MEGA

SEE THE BIGGER PICTURE

6 Steps to GDPR Compliance-by-Design

Accelerate your journey to GDPR compliance

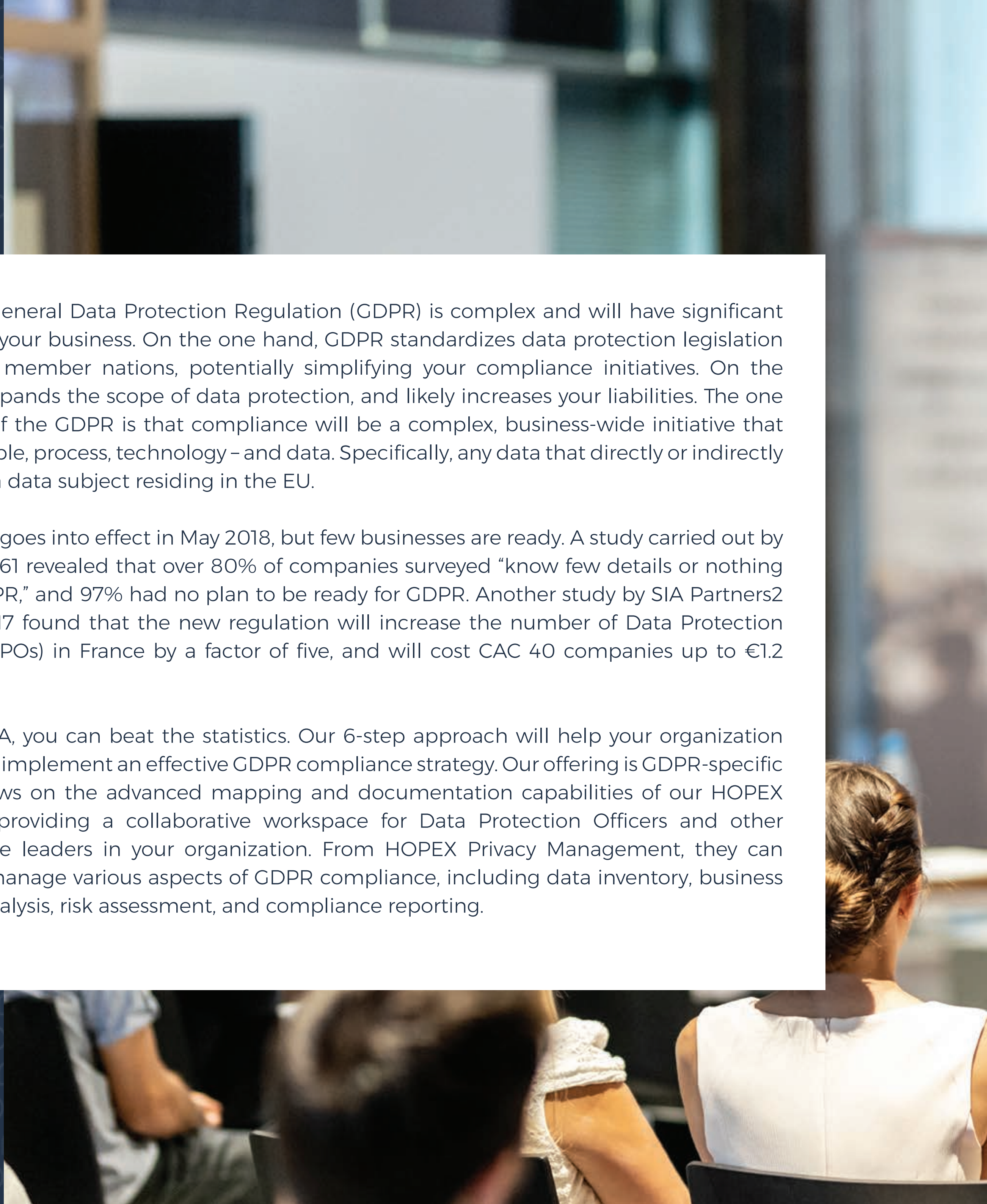
White paper

Introduction

The new General Data Protection Regulation (GDPR) is complex and will have significant impact to your business. On the one hand, GDPR standardizes data protection legislation for all EU member nations, potentially simplifying your compliance initiatives. On the other, it expands the scope of data protection, and likely increases your liabilities. The one certainty of the GDPR is that compliance will be a complex, business-wide initiative that spans people, process, technology – and data. Specifically, any data that directly or indirectly identifies a data subject residing in the EU.

The GDPR goes into effect in May 2018, but few businesses are ready. A study carried out by Dell in 20161 revealed that over 80% of companies surveyed “know few details or nothing about GDPR,” and 97% had no plan to be ready for GDPR. Another study by SIA Partners2 in May 2017 found that the new regulation will increase the number of Data Protection Officers (DPOs) in France by a factor of five, and will cost CAC 40 companies up to €1.2 billion.

