Solution Sheet

BUTOS

Business Context

GDPR governance can be applied to meet data management challenges such as consent and right to be forgotten (GDPR §3, and §1, Article 30). – our product is supporting companies to eliminate data and records of a person highly automated!

The GDPR/DSG policies force all companies, that holding personal data of data subjects, to get to work immediately. Fines are 4% of annual global turnover or 20 Mio EUR. Unfortunately, many enterprise organizations address compliance tactically, using spreadsheets and employ lots of manual processing – but such an approach will fail for future. Regulatory compliance is hardly ever "one and done" – GDPR/DSG will change.

Organization will need to document how their implementations are working - e.g. which personal data do they have, what's the purpose, who is the owner, what are the retentions?

And most important, how is the procedure managed, controlled and documented to delete records.

- ✓ Centralized orchestration
- ✓ Automated approach
- ✓ Dynamic adaption
- ✓ Flexible transaction sequences
- ✓ Data quality checks
- ✓ Workflows and lifecycle management

About Butos:
Provides compliance and process consulting, out of the box business solutions and implementation services based on requirements of international enterprises.

Partner of Tibco:
Leading provider of analytical and data management tools since years (rated by Gartner).

Release Reference: smart.GDPR-R1.0.x
April 2018 – Butos AG ©

Solution Vision

smart.GDPR

Centralized compliance orchestration with smartGDPR is designed to solve all this in a complex enterprise environment highly efficient and guarantees to be GDPR/DSG compliant with 100% traceability. But not only that, the use of the smart.Engine also allows adjustments by configuration at any time, which are also logged.

With the smart.GDPR module all major requirements of the GDPR law, such us

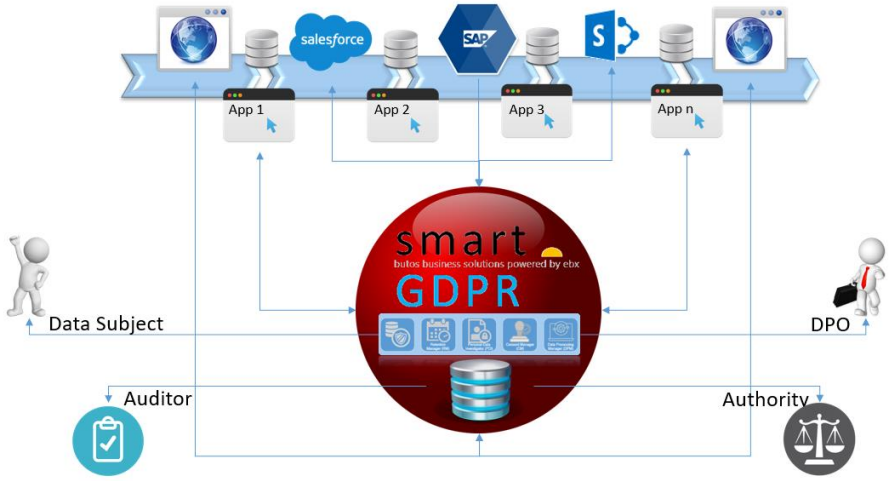
- Consent Management - Art 6&7
- Right of access – Art. 15
- Right to be forgotten – Art 17
- Report processing activities – Art. 30
- Data breach reporting – Art. 33

can be implemented by using the GDPR components:

- Personal Data Investigator (PDI: RfI, RfR, RfD, RfiD)
- Retention Manager (RM),
- Data Processing Manager (DPM)
- Consent Manager (CM)
- Data Breach Investigator (DBI).

Together with the reference data of the GDPR accelerator smart.GDPR is a holistic solution that fulfils GDPR and DSG audits in best matter.

Solution Architecture



Component Set*

Personal Data Investigator (PDI) – Right of access	
▪ Request for Information (PDI.RfI process)	The request of a data subject must be answered within 30 days. An order will be created, and a workflow initiated. All personal data of a data subject stored in any system of the company are gathered and listed transparently by configured transaction sequence. With a configurable template the data is processed into csv file or PDF and sent via letter or can be made available via client portal. Optional: Word integration with smart Office. Order will be closed. Dashboard KPI's are generated: Amount of RfI request (total, new, identified, retrieved, documented, delivered) and duration of RfI workflow (average, min, max).

Component Set*

Personal Data Investigator (PDI) – Right of access	
▪ Rectification request (PDI.RfR process)	Requires the data subject a correction of its data, the rectification request must be done within 30 days and an appropriate confirmation of the changes must be sent back. Order will be processed via initiation of a workflow. Rectifications will be protocolled and then confirmed to the data subject.
▪ Data portability request (PDI.RfD process)	At any time, a data subject can ask for the delivery of its data in a digital readable format, such as XML, CSV or XLS. Order will be processed via initiation of a workflow. Data gathering process is similar to the RfI process, but data will be delivered digital encoded.
▪ Request for deletion (PDI.RfiD process)	Data subject can ask for individual deletion of data, if there is no consent or data subject revokes consent. Individual delete order will be created, and workflow initiated. Of course, any legal retention period must be considered. Confirmation of deletion will be sent to data subject and workflow can be closed. Two dashboard KPI's are generated: Amount of individual deletion request (total, closed, in progress, new) and duration of RfID workflow (min, max, average).

