

GDPR data processing inventory, Automated

Leveraging CAST Application Engineering Platform

Nicolas Derivery – VP Business Development EMEA

December 2017

- GDPR broader initiative and where CAST plays
- GDPR Automated Data Processing inventory with CAST
- Sample outputs – Let's be concrete !

Principles:

The GDPR is based on a set of principles, outline within article 5 concern fairness, lawfulness and transparency, purpose limitation, data minimization, data quality, security, integrity and confidentiality.

A new further principle is laid out in the GDPR is that of **“accountability”**: **stating that controllers shall demonstrate the compliance of their data processing.**

Accountability for all these aspects:

Lawfulness, fairness and transparency



Integrity and confidentiality



Purpose limitation



Storage limitation



Data minimization



Accuracy



Impacts:

Besides the uniformity of the principles, it is evident that a number of new measures are taking into account the **pervasiveness of IT and the risks connected to the flow of digital data within and across organizations.**

Of relevance, for every principle:

Lawfulness now implies transparency to the data subject

Data minimization is a direct consequence of the purpose limitation: no data exceeding the specific purposes of the processing shall be collected and stored

Accuracy is to be taken seriously in as far as updating, removing or promptly rectify incorrect data

Storage allowing the identification of data subjects is admissible as long as the purposes of the original collection is still be valid

Protection (291 instances) from unauthorized, unlawful processing as well as from accidental loss or damage is to be assured Finally the accountability principle requires the controller to demonstrate and document compliance with all the above mentioned principles

Implications:










All organizations processing personally identifiable information (a broader concept then sensitive data) of EU citizens (be it clients or employees) **shall comply with the principles and be able to demonstrate their compliance.**

Depending on an initial gap analysis the Regulation is implying actions on following topics:

- **Documentation**
 - Inventory of processing, risk analysis, security analysis
- **Security measures**
 - Systems security, authorization schemes, encryption, anonymization, infrastructural security
 - Implementation of data security and integrity measures
- **Data subjects rights**
 - Assure portability, right to know own data, right to opt out from automated decisions
 - Implement of new functionalities for honoring the data subject rights

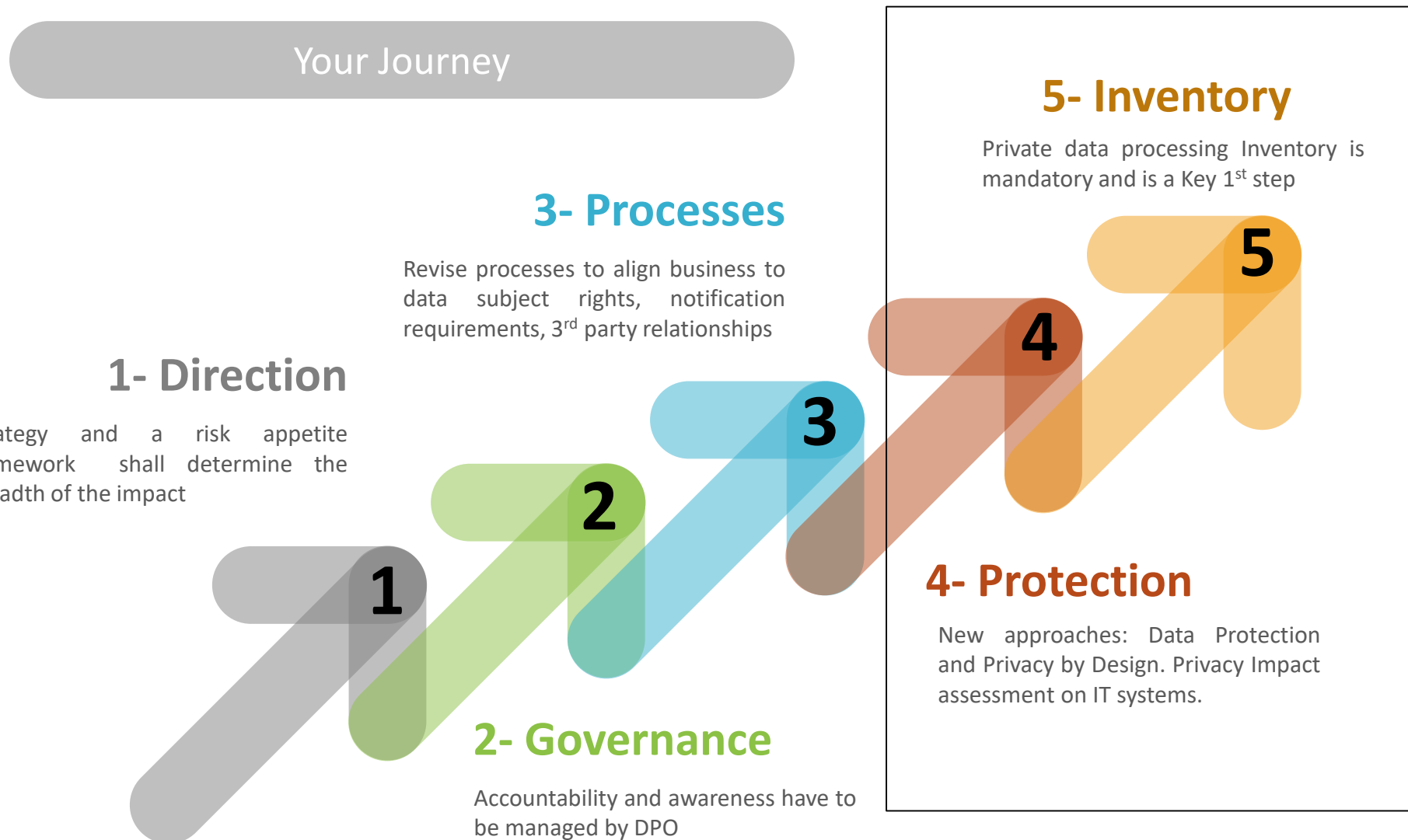
Strategy and implementation will vary across industries and depending on organization maturity might range from updating a few documents to a complete overhaul of the technical and organizational aspects of data processing

✓ A large spectrum of requirements with high stake

 Fines	administrative fines up to 4 % of the total worldwide annual turnover
 Accountability	controllers and processors must document their compliance
 PII is broadened	location data, IP addresses, voice takings are included in the new definition
 Rights	data subjects are entitled to new rights: portability, transparency, oblivion ...
 Consent	opt-in must be clear and never by default
 Notifications	by 72h since discovering any breach, authority and subjects shall be notified
 Extra Territorial	regulation applies to data related to EU citizens, globally
 DPIA	impact assessments have to be carried out on any new processing
 by Design	both at determination and at operation time, technical and organizational measures shall be taken to protect data