With MEGA, you can beat the statistics. Our 6-step approach will help your organization assess and implement an effective GDPR compliance strategy. Our offering is GDPR-specific and it draws on the advanced mapping and documentation capabilities of our HOPEX platform, providing a collaborative workspace for Data Protection Officers and other compliance leaders in your organization. From HOPEX Privacy Management, they can centrally manage various aspects of GDPR compliance, including data inventory, business process analysis, risk assessment, and compliance reporting.



GDPR Explained

The GDPR is EU legislation that aims to standardize data protection regulations across all member nations. It further aims to expand the protection of its citizens by including new rights and applying them to any entity, even those outside the EU, controlling or processing any data that can directly or indirectly be used to identify a person. These rights include:

Right to Access

A data subject's right to know what personally identifiable information (PII) is collected and processed by which authority, and for what purpose. Additionally, the right to obtain a copy of that data, free of charge.

Right to be Forgotten

A data subject's right to stop dissemination and processing of PII and, when practical, to erasure. Conditions for erasure may include purpose for data is no longer valid or withdrawal of consent by data subject.

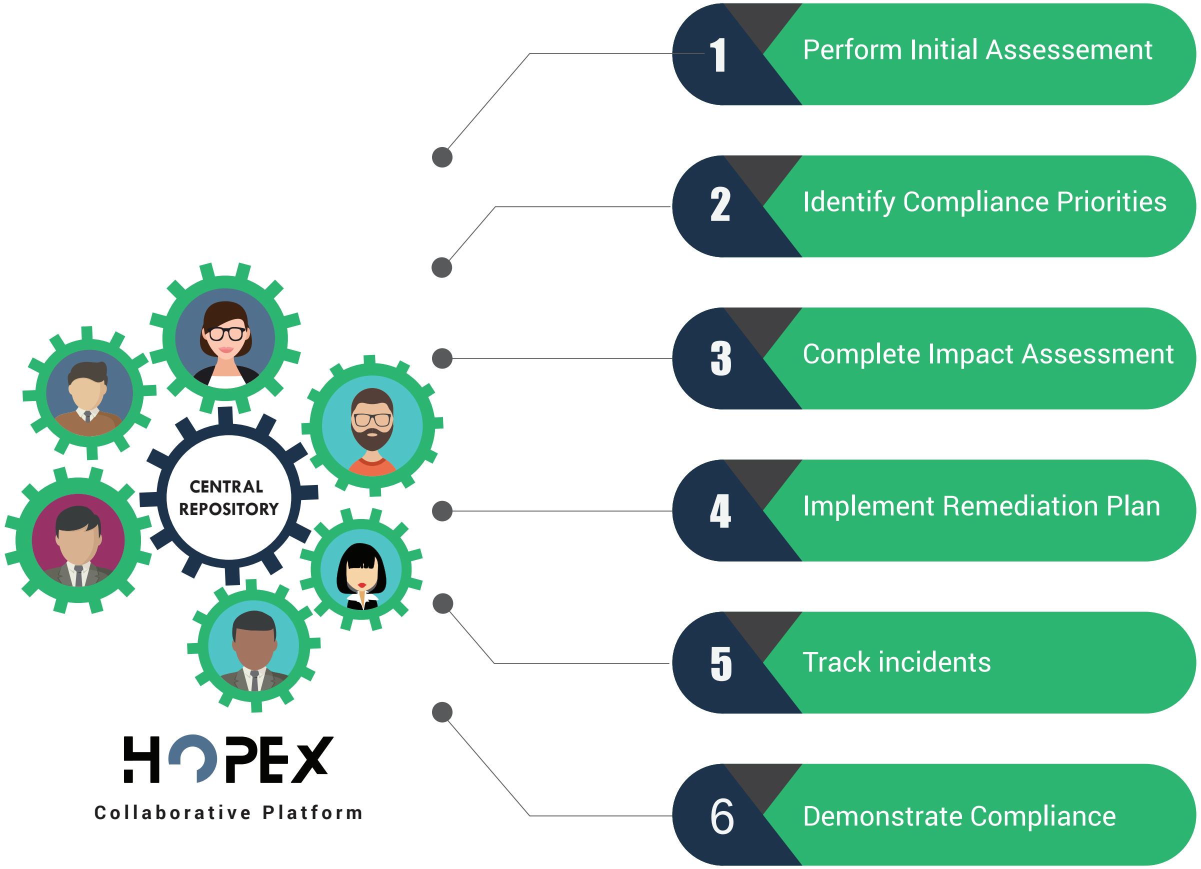
Right to Data Portability

A data subject's right to transfer PII from one controlling authority to another.

