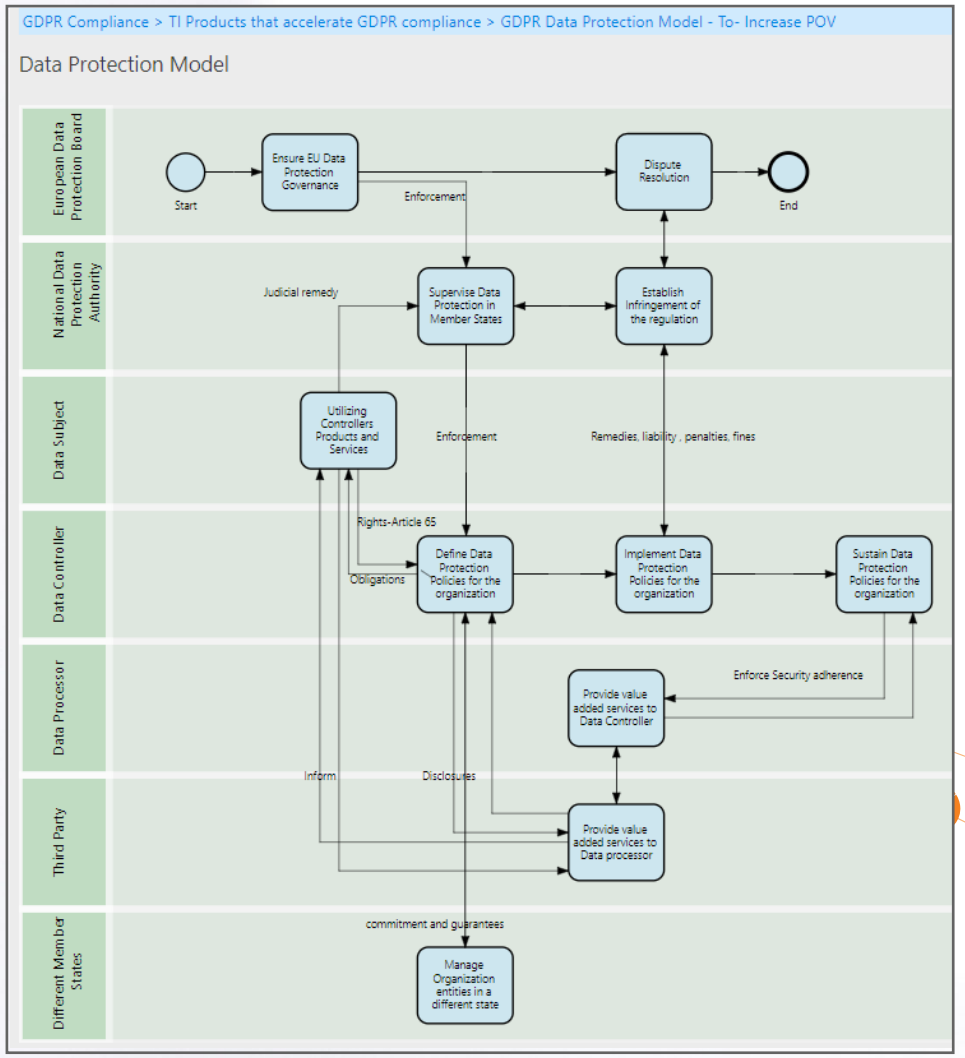
13. Conduct a data mapping exercise in RapidValue BPM suite. Store all DPIA related "Questions" as RapidValue Solution Questions. These can be used whenever a DPIA Exercise is done.

14. Use RapidValue BPM Suite to create Acceptance Test plan, Test specifications, and Report.

15. Perform the acceptance test involving all flows with Personally Identifiable Information (PII) in D365 for FOE or other applications.

16. Once GDPR compliant, use RapidValue BPM suite as the primary business process management and knowledge management tool across your organization.