Retention Manager – Right to be forgotten	
▪ Report delete candidates	Application can report delete candidates (active or inactive). Inactive means the retention period has not yet been expired and delete process has to be postponed. As soon a retention period has been expired, the deletion candidate is active for veto / hold check and then for the deletion process.
▪ Calculate retention period	Retention period will be calculated by the amount of years defined by the retention class.
▪ Check veto / legal hold	By configuration dependent applications of a business object will be checked, if there is any veto or hold against a deletion.
▪ Check delete lock	Check, if there any locks on level business object, application or business risk reasons, that avoid a deletion

Retention Manager (RM) – Right to be forgotten	
▪ Delete by sequence	Different dependencies and references between business objects and applications can be configured in the transaction sequence. The delete sequence can be sequential or parallel. Different deletion types can be processed: ▪ delete foreign key ▪ anonymize foreign key ▪ delete master object
▪ Data Anonymization	For reference or statistic reason (Data Ware House or Data Lake) data cannot be deleted but must be anonymized. Appropriate orders will be managed by the RM module.
▪ Delete summary	Pseudo master application can report deletion summaries. E.g. the payment transfer reports, that 50'000 records have been deleted. System will archive such kind of reports for audit reasons.
▪ Escalations	Based on responsibilities and roles, several escalation levels can be configured, and email messages will be sent, if appropriate business rule expires.
▪ Volume Queueing	Based on initial work load or peak load due to contract periods a massive amount of delete candidates will be delivered. Therefore, the system can be configured with thresholds based on applications and business object. This allows the data administrator to balance the daily throughput of business objects.
▪ Threshold limits	To avoid errors and detect discrepancies, min and max volumes can be set by business object and application. Is there a behavior outside this range, the systems starts an escalation and stops deletion for this business object.
▪ General Configuration	Additionally, to the veto/hold sequence the deletion sequence can be configured. Escalation levels can be configured as well as Key Types to identify Business objects.

Data Processing Manager (DPM) – Reporting processing activities	
▪ Check interface definitions	Check the meta data of the interface definitions (based on the EAR DB model), if any attributes are used with privacy or sensitive definition of data subjects. If so, workflows for data stewards will be initiated to generate entries in the data processing report table.
▪ Report data processing with privacy data	Application and data stewards can report data processing activities with privacy data via Web Services or Workflow. Reports and KPIs will be generated, periodically. Thresholds will be checked and reported to the data breach investigation module (DBI).
▪ Dashboard	The following default KPI's will be reported: ▪ Number of interfaces with privacy data ▪ Amount of records processed by each application ▪ Total amount of records processed by month

Component Set*

Consent Manager (CM) – Consent Management	
▪ Register consent	Applications or departments getting a consent, consent reject, advertisement barrier or other restrictions of a business object (client or partners), can send the appropriate transaction: ▪ Register consent, ▪ Reject consent, ▪ Register adv-barrier to the smart.Engine via Web Service, File or manually entry with a workflow. The consent for the business object and application (usage) will be notified with the appropriate business object reference.
▪ Check consent	With a query request transaction: ▪ Consent-Query and Key: BO-ID an application can ask the GDPR/DSG platform about consent and restriction entries to any appropriate business objects. Pre-Requisite: Applications with consent transactions have been registered in advance using the possibilities of the application registration manager. Allowed consent transactions can be configured individually

Data Breach Investigator (DBI) – Data breach reporting	
▪ Define thresholds	Application, product and data owner are allowed to define thresholds (min/max) of interfaces to control and monitor processes.
▪ Control thresholds	Entries produced by the data processing manager (DPM) will be controlled, if the amount of records processed is within the min and max threshold.
▪ Start Investigation	If amount of processed records is out of the threshold range (min, max), an escalation workflow will be initiated immediately to the stakeholders (to be configured).
▪ Dashboard	The following default KPI's will be reported: ▪ Number of processed interfaces in total by month ▪ Number of interfaces out of range ▪ Number of escalation workflows (initiated, in progress, closed)

*More details and feature list will be found in the Component Sheets of the modules

Roles & Permissions (customization by client needs)

Role		C	R	U	D	A	M	P	WF[2]
Business User		-	x	-	-	-	-	-	-
Data Owner		x	x	x	x	x	-	-	-
Product Owner		-	-	-	-	x	-	-	-
Data Steward		x[1]	x	x[1]	-	-	-	-	-
Data Admin		x	x	x	x	-	-	x	x
System Admin		x	x	x	x	x	x	x	x

C=create, R=read, U=update, D=delete, A=approve, M=monitor, P=permission

[1] needs approval of Data Owner

[2] Workflow configurations

Solution Roadmap (next releases)

- Configuration of messaging approach (push/pull)
- Configuration and calculation of retention
- smart.PDI.RfR, smart.PDI.RfD, smart.PDI.RfiD, smart.CM, smart.DBI, smart.DPM
- smart.Outsourcing
- smart.Office and smart.eDOC integration
- Usage of smart.Engine features
- KPI workflow duration (min, max), Threshold management