A long journey....Inventory Being the Hardest step





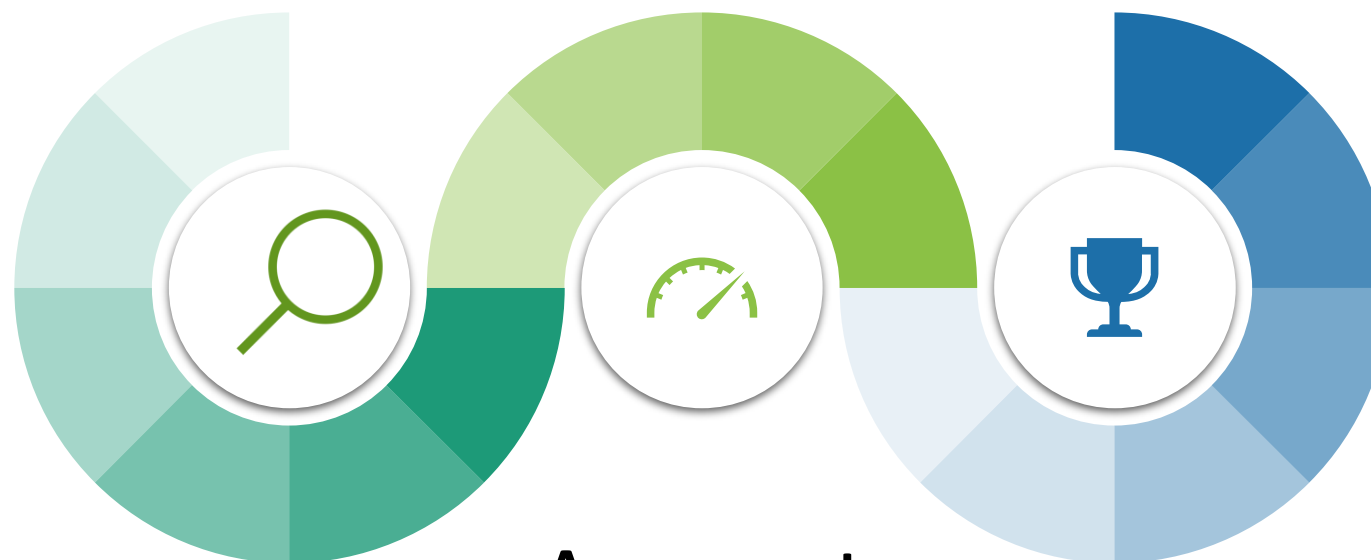
Protection: Data Protection and Privacy by Design. Privacy Impact assessment on IT systems

Data protection by Design

Data protection Impact Assessment

4- Protection

Privacy Impact Assessment (PIA) shall be conducted consistently on existing and ongoing systems.



Identification

Identifying data and processing types carrying risks shall be carried out to have enough information to prioritize correctly areas for further investigation

Assessment

Protection Impact Assessments are a sequence of steps including analysis of software assets, to determine the risk level and mitigations thereof

Remediation

Mitigation actions flow according to defined privacy risk mitigation processes, with a clear scope for residual risk –

By Design

Protecting data by design entails: both *at the time of the determination of the means for processing* and at the time of the processing itself

5- Inventory

Inventorying data and their processing is mandatory for the organizations and its systems



Personal data inventory contains:

- Legal or consent and purpose for processing
- Data involved (categories down to items)
- Applications and data location (+transferrals)
- Duration of consent
- Indication of responsibility
- Conducted risk analyses (PIAs)

The inventory of all the processes involving personal data within the organization. An inventory is essential for your oversight of processing activities and is a mandatory element of GDPR compliance (art. 30).

The inventory allows to demonstrate its awareness of its obligations as a data controller, including the keeping of records of processing activities

Knowing which personal data is processes enables mitigation actions against the risk of data breaches which might go unidentified, or reckoned too late.

- GDPR broader initiative and where CAST plays
- **GDPR Automated Data Processing inventory with CAST**
- Sample outputs – Let's be concrete !

CAST - Software Intelligence Pioneer



CAST by the Numbers

- 250+ customers worldwide
- 25+ years of software analytics experience measuring some of the most complex IT systems in the industry
- \$150M investment in R&D



Recipient of Gartner Cool Vendor Award – ‘CAST is the de facto standard for measuring quality and productivity’



‘CAST is driving standards adoption for robustness, security, maintainability, and automated function points’



‘CAST is the leading technology of its kind’



‘CAST is the leader in the business IT space’



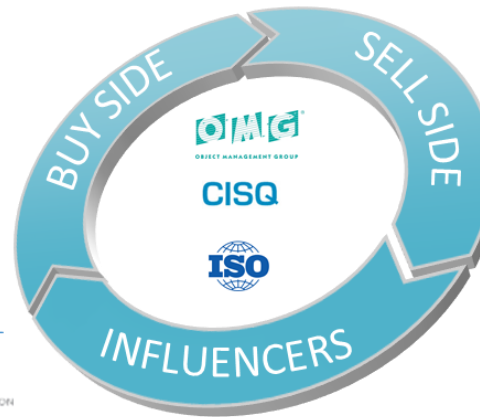
Recipient of Editor’s Choice Award – ‘A top-10 company to watch’

CAST’s technology creates a digital image of the software internal composition. Unlike code or application analysis technology, CAST applies architectural and engineering assessments. The Application Intelligence Platform’s system-level to code-level analysis examines how components interact, how they work across technology layers, data structures and end-to-end transactions - from user entry to data access. The result is a comprehensive understanding into complex software composition and unprecedented intelligence into its internal integrity.

250+ Enterprise Customers Count on CAST



Consulting Firms Recommend CAST



Global SI's ADM Delivery Rely on CAST



Global SI Provide Services Powered by CAST





CAST Application Intelligence Platform measures Resilience, Functional Sizing, Architecture from process to data

Management and Engineering Dashboards to deploy on most critical apps

Get unique analytics and insights on Risk, Agility & Cost Drivers

- System-level analysis identifies structural flaws involving interactions between components / layers that results in business disruptions
- Actionable insights on all major technologies (J2EE, .NET, Cobol, C++, ERPs)

Automated, Benchmarked, Standards-based (Appmarq Benchmarking)

- Automation ensures consistency, reliability
- Benchmarking against Industry and Technology peers
- Objective measurement based on industry standards

Engineering dashboard to remediate, improve, transform

- Mapping of best practices & flaws with KPIs
- Spots system-level flaws that code checkers can not see

Unique architecture module to discover, transform, develop apps

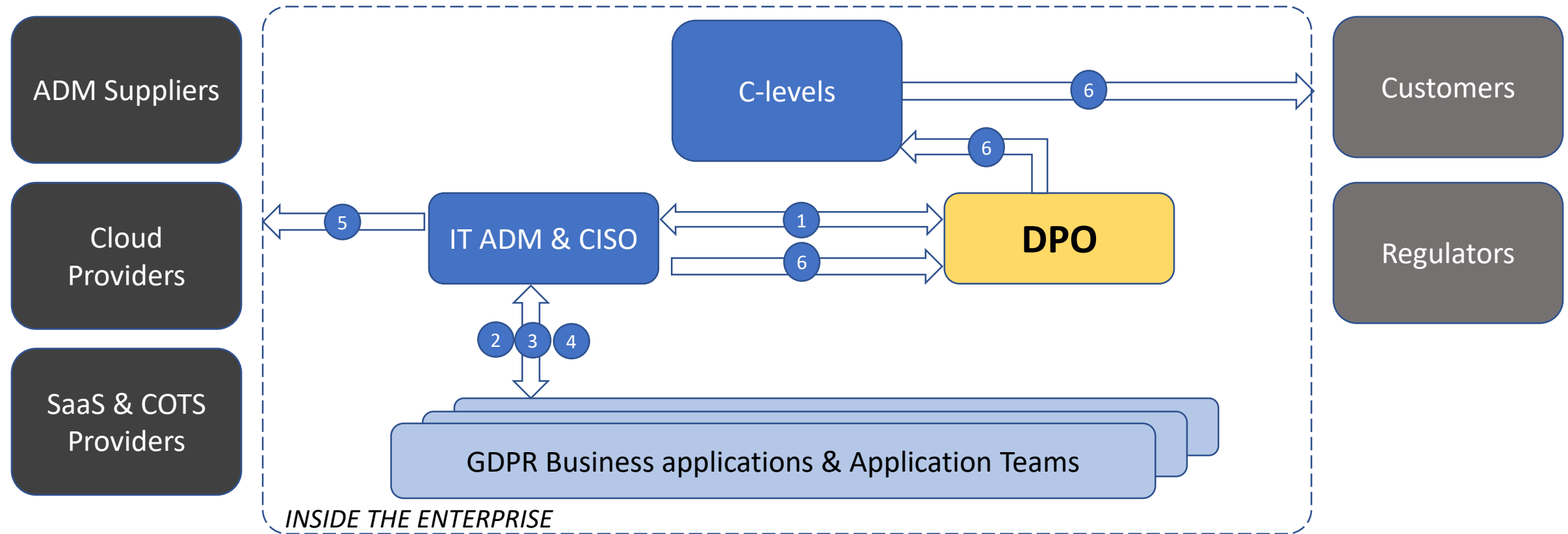
- Discover if the architecture is sustainable for Digital
- Design & track modernization strategy
- Enforce end-to-end architecture rules in Dev & Legacy Digital Transformation
- Run the GDPR Discovery and Ongoing compliance