Such broad sweeping legislation effectively makes the HOPEX Privacy Management the first global data protection law. Other key elements of the HOPEX Privacy Management are data privacy impact assessments, mandatory disclosure of data breaches within 72 hours of identification and, in some cases, a dedicated DPO. Not to mention, mandated privacy by design and demonstrable achieved compliance. Failure to comply with the HOPEX Privacy Management can lead to fines of €10-20 million or 2-4% of total revenues, whichever is greater.

6 steps to HOPEX Privacy Management Compliance-by-Design

You can take the lead on GDPR compliance following 6 steps. Review effective strategies to assess your compliance needs, focusing on identifying and prioritizing PII processing. Learn new tactics to remediate non-compliance, leveraging business process modeling. See how to demonstrate compliance to your executive leaders and supervisory authorities with in-depth documentation and reporting capabilities.



1 Perform Initial Assessement

2 Identify Compliance Priorities

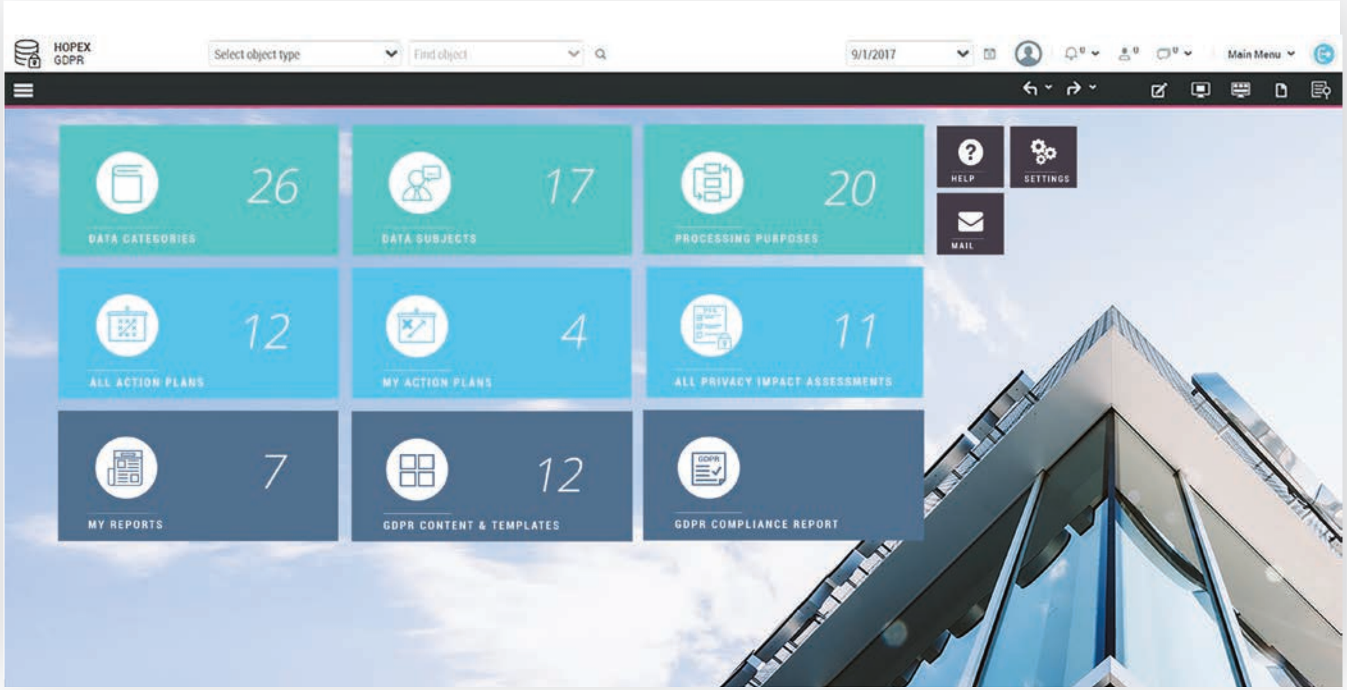
3 Complete Impact Assessment

4 Implement Remediation Plan

5 Track incidents

6 Demonstrate Compliance

HOPEX Privacy Management home page



1. Perform the Initial Assessment

The requirements of the GDPR are extensive and require cross-functional collaboration from members of every facet of the business – from marketing and sales, to legal and human resources, to security and IT. Together, compliance leaders are responsible for the planning and execution of regulatory activities. However, to be truly effective in their pursuits, they must not only engage one another in this context, but must also work to instill a “data privacy first” culture within their organization.