17. And finally, maintain and continuously evolve your business processes to keep them relevant.

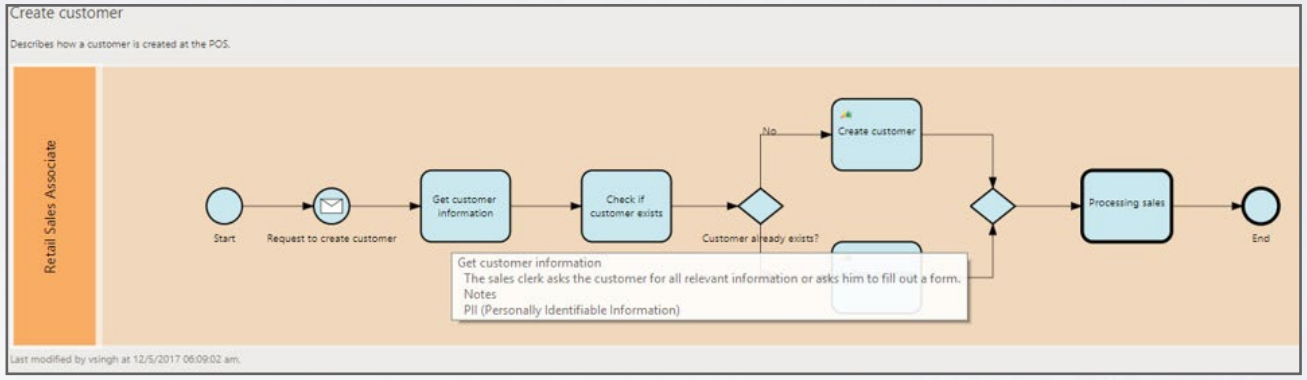


1.3 Data Protection Model

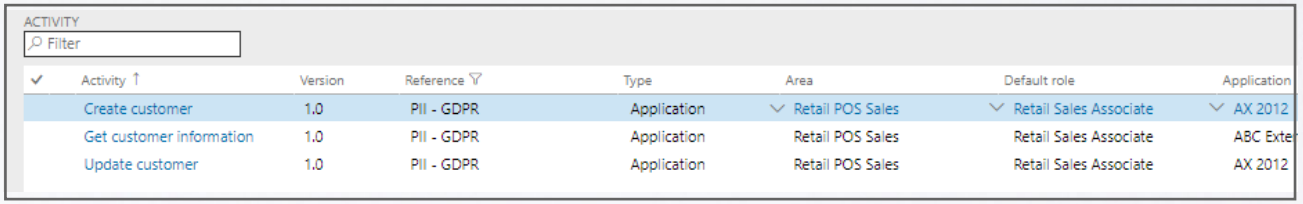
Data flow example during DPIA (Data Protection Impact Assessment)

RapidValue BPM suite helps you identify, capture, categorize, and analyze all activities which involve dealing with personally identifiable information or protected health information. An example of a retail sale is shown below. Flow activity highlights any PII data processing in an activity.

All business processes, flows, and activities related to GDPR compliance can be sorted easily to identify an organization's exposure and help it focus on high-risk areas. This helps prioritize the activities as well.



1.4 PII data processing



Activity	Version	Reference	Type	Area	Default role	Application
Create customer	1.0	PII - GDPR	Application	Retail POS Sales	Retail Sales Associate	AX 2012
Get customer information	1.0	PII - GDPR	Application	Retail POS Sales	Retail Sales Associate	ABC Exte
Update customer	1.0	PII - GDPR	Application	Retail POS Sales	Retail Sales Associate	AX 2012

1.5 An example of a retail sale

How Columbus Security and Compliance Studio supports GDPR compliance

Columbus Security and Compliance Studio helps you implement your GDPR Audit and privacy requirements in one place if you are using D365 for FOE.

It also supports the key GDPR requirement of "Data protection by design and default" by ensuring the security concepts are implemented in a fashion where the users get the minimum possible access that helps them complete their work optimally.

Columbus Security and Compliance Studio has features to track any changes to user-defined PII (Personally Identifiable Information) information in D365 for FOE using data security. Key cornerstones of this solution are Security, Audit, Compliance, and Transparency.

6 key GDPR compliance takeaways from Columbus Security and Compliance Studio

1. **Security Management** - Easily setup role based security – simply record your process and match and/or create your security role. Supports the GDPR principle of "Data protection by design and default" by assigning the roles to the user with minimum required access.

2. **Audit Management** - Significantly reduce time on internal IT audits since auditors are provided dynamic access to all the relevant data in simple-to-understand views. In case of a data breach or fraud, these audit logs are of tremendous help to track the reason and subsequently also inform the Data subject.

3. **Compliance Management** - Avoid data misuse and fraud by making sure that users can only access data and functions that are needed for their role. Organizations should ensure that they capture all GDPR specific SoD rules and violations in D365 FOE and regularly monitor the in-compliance charts in SCS.