Engineering capabilities to use for GDPR



GDPR Steps in motion and CAST fit in the IT related Topics

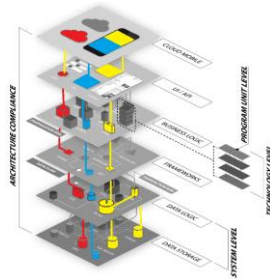


- 1 ✓ Define Private data ("GDPR Data")
- 2 ✓ Identify Applications accessing Private data ("GDPR Applications") – EA Tools like Mega
- 3 ✓ Build GDPR inventory in 2 Steps: 3.1 GDPR Data storage discovery 3.2 GDPR Data Processing discovery
- 4 ✓ Build and implement remediation plan to reach Protection by Design Processing
- 5 ✓ Drive and mitigate 3rd Party risks
- 6 ✓ Report on Protection by Design on a recurring mode with actions on deviations

CAST Key Contribution



Starting Point: CAST Software Engineering platform native Capabilities



Deep automated understanding across layers and technologies of actual data storage and data processing

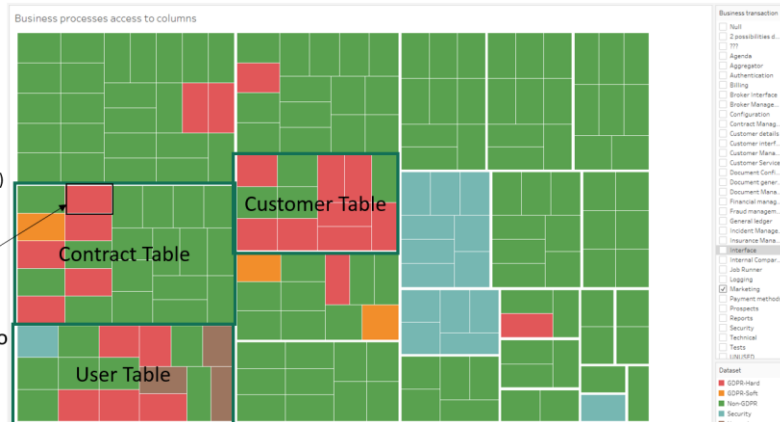
CISQ/OWASP/CWE quality rule tracing 90% of outages and advanced security flaws in the code

Ending point: GDPR Data automated inventory navigation, non-compliance and security remediation/Tracking

Questions for DPO on « Marketing » business process Data processing ?

- Business process owner
- Data processing Purpose 5.1b
- Data Minimization principle 5.1c + 25-1
- Basis for processing (article 6)
- Data conservation policy defined (17,18)
- Access rights granted to this process (5,1 b, c 25.1)
- Functional maintenance access
- Technical maintenance access
- 3rd party access
- Cross boarder access
- Portability (20)

Column with Hard GDPR Data (Click to Find Links)

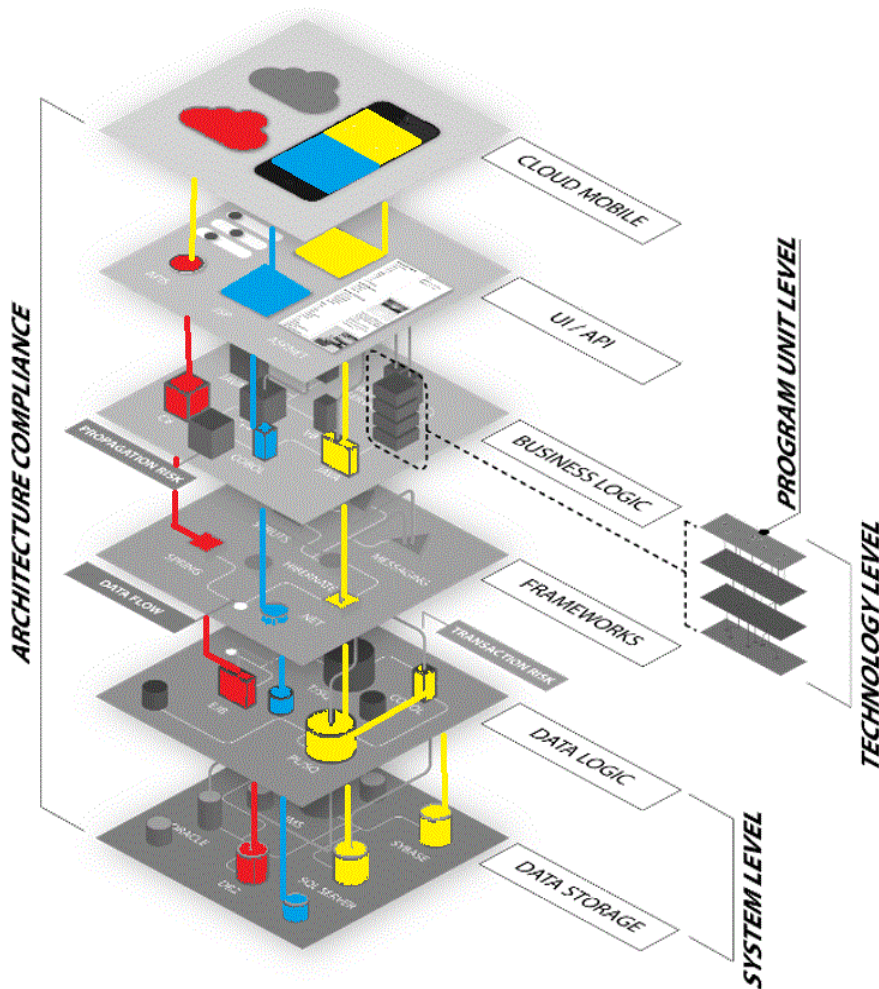


Detail of actions			0	11	added 62	
		QUALITY RULE				OBJECT NAME LOCATION
<input type="radio"/>	●●●●	added	Avoid cross-site scripting DOM vulnerabilities (CWE-79)			[C:\CASTMS\Webgoat...SiteScriptingSearchStaffDBCSS.jsp]
<input type="radio"/>	●●●●	added	Avoid cyclical calls and inheritances between packages			org.owasp.webgoat.lessons
<input type="radio"/>	●●●●	added	Avoid empty catch blocks			org.owasp.webgoat...dmin.ReportCardScreen.createContent
<input type="radio"/>	●●●●	added	Avoid empty catch blocks			org.owasp.webgoat.session.LessonTracker.load
<input type="radio"/>	●●●●	added	Avoid empty catch blocks			org.owasp.webgoat.session.LessonTracker.store
<input type="radio"/>	●●●●	added	Avoid instantiations inside loops			org.owasp.webgoat...lessons.AbstractLesson.readFromURL
<input type="radio"/>	●●●●	added	Avoid instantiations inside loops			org.owasp.webgoat...mmaryReportCardScreen.createContent
<input type="radio"/>	●●●●	added	Avoid instantiations inside loops			org.owasp.webgoat...lessons.BackDoors.addDBEntriesToEC

Initial and ongoing actionable Remediation plan:
Deduplication, Security Violations, Inappropriate data processing's to remove/modify - Ongoing

Interactive inventory: Private data & Business process Mapping navigation

✓ Unique value of cross application data path discovery



Entry point	Data Path	Access type	Persistence
MobileClick	{technical}	INSERT	UserTrack
Login	{technical}	READ	UserPassword
APIgetName	{technical}	READ	FamilyNames

This is documenting all the data flows, in an **automated fashion**.

