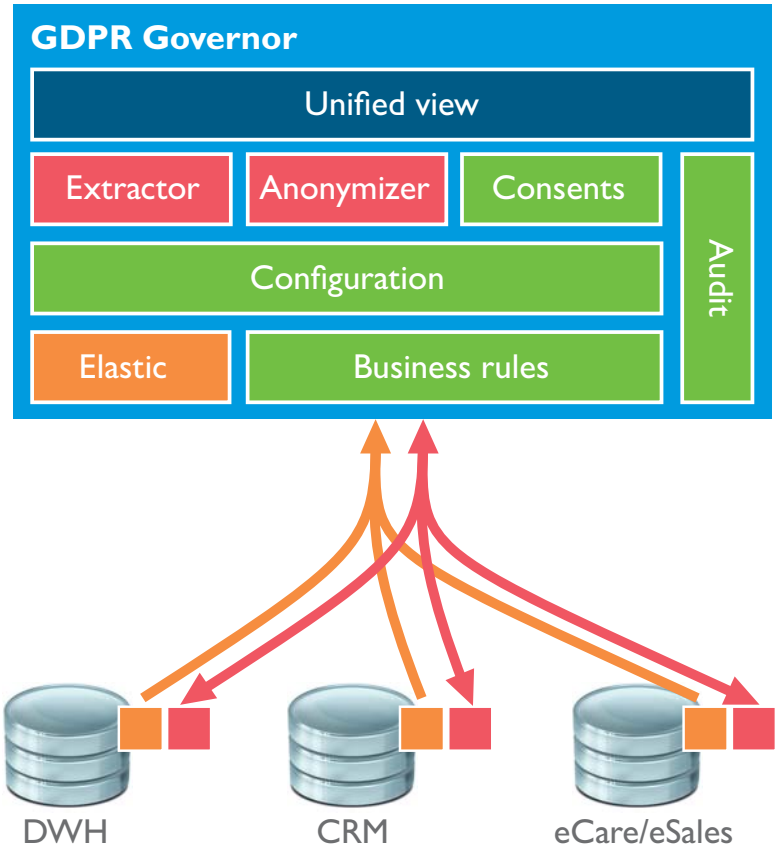
Ness Technologies

# GDPR Governor

## GDPR Governor is a single tool to fulfil GDPR requirements for

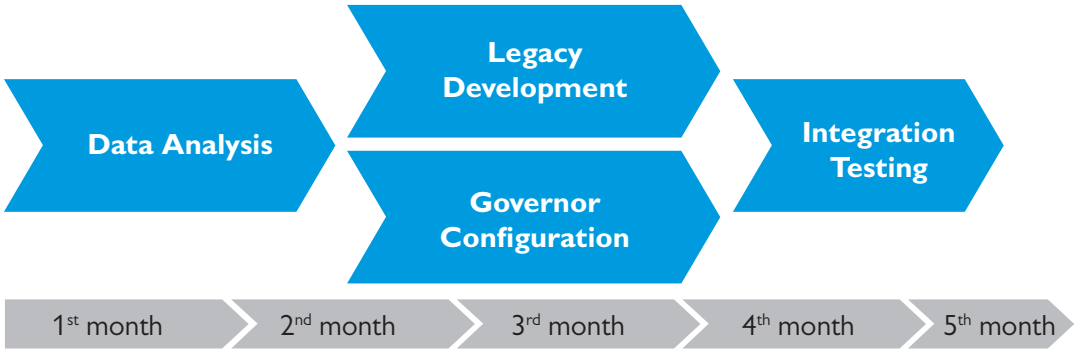
- Single view of the stored customer data within your existing systems
- Reporting personal data of your customers
- Managing their consents
- Anonymizing their personal data
- Personal data access audit




## Benefits

- Lowers costs and time to delivery by 30% on average to comply with GDPR
- Comes with a template for easier GDPR related data identification and analysis
- Can be implemented in stages
- Proven, centralized solution with support
- Additional benefits:
  - Automated suspicious access identification based on audit
  - Provides unified view of Customer GDPR data (can be extended to non-GDPR data in the future)

# Road to GDPR Governor




Correct time schedule is an essential part of the GDPR implementation as GDPR must be fully implemented by 25th May 2018.

GDPR Governor is designed to shorten time to market for GDPR compliancy by helping during all three phases (analysis, implementation, testing).

**Crucial part is an analysis** of your current data in the existing system. This part must be carried out with any approach taken to comply with GDPR. Governor comes with predefined templates/questionnaires to simplify this task.

**The implementation consist of two tasks which shall be running in parallel**

- Implementation of GDPR Governor Connector in your legacy systems to expose data from you legacy systems and to anonymize them when Governor demands anonymization
- GDPR Governor core is already implemented, only the configuration to support your legacy system data structure and your business rules needs to be done.

**Governor core is already tested**, so integration testing shall verify that development in legacy system and Governor configuration work as designed together.

Average GDPR project takes 4–5 months (1 ½–3 for analysis, 1 ½–2 for legacy implementation, 1 for integration testing). However, it greatly depends on the number of legacy systems and complexity of their data structures.