The role of the DPO, new to the GDPR, should support compliance leaders and include responsibility for coordinating data protection efforts and providing organizational training to ensure their effectiveness. The role will include many other responsibilities that may or may not require a dedicated resource. That will depend on the complexities of the business. For instance, businesses controlling and processing categories of PII relating to criminal activities will have greater regulatory demand and require a dedicated DPO resource.

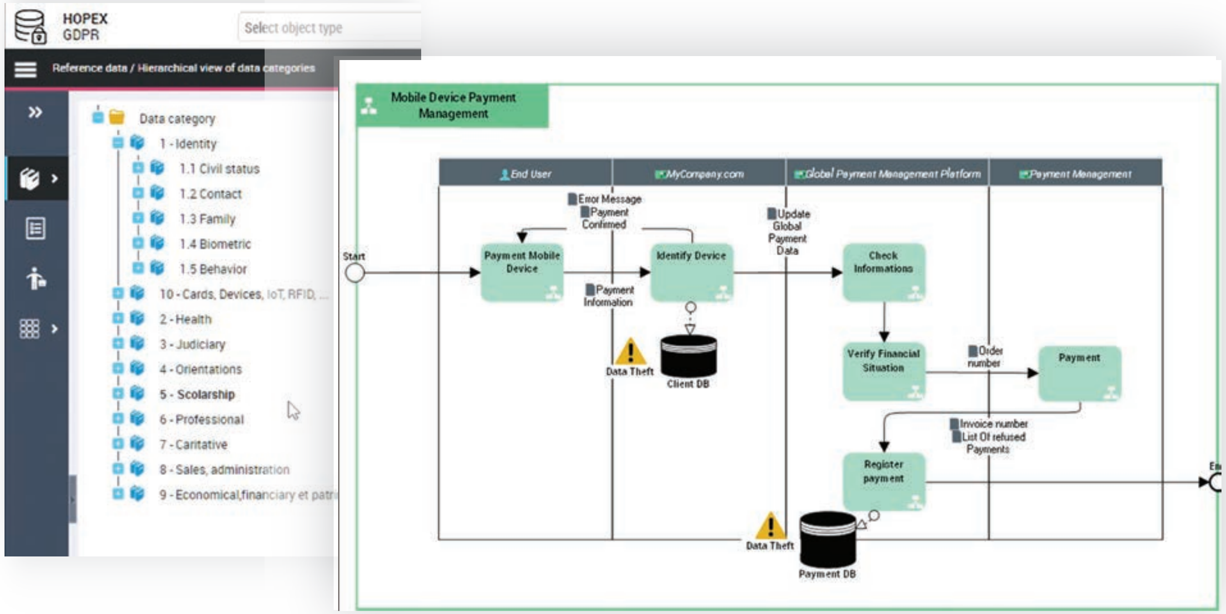
The initial responsibility of the DPO and compliance leaders will be to perform a preliminary GDPR impact assessment that includes the following activities:

- Identify all data, associated applications and storage
- Identify PII that directly or indirectly identifies a data subject
- Determine controlling and/or processing authority of PII
- Identify business processes utilizing PII
- Identify people interacting with PII

Additionally, the preliminary assessment should consist of a categorized and prioritized data inventory. This will make it easier to identify critical PII in business processes and to understand the interactions between data and people.

MEGA's HOPEX Privacy Management includes a centralized workspace dedicated entirely to GDPR compliance. Designed for the DPO and compliance stakeholders, the centralized workspace fosters cross-functional collaboration and makes it easier to categorize and prioritize data, review data flow charts and generate reports.

A central repository of your data inventory that also includes associated applications and business processes like HOPEX Privacy Management, can further simplify stakeholders' work and serve as a foundation for many other compliance efforts.



HOPEX GDPR

Select object type

Reference data / Hierarchical view of data categories

- Data category
  - 1 - Identity
    - 1.1 Civil status
    - 1.2 Contact
    - 1.3 Family
    - 1.4 Biometric
    - 1.5 Behavior
  - 10 - Cards, Devices, IoT, RFID, ...
  - 2 - Health
  - 3 - Judiciary
  - 4 - Orientations
  - 5 - Scolarship
  - 6 - Professional
  - 7 - Caritative
  - 8 - Sales, administration
  - 9 - Economical,financiary et patri