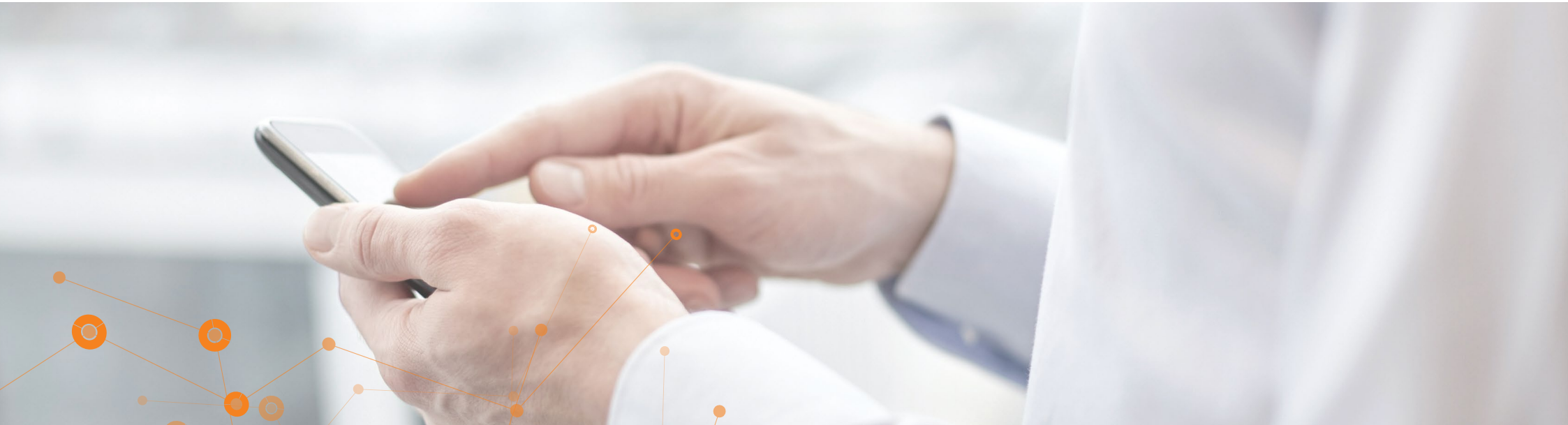
4. **Security Request Management** - GDPR related Security, Audit and compliance requirements can be captured in Security request management system. It helps security or compliance officer to implement requests like; Copy security setup, Import users from Azure AD with multiple options, etc.

5. **Actionable BI charts** - Enhance transparency with predefined embedded insights. Charts provide actionable BI in workspaces with drill-down features. All workspaces come with predefined charts and graphs.

6. **Data Security** - Data security feature in Security and Compliance Studio helps you define and monitor track any changes to user-defined PII (Personally Identifiable Information) or PHI (Protected Health Information) in D365 for FOE using data security.

10 ways to make your GDPR Compliance a Success

1. Treat GDPR compliance project as a strategic investment with perennial benefits.
2. Ensure top management support. Business and IT Leadership (Chief information officer and legal head) should own the responsibility for GDPR compliance project deliverable.
3. Proper organizational alignment. This should involve chief information security officer, legal, compliance, HR, and data Protection officer.
4. Initiate an organization-wide data mapping and analytics project. Minimize platforms for data and procedure management for cloud, on-premise and unstructured data. Ideal will be having just one platform which provides a complete overview at any time.
5. Ensure process governance .i.e. ongoing maintenance of process documentation.
6. Setup a continuous improvement framework which involves SOTA (state-of-the-art) targets.
7. Put in place a robust response and communication process if in the worst case a breach happens.
8. Once GDPR compliant, know how RapidValue BPM Suite can implement specific GRC (governance, risk management, and compliance) and GDPR business processes and flows
9. Align your GDPR compliance goals and objectives with RapidValue BPM Suite.
10. As an extension, know how Security and Compliance Studio for D365 for FOE enables companies to take a major step towards safeguarding data assets and resources in alignment with GDPR compliance.



Columbus® Once you know how...

Next steps

Columbus serves organizations in many industries and across the world's regions by helping them transform their business for the digital era and by mitigating the risks of running a company in a competitive, fast-changing environment, using innovative technology.

If you would like to discuss your GDPR compliance journey, Contact Columbus

www.columbusglobal.com