For every identified process, the connection between data usage (automated or human) and data persistence is identified, analyzed and described.



CAST flips the inventory/action Plan to Inside-Out approach

C A S T

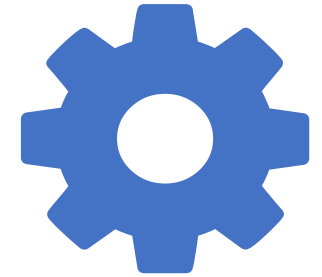


Outside In

GDPR solutions offerings rely on an “Outside-In approach” where consultants take bandwidth from internal stakeholders with “having them asking us the questions we paid them to answer in the first place”.

Inside out

Internal stakeholders need actionable and precise outcomes early enough to plan corrective and preventive actions : factoring in existing internal information sources guarantees efficacy.



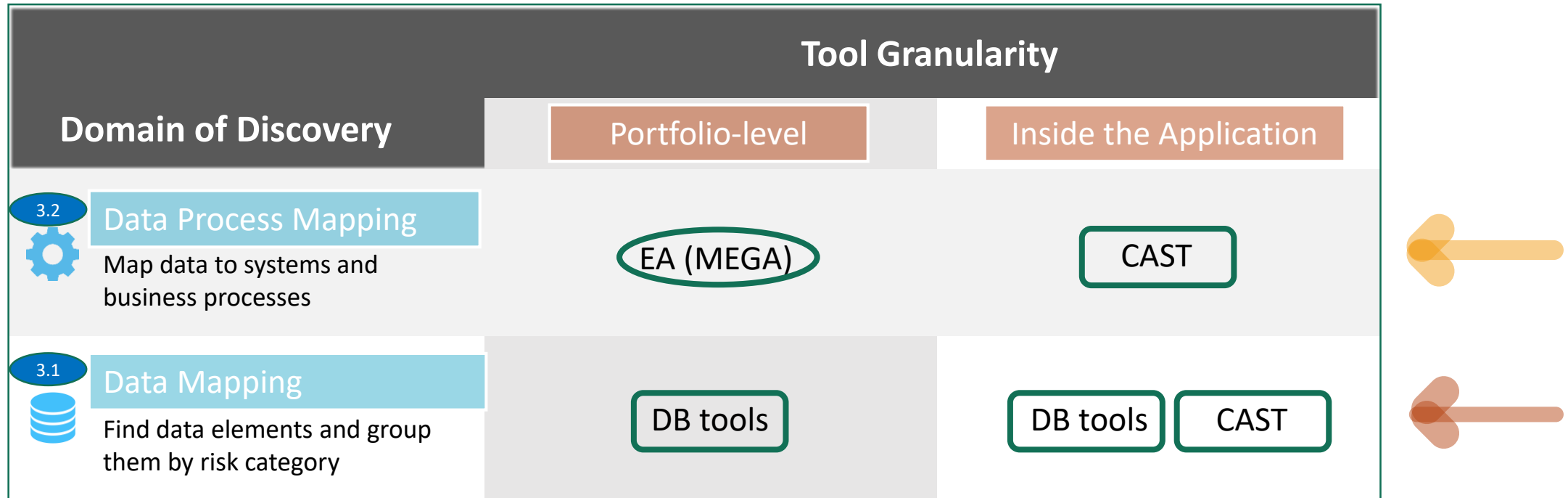
The **optimal mix** between the outside-in methodology and the inside-out on depends on:

- a) The **degree of control the organization decides to outsource to consultants**, which, in turn, depends on the risk appetite as strategically evaluated to be aligned with the business.
- b) The maturity of the organization and its capability to adopt and sustain **inside-out approach to complement and facilitate the consultants’ job**.



Tooling landscape to do the inventory & action Plan

Be it internal or externally supported, discovery work is a consulting business, aided by tools to document and discover data elements and how they are processed by systems, and then mapped to business processes



EA: including Mega, Erwin/Casewise, Planview/Troux, Software AG/Alfabet

DB: including Oracle, Informatica and specialized tools like LTI iDiscover and SAS

Manual Automated (which can leverage discovery work in ongoing compliance)



Data Protection is also a matter of Security

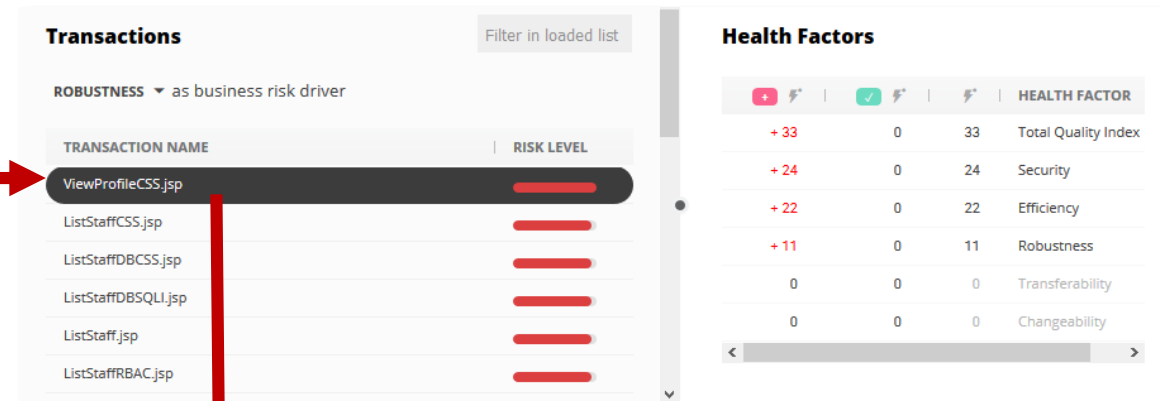
Entry point	Data Path	Access type	Persistence
MobileClick	{technical}	INSERT	UserTrack
Login	{technical}	READ	UserPassword
DoFilterProducts	{technical}	READ	Catalogue
APIgetName	{technical}	READ	Ana1_Names
CheckCredit	{...}	READ	Balance
EraseObject	{...}	DELETE	Cart
PriceQuery	{...}	READ+CALC	Catalogue
DetailCart	{...}	READ	Cart
UserAddName	{...}	INSERT	Ana1_Names

Data security in the code:

Application code reveals a great deal about the security of the processing. It is also empirically known to be heavily connected to the risk of data breaches.

Data risk drives actions:

Distinguishing application parts which are manipulating personal data from other parts enables risk focused action plans, reducing the effort to secure application code.