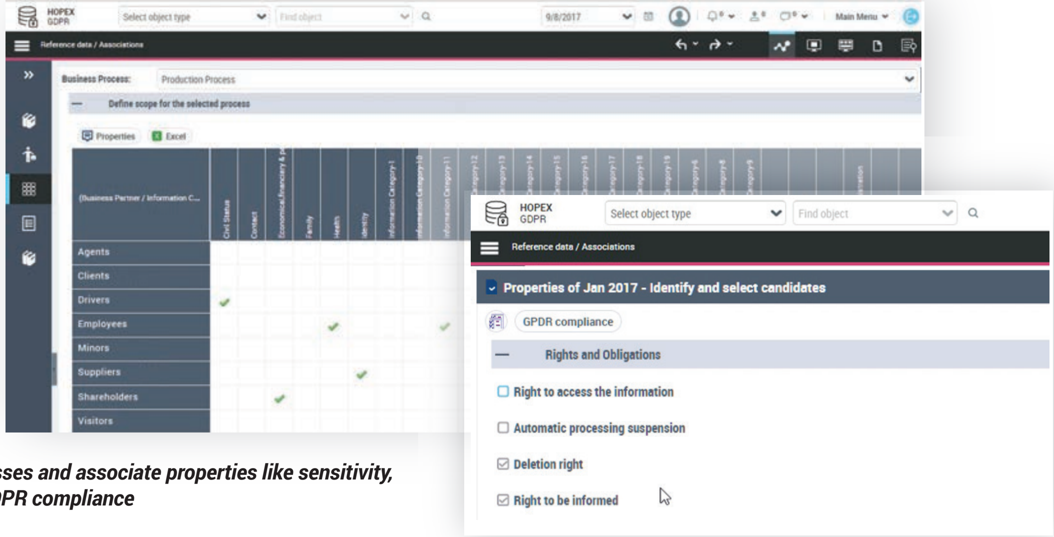
From a central repository, compliance leaders can categorize data, map data to business processes and review individual processes in detail

2. Identify Your Compliance Priorities

The GDPR aims to regulate the life cycle of data, requiring business to not only know what data they have but also why they have it and how they care for it. Data inventory must therefore be more than a list of data controlled and/or processed by your business or associated third parties. It must also reflect the need and use of the data. Categorization and mapping of data to people, processes and technology helps to assess the use, while prioritization of data (where priority is based on sensitivity) helps to assess the need. When the two are cross-referenced, interactions with the most critical PII are exposed. This is essential in your efforts to further assess your compliance needs.

Data categories are logical groupings of individual data elements. Each data category allows for further description and assessment of data sensitivity. The categories, when aligned with business processes, enable you to quickly associate groups of data and expose prioritization of compliance actions. Remember, any data that can directly or indirectly be used to identify a data subject is subject to the regulation. Meaning, data that does not identify a data subject on its own (but does when grouped with other data) is subject to the regulation. This is why mapping data elements to data categories, to data flows, and to people is a critical step. When you can logically view the relationships between data, categories, processes, and people, you see the logical links to the data subjects. You have full insight to what specific data elements are personally identifiable and therefore, can determine appropriate compliance measures.

HOPEX Privacy Management automatically cross-references data categories and business processes to expose processes that manage PII. Users can drill down on these intersections to see their prioritization, define compliance actions to be taken, and share them with other team members.



Properties of Jan 2017 - Identify and select candidates

GPDR compliance

Rights and Obligations

☐ Right to access the information

☐ Automatic processing suspension

☑ Deletion right

☑ Right to be informed

Cross reference data categories and processes and associate properties like sensitivity, to manage GDPR compliance

3. Complete an Impact Assessment

The Data Privacy Impact Assessment (DPIA) is a key component of the GDPR. The regulation requires an impact assessment be performed against any process that is at risk of violating the data privacy rights of data subject. Ideally, the assessment is completed prior to implementing processes, allowing the business to mitigate any identified risks. In many cases, this mandatory document will be requested by a regulator. The report should include data processing activities that potentially impact the rights and freedoms of data subjects. A DPIA report may contain the following:

- Description of the process, its operations and purpose
- Assessment of the impact to data subjects' rights and freedoms
- Measures taken to mitigate this impact, including the mechanisms used to ensure personal data protection

MEGA's recommended approach for performing a DPIA is as follows, and it can and should be tailored to suit your company's specific needs:

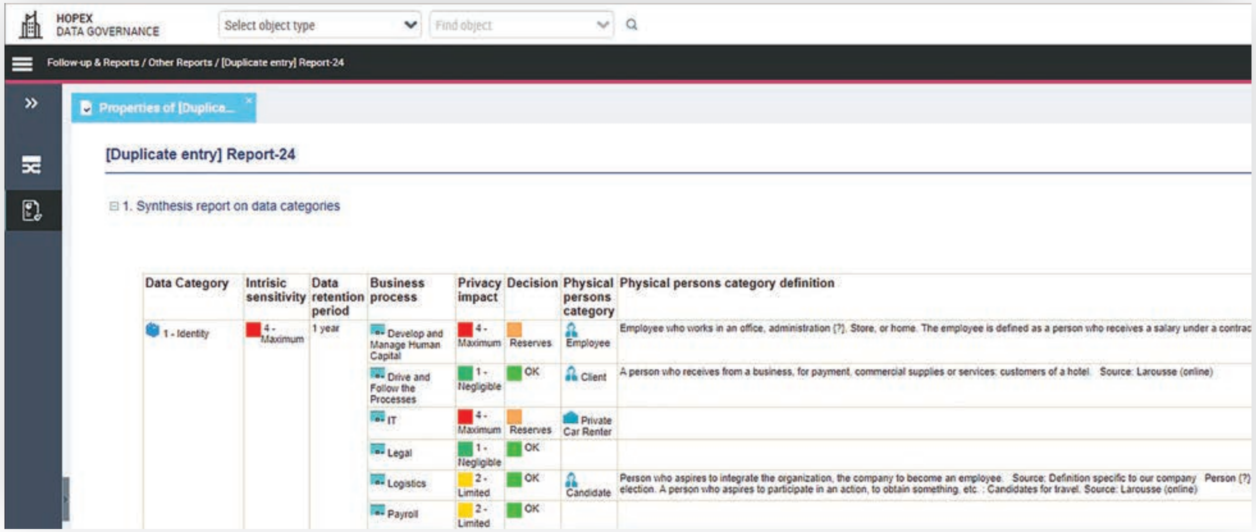
Document high risk business processes
Describe in detail current and planned data processes that pose a high risk to data subjects' rights and freedoms, including their operations and purpose. Utilize business process maps to show specific PII processing activities.

Perform impact assessment of processing activities
Evaluate the risks to the rights and freedoms of data subjects. Associate process operations to supporting technologies and people to show impact to GDPR compliance and expose the risks of non-compliance.

Describe specific measures taken to mitigate risks
Risk mitigation may include the implementation of data security technologies (like encryption), but could also include modification to business processes or the training of employees on proper PII handling.

Define operating models that are secure-by-design
Communicate how your business will adjust over time to be compliant-by-design in a specific area.

Business process maps that illustrate data flow and show where it intersects with applications and people are foundational elements to GDPR compliance and integral components of a DPIA. MEGA's solution provides additional process modeling capabilities that enable you to analyze modifications prior to implementation so you can assess business impact and compliance impact. These modeling capabilities can be used further to define secure–by-design operations, strengthening your compliance.


HOPEX
DATA GOVERNANCE
Select object type
Find object
Follow-up & Reports / Other Reports / [Duplicate entry] Report-24
Properties of [Duplica...

[Duplicate entry] Report-24

⊟ 1. Synthesis report on data categories

Data Category	Intrisic sensitivity	Data retention period	Business process	Privacy impact	Decision	Physical persons category	Physical persons category definition
1 - Identity	🟥 4 - Maximum	1 year	Develop and Manage Human Capital	🟥 4 - Maximum	🟧 Reserves	Employee	Employee who works in an office, administration (?). Store, or home. The employee is defined as a person who receives a salary under a contrac
			Drive and Follow the Processes	🟩 1 - Negligible	🟩 OK	Client	A person who receives from a business, for payment, commercial supplies or services: customers of a hotel. Source: Larousse (online)
			IT	🟥 4 - Maximum	🟧 Reserves	Private Car Renter	
			Legal	🟩 1 - Negligible	🟩 OK		
			Logistics	🟨 2 - Limited	🟩 OK	Candidate	Person who aspires to integrate the organization, the company to become an employee. Source: Definition specific to our company Person (?) election. A person who aspires to participate in an action, to obtain something, etc. : Candidates for travel. Source: Larousse (online)
			Payroll	🟨 2 - Limited	🟩 OK		

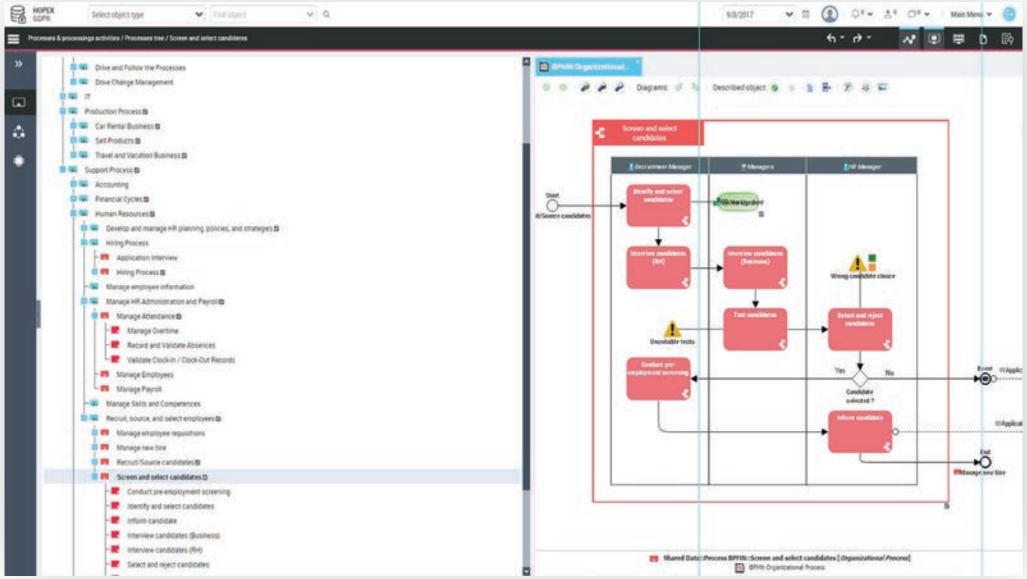
GDPR synthesis report showing data level results of a DPIA