# GDPR Governor

## Analysis

- **Analyse current systems and their sensitive data**

  We can analyse your systems for you. If you want to do it by yourself or with your current system vendors, Ness shall provide you with a questionnaire to simplify identification of such systems and data.

  Ness provides consultancy of legal aspects of GDPR in cooperation with an established privacy lawyer.

- **Analyse the status of audit of access to GDPR sensitive data**

  We can provide you with the best practices of how to audit access to sensitive data in different systems.

- **Reduce duplicities and remove unused sensitive data**

  Avoid of storing sensitive data you don't need anymore and deduplicate sensitive data for you system to reduce both the implementation and operation costs of GDPR.

- **Identify which sensitive data shall be kept**

  Identify the systems which are GDPR related when all duplicities and unused data are removed. Identify master systems and interconnections among sensitive data across the systems.

## Implementation

### Legacy

- Implement GDPR Connector in legacy systems

  Each GDPR needs to implement predefined connectors for GDPR Governor to support GDPR Governor processes. We expect the modification of your current systems is carried out by you or your current vendors. We can offer consultations to smoothen the process.

### GDPR Governor

- Configure and deploy GDPR Governor

  This task is performed by Ness based on the information gathered in previous phases. It runs in parallel with implementation in legacy systems.

## Testing

GDPR Governor is already a finished and tested product so the goal of integration testing is to verify that Governor configuration is aligned with legacy connector implementation.

# GDPR Governor

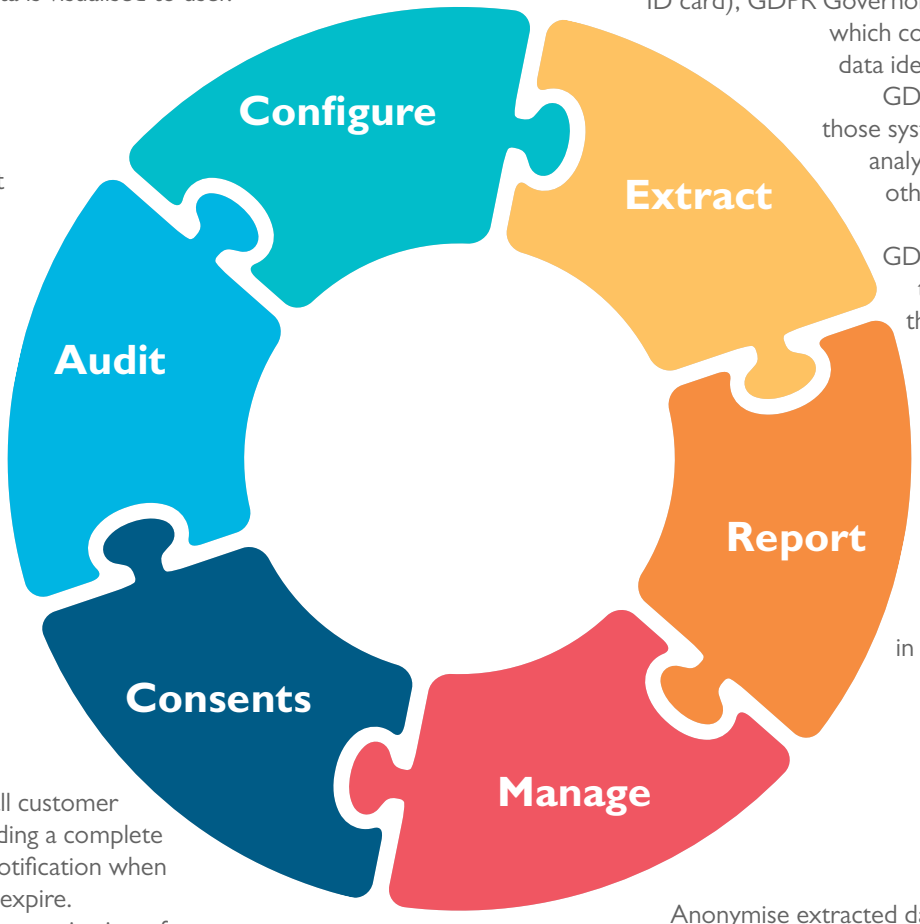
GDPR Governor has a configuration which data are stored in which system and how are data sets identified within the system (e.g. birth number). Data are categorised and configuration is aware of the interconnections among data in other systems. It stores link between consents and data sets in multiple systems.

It also contains data retention policy and configuration how the extracted data is visualised to user.

Your existing systems are required to implement GDPR data connector. A unified API for all legacy systems to gather personal data from the existing system.

**Extract** › **Categorize** › **Analyse**

Based on the entered search criteria (e.g. birth number, ID card), GDPR Governor identifies all systems which could contain customer data identified by the criteria. GDPR Governor queries those systems, categorizes and analyses the results to find other systems containing interconnected data. GDPR Governor queries those systems until all the data are extracted.




View and search audit logs with a powerful Elasticsearch tool. Automated detection of suspicious access to sensitive data.

The access to GDPR Governor itself is audited.

GDPR Governor gathers data from various systems in a single configurable structured UI. Export in the machine readable format (XML/JSON) is supported.

Stores and manages all customer GDPR consents including a complete history. Automated notification when a consent is about to expire. Triggers automated anonymization of