Risk focused data paths (transactions) report



Detail of actions

11

added 62

QUALITY RULE

OBJECT NAME LOCATION

added

Avoid cross-site scripting DOM vulnerabilities (CWE-79)

[C:\CASTMS\Webg ... SiteScripting\SearchStaffDBCSS.jsp]

added

Avoid cyclical calls and inheritances between packages

org.owasp.webgoat.lessons

added

Avoid empty catch blocks

org.owasp.webgoat.dmin.ReportCardScreen.createContent

added

Avoid empty catch blocks

org.owasp.webgoat.session.LessonTracker.load

added

Avoid empty catch blocks

org.owasp.webgoat.session.LessonTracker.store

added

Avoid instantiations inside loops

org.owasp.webgoat.lessons.AbstractLesson.readFromURL

added

Avoid instantiations inside loops

org.owasp.webgoat.mmaryReportCardScreen.createContent

added

Avoid instantiations inside loops

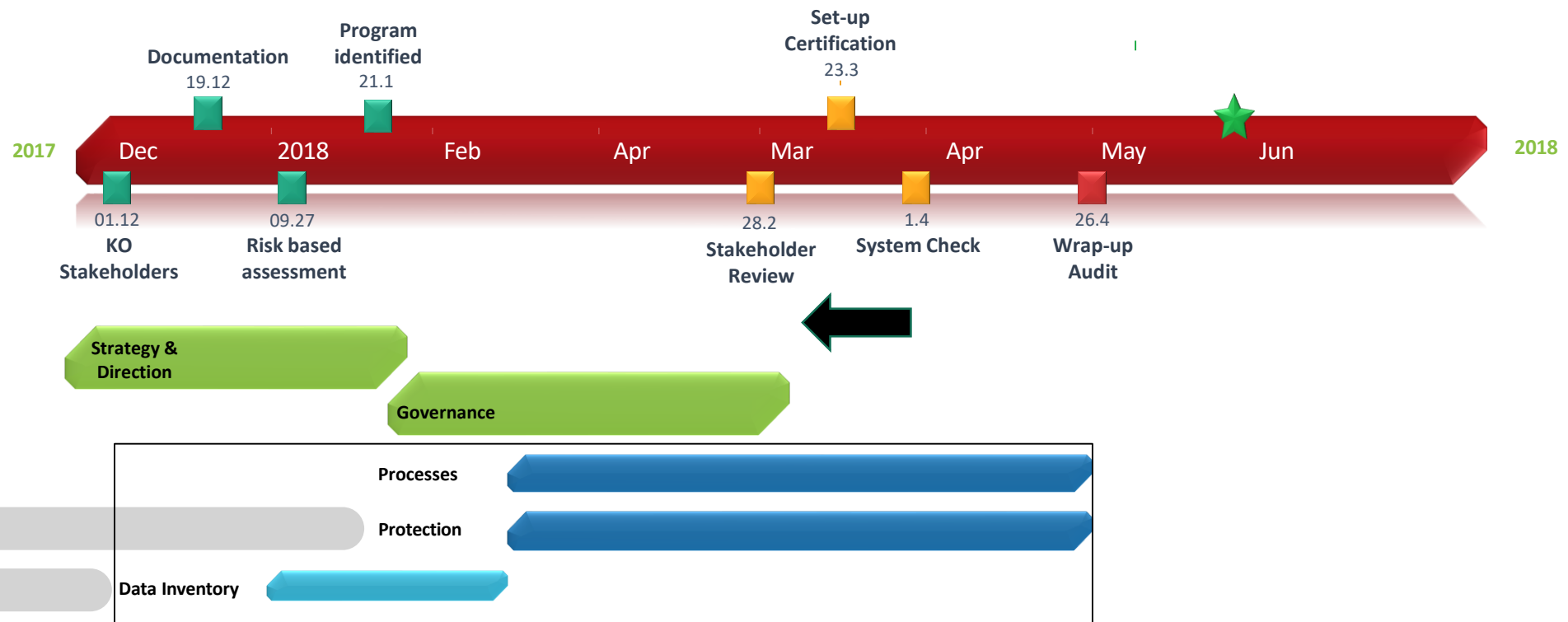
org.owasp.webgoat.lessons.BackDoors.addDBEntriesToEC

Risk focused remediation Plan






Contains: Duplications to be removed, Security Violations, Transactions to remove/modify

Typical implementation plan (illustrative)

CAST accelerates inventory population and minimizes protection efforts





Entry point	Data Path	Access type	Persistence	GDPR index
MobileClick	{technical}	INSERT	UserTrack	
Login	 {technical}	READ	UserPassword	2.0 
DoFilterProducts	{technical}	READ	Catalogue	
APIgetName	 {technical}	READ	Ana1_Names	1.5 
CheckCredit	{...}	READ	Balance	
EraseObject	{...}	DELETE	Cart	
PriceQuery	{...}	READ+CALC	Catalogue	
DetailCart	{...}	READ	Cart	
UserAddName	{...}	INSERT	Ana1_Names	4.0 

Compliance baselinining And monitoring

The initial applications snapshot is taken as the baseline, to anticipate any difference in applications evolutions:

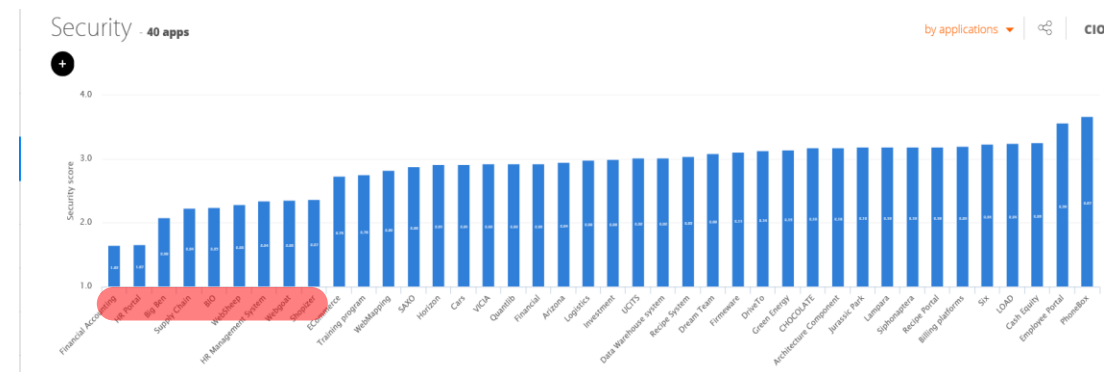
- ➕ New processing on personal data
- ➡ Modification in existing processing
- ◀▶ GDPR index level change in the relevant code

Secure the software supply chain

Applying focused security scrutiny on ADM providers' work through software SLA for GDPR lowers the risk intake from third parties.

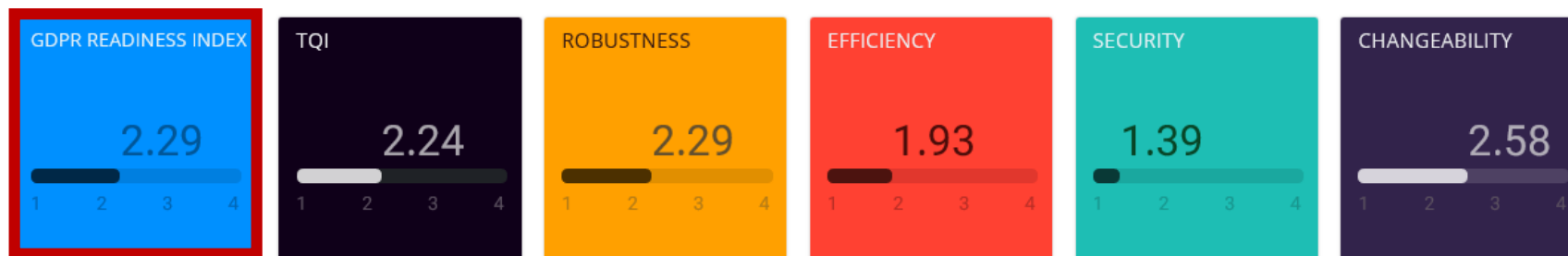
Portfolio prioritization

Applications can be quickly prioritized in order to spot weak components in the overall portfolio.



Version: 1.0 - October 27 2017 ▼

Overview



High level dashboard

DPO, CISO and Risk and Compliance executives share a single objective reference reading application data risk directly from dev, staging or production, enabling neutral discussion on priorities and actions to be taken.

Technical drill down

Drill down to technical level offers no ambiguity regarding actions to be taken. Within the GDPR Readiness Index, aggregating all findings related to personal data transactions, smart targeting can be used to further narrow the list of immediate actions.