4. Implement a Remediation Plan

DPIA findings expose areas that require remediation work. One element of remediation will be business process analysis as many of the processes that were identified as controlling or processing PII will need to be secured. It is important that this be done without negatively impacting the business, and mapping updates is an effective means to uncover dependencies and avoid unnecessary costs.

Also, while one aim of the GDPR is to secure the life cycle of PII, another is to expand the data privacy rights for data subjects. The right to access, to be forgotten, and to portability will each require new business processes to support them.

Specialized software like HOPEX can help you design, model, and communicate new and updated process. When these changes also incorporate IT systems, your business can organize operations to deliver “compliant-by-design” products and services without sacrificing business agility. The ability to fully support continuous business change without impact on compliance is critical in the digital era.


HOPEX GDPR
Select object type
Find object
9/8/2017
Main Menu
Processes & processings activities / Processes tree / Screen and select candidates
Drive and Follow the Processes
Drive Change Management
IT
Production Process
Car Rental Business
Sell Products
Travel and Vacation Business
Support Process
Accounting
Financial Cycles
Human Resources
Develop and manage HR planning, policies, and strategies
Hiring Process
Application interview
Hiring Process
Manage employee information
Manage HR Administration and Payroll
Manage Attendance
Manage Overtime
Record and Validate Absences
Validate Clock-In / Clock-Out Records
Manage Employees
Manage Payroll
Manage Skills and Competences
Recruit, source, and select employees
Manage employee requisitions
Manage new hire
Recruit/Source candidates
Screen and select candidates
Conduct pre-employment screening
Identify and select candidates
Inform candidate
Interview candidates (Business)
Interview candidates (RH)
Select and reject candidates
BPMN Organizational...
Diagrams
Described object
Screen and select candidates
Recruitment Manager
Managers
HR Manager
Start
R/Source candidates
Identify and select candidates
Interview candidates (RH)
Interview candidates (Business)
Wrong candidate choice
Test candidates
Select and reject candidates
Unsuitable tests
Conduct pre-employment screening
Yes
No
Candidate selected ?
Event
Inform candidate
End
Manage new hire
Shared Data::Process BPMN::Screen and select candidates [Organizational Process]
BPMN Organizational Process

Model business processes and data flows to be "compliant-by-design"

5. Track Incidents

The GDPR Article 33 requires the controller to notify a Supervisory Authority of a personal data breach within 72 hours of discovery, unless the breach is unlikely to infringe on data subjects' privacy rights. Therefore, monitoring data processing activities and tracking incidents – where an incident may directly or indirectly result in non-compliance or a data breach – will be ongoing compliance efforts for every business.

HOPEX Privacy Management provides a portal for any person within a business to report an incident. The DPO and other compliance leaders can centrally review reported incident, assign severity and notate remediation activities to manage ongoing compliance. Relative to data breaches, the central reporting capabilities can speed time to discovery and response, ensuring companies react appropriately, within the allotted 72-hour period.

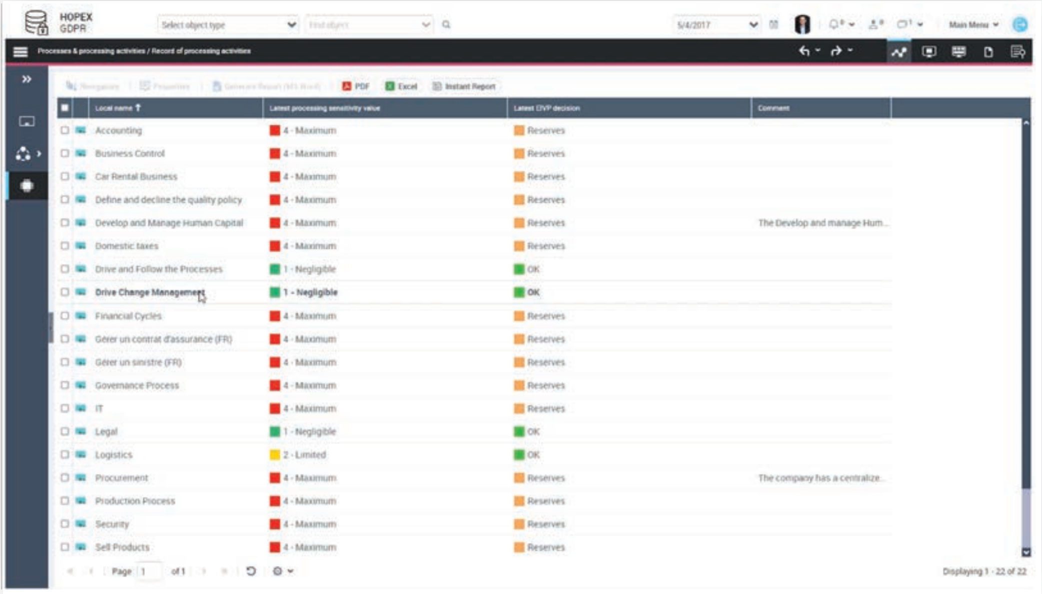
As incidents are reported and tracked, it is also important to identify their root cause. Was it a one-time failure or the result of a structural problem? Understanding the scope of the incident, where it occurred (e.g., process, business line, subsidiary), the type of data involved, the category of data, and the risk to data subjects' rights can assist in resetting compliance priorities and implementing corrective measures. Key internal stakeholders can regularly review operations and monitor associated risks from HOPEX so they can create a cycle for continuous improvement and ongoing compliance.

6. Demonstrate Compliance

The GDPR places great emphasis on proving, in a complete and comprehensive manner, that all data protection requirements are met. A Supervisory Authority may ask the DPO or other compliance leaders to provide specific information that demonstrate compliance, sometimes with a very short deadline. Requested information may include:

- A record of PII processing activities
- A record of data breaches
- Detailed DPIA on high-risk processing activities
- Contractual details between your organization and third-party vendors that process and/or control data on your behalf

The powerful reporting function available in HOPEX Privacy Management solution enables you to generate a single document that describes your processes for handling personal data, the results of your DPIA, customer requests related to personal data, and your personal data protection risks, incidents, and action plans (including progress on those plans). These records are legal documents that can be sent to your Supervisory Authority. The reports are easily configurable on format and content. The HOPEX repository is extendable to broader audience through the numerous export formats.



Local name	Latest processing sensitivity value	Latest DVP decision	Comment
Accounting	🟥 4 - Maximum	🟧 Reserves	
Business Control	🟥 4 - Maximum	🟧 Reserves	
Car Rental Business	🟥 4 - Maximum	🟧 Reserves	
Define and decline the quality policy	🟥 4 - Maximum	🟧 Reserves	
Develop and Manage Human Capital	🟥 4 - Maximum	🟧 Reserves	The Develop and manage Hum...
Domestic taxes	🟥 4 - Maximum	🟧 Reserves	
Drive and Follow the Processes	🟩 1 - Negligible	🟩 OK	
Drive Change Management	🟩 1 - Negligible	🟩 OK	
Financial Cycles	🟥 4 - Maximum	🟧 Reserves	
Gérer un contrat d'assurance (FR)	🟥 4 - Maximum	🟧 Reserves	
Gérer un sinistre (FR)	🟥 4 - Maximum	🟧 Reserves	
Governance Process	🟥 4 - Maximum	🟧 Reserves	
IT	🟥 4 - Maximum	🟧 Reserves	
Legal	🟩 1 - Negligible	🟩 OK	
Logistics	🟨 2 - Limited	🟩 OK	
Procurement	🟥 4 - Maximum	🟧 Reserves	The company has a centralize...
Production Process	🟥 4 - Maximum	🟧 Reserves	
Security	🟥 4 - Maximum	🟧 Reserves	
Sell Products	🟥 4 - Maximum	🟧 Reserves	

Demonstrate compliance with detailed data processing reports

Conclusion

The GDPR is here to stay and it doesn't discriminate on size, industry, or revenue. You're running out of time to get into compliance. Have you planned out your scope of work? Do you know how much information you already have available, and which information you need to collect and assess? What about the risks? With HOPEX Privacy Management, we can support your compliance efforts over the short- and long-term.

About MEGA

Founded in 1991, MEGA is a global software company and recognized market leader for over ten years. The company partners with customers to improve governance and accelerate transformation by leveraging technology. MEGA helps companies better analyze how they can operate and make the right decisions to accelerate the creation of value. The HOPEX Platform connects business, IT, data and risks perspectives in a single place that integrates across an entire company's ecosystem. The MEGA Services team partners with customers to deliver projects with a pragmatic approach.

www.mega.com

MEGA
SEE THE BIGGER PICTURE