Version: 1.0 - October 27 2017 ▼



Quality Rules

RULES	WEIGHT	% COMPLIANCE
GDPR Programming Practices - Error and Exception Handling		Average: 84%
GDPR Programming Practices - Unexpected Behavior		Average: 100%
GDPR Efficiency - Memory, Network and Disk Space Management		Average: 50%
GDPR Secure Coding - Time and State		Average: 100%
GDPR Avoid double checked locking		100%

Quality

- ✓ Increase Non-compliance tracking efficiency to actually protect private data

Cost

- ✓ Reduce IT Costs related to manual Investigation (Internal/External)
- ✓ Reduce High Licensing costs for tool that will only do the Data inventory

Speed and Scale

- ✓ Reduce the need for scarce resources being a bottleneck
- ✓ Inside-Out process in Application Clusters allowing to parallelize

- GDPR broader initiative and where CAST plays
- GDPR Automated Data Processing inventory with CAST
- **Sample outputs – Let's be concrete !**

Implementation Steps



Input: Customer to group applications into clusters accessing a consistent set of databases and to provide CAST all the code and database structure. (Clusters can be defined by Customers EA Tools like MEGA for instance)

1) Analysis by CAST of Cluster Applications Code and databases (Managed Services)

2) Workshop 1 with App teams: GDPR datasets categorization

- Client to Categorize the data from an Excel (2j) inside DPO Defined datasets
- CAST to review cluster completeness and specific calling patterns (optional)

3) Workshop 2 with App Team – GDPR datasets processing categorization

- Review GDPR datasets access and link attach them to a Business Process or for cleaning
- Client trained to be autonomous on building remediation plan for Data model, Transactions, and quality violations cleaning impacting the GDPR data
- When done the DPO can take back

4) DPO Training on leveraging the results through a data visualization interface

Tables / Columns

GDPR Datasets

Schema	Table	Columns	Data Type	Ignore	Dataset
MAINTENANCE_INT.DIVAFD.dbo	tblDailyData	DailyDate	datetime		Other
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	BlockGuid	nvarchar		Customer
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	ChannelPdfID	int		Personal
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	ChannelPdfStatusID	int		Personal
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	ContentText	text		Bank
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	ContentTypeID	int		Invoice
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	DateChanged	datetime		Invoice Data
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	DateCreated	datetime		
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	DateProcessed	datetime		
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	Extension	nvarchar		
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	ExtraInfo	nvarchar		
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	FailCount	int		
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	FailReason	nvarchar		
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	FooterType	int		
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	InsAdvisorID	int		
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	InstanceID	int		
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	IsProcessed	bit		
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	MailType	nvarchar		
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	OwnerId	int		
MAINTENANCE_INT.DIVChannel.dbo	tblChannelPdf	OwnerObjectName	nvarchar		

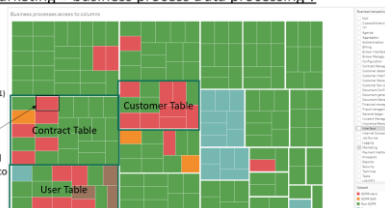
GDPR Tables / Columns

Business Processes

Table Full Name	Column Name	Default	Transaction Name	Transaction Full Name	Business transaction
SecurityTokenService.users.UserAccounts	Username	Security	Account/Reserve/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.operational.Tenants	Name	Security	Account/Reserve/Password/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	CurrentForStatusAndStatus	Security	Account/Reserve/Password/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	Email	Security	Account/Reserve/Password/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	ID	Security	Account/Reserve/Password/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	IsAccountVerified	Security	Account/Reserve/Password/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	Key	Security	Account/Reserve/Password/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.operational.Tenants	Tenant	Security	Account/Reserve/Password/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.operational.Tenants	LifeTimeCodeMinutes	Security	Account/ValidatesmsCode/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	Name	Security	Account/ValidatesmsCode/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.operational.Tenants	SmsClientID	Security	Account/ValidatesmsCode/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	Email	GDPR-hard	Account/ValidatesmsCode/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	ID	Security	Account/ValidatesmsCode/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	IsAccountVerified	Security	Account/ValidatesmsCode/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	LastUpdated	Security	Account/ValidatesmsCode/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	MobileCode	Security	Account/ValidatesmsCode/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	MobileCodeSent	Security	Account/ValidatesmsCode/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	MobileCodeSent	Security	Account/ValidatesmsCode/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	MobileCodeSentNumber	Security	Account/ValidatesmsCode/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	MobilePhoneID	GDPR-hard	Account/ValidatesmsCode/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
SecurityTokenService.users.UserAccounts	Tenant	Security	Account/ValidatesmsCode/	Authorization/IsqplLibrary/CustomerTRLSecurityTokenService/CustomerTRLSecurityAuthentication	Authentication
CustomerUID.dbo.tblInsAdvisor	ABSParticipant	Non-GDPR	ActivateBilling	CustomerTRLSNightJobs.ActivateBilling	Customer Management
CustomerUID.dbo.tblInsAdvisor	InsAdvisorID	Non-GDPR	ActivateBilling	CustomerTRLSNightJobs.ActivateBilling	Customer Management
CustomerUID.dbo.tblInsContract	CustomerID	Non-GDPR	ActivateBilling	CustomerTRLSNightJobs.ActivateBilling	Customer Management
CustomerUID.dbo.tblInsContract	DateNextPayment	Non-GDPR	ActivateBilling	CustomerTRLSNightJobs.ActivateBilling	Customer Management

Questions for DPO on « Marketing » business process Data processing ?

- Business process owner
- Data processing Purpose 5.1b
- Data Minimization principle 5.1c + 25-1
- Basis for processing (article 6)
- Data conservation policy defined (17.18)
- Access rights granted to this process (5.1 b, c + 25.1)
- Functional maintenance access
- Technical maintenance access
- 3rd party access
- Cross border access
- Portability (20)



Processing details (Transactions)



Step 1 UX – Filtered Dataset Classification visualization

- ✓ *User can Visualize Private data in the database once categorized by IT and visualize the attributes with his mouse*



✓ Step 2 UX - Used data categorized by business process

CAST

✓ Having mapped the Private data accesses to the Business processes, User can visualize which private data are Accessed by which business process

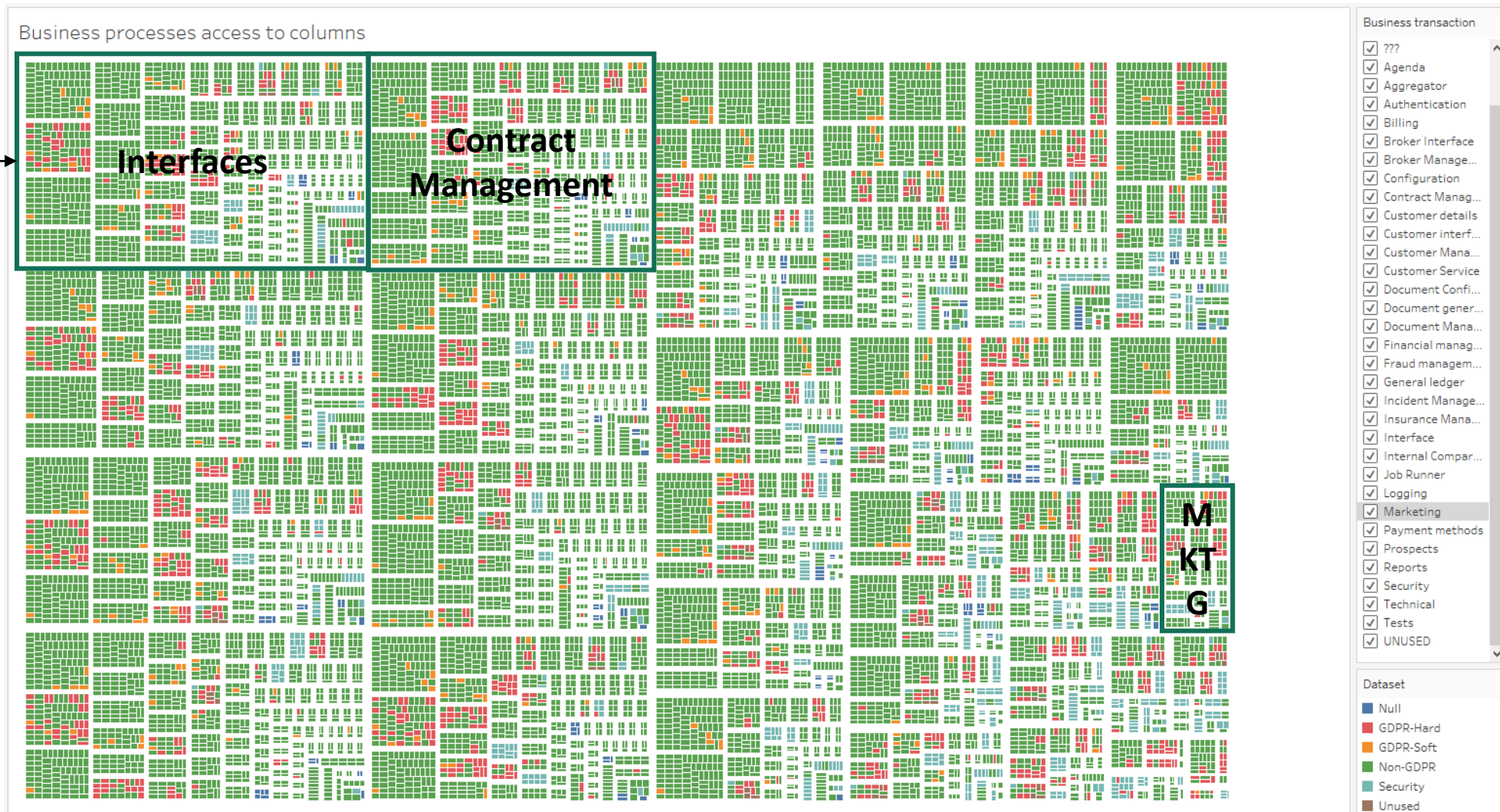
Tables/columns accessed by
A Business Process →

CAST AIP Export, list of

- 101 383 Access to the data columns
- 3639 Access to tables

Classification

- 32 main business processes



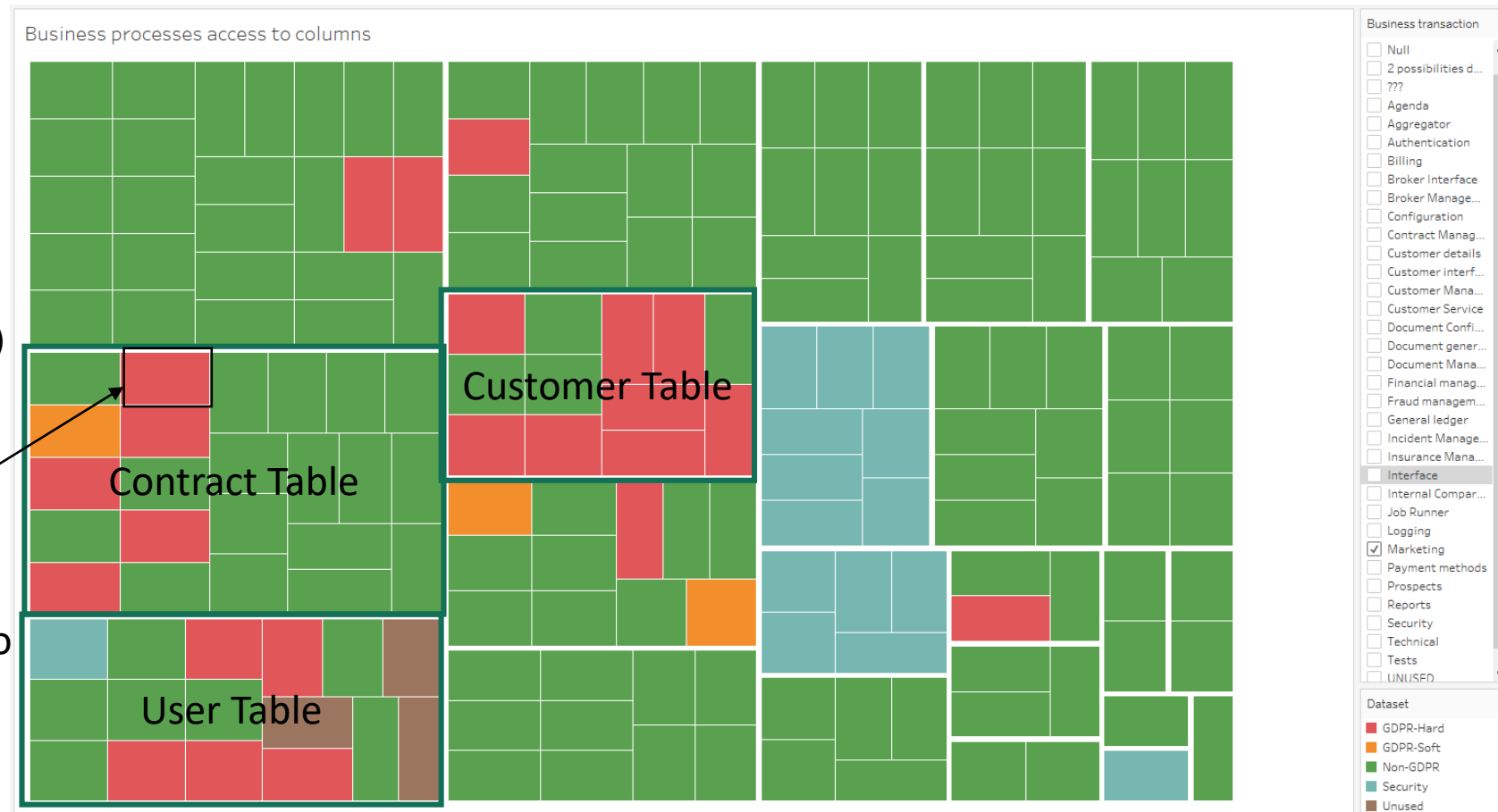
Step 3 UX – Review the GDPR Questions zooming on the Used GDPR Tables for a given Business Process and define actions

- ✓ DPO Can now ask himself what is part of the inventory V1.0 and what shall be remediated moving forward
➔ Example on the GDPR Data accessed by the Marketing Business process

Questions for DPO on « Marketing » business process Data processing ?

- Business process owner
- Data processing Purpose 5.1b
- Data Minimization principle 5.1c + 25-1
- Basis for processing (article 6)
- Data conservation policy defined (17,18)
- Access rights granted to this process (5,1 b, c 25.1)
- Functional maintenance access
- Technical maintenance access
- 3rd party access
- Cross boarder access
- Portability (20)

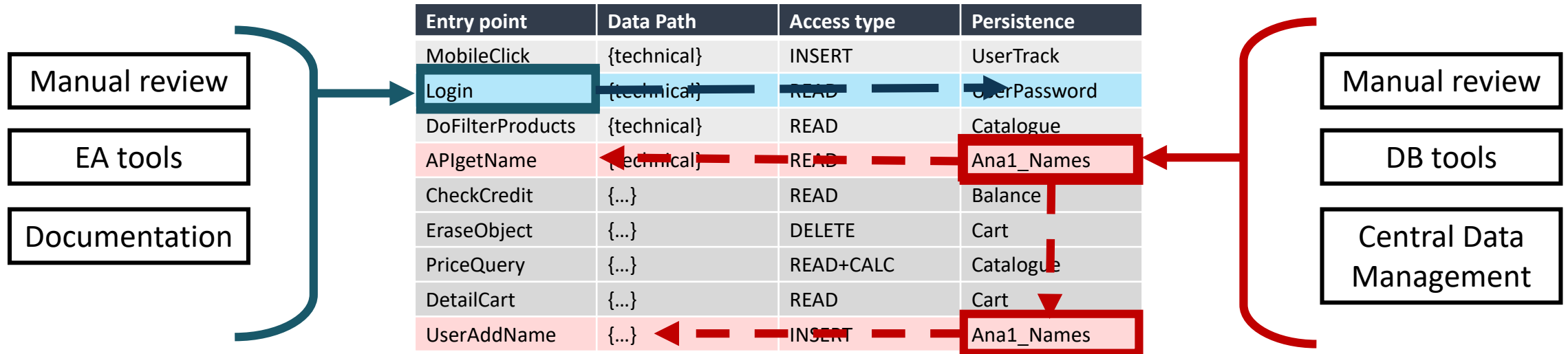
Column with Hard
GDPR Data (Click to
Find Links)





BACKUP SLIDES

Data paths inventory is a value source



Two birds with one stone:

Front end to data:

Organizations might have a rich functional expertise which can tell swiftly application interfaces manipulating personal data, letting the data discovery output map their knowledge on the physical data, whatever form it might have.

Leveraging existing information, from either side of the processings is a sure plus in as far as a complete data mapping would result.

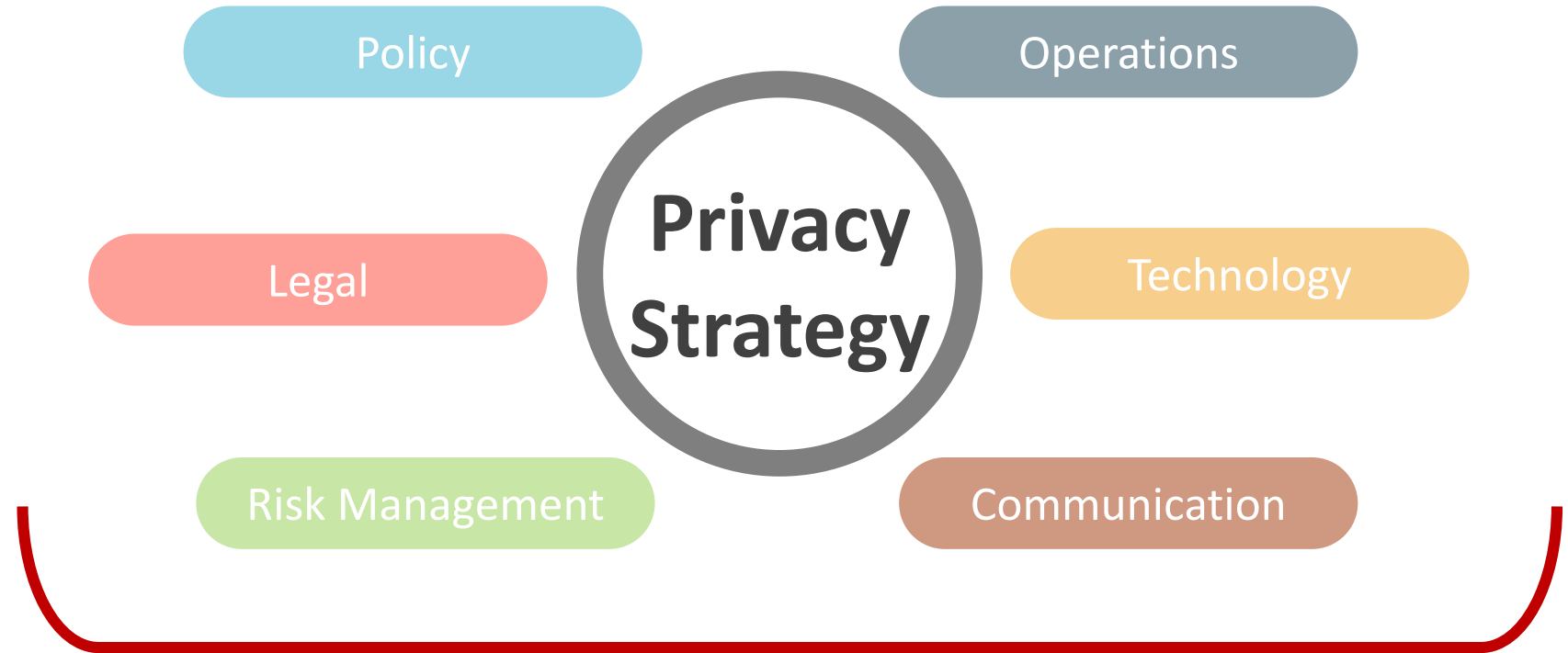
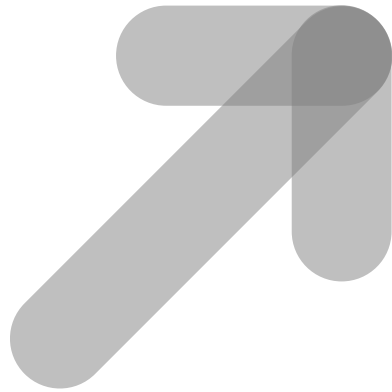
On top of this, all the code involved in manipulating personal data can be marked for security review, narrowing the scope of further analyses.

Data to front end:

Modern automatic tools can tell personal data automatically from not personal, while mature organizations might have central data management already in place. Lacking those manual review can be accelerated by smart search rules across the whole data model.

1- Direction

Strategy and a risk appetite framework shall determine the breadth of the impact



Includes, but goes well beyond the simple legal perspective.

It is the unifying direction for all different perspectives.

It is a top down decision flow, from the board through the data and process inventory, aligned with business, implemented by the privacy and security organization.

2- Governance

Accountability and awareness have to be managed by a key role: choosing the DPO with the right cross functional skills is the first key step towards maturity



Roles

Definition of management roles, functions and responsibilities.

Structure

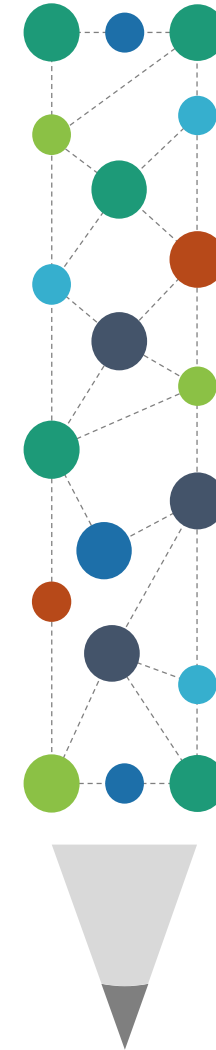
Design of the privacy organization and its communications channels.



Responsibilities

The various responsibilities across the organization have to be clarified in a DAI/RACI matrix

	Executive team	Sponsor	Process owner	Steering committee	MSB	MSO
Implement roadmap	A		R	C	I	
Identify and select projects		A	C	R	I	I
Implement projects		A	C	I	R	C
Track and monitor projects		A	I	R	C	I
Maintain operational policy	I	I	R	A	I	
Monitor overall progress	A		I	R	C	
Coach and mentor	A		I	C	R	



Adequate resources must be provided to enable DPOs to meet their GDPR obligations, and they should report directly to the highest level of management

3- Processes

Revise processes to align business to data subject rights, notification requirements, relationships with processors and data transfers



Ensure that your governance processes will make you able to demonstrate how decisions to use data for processing purposes have been reached and that relevant factors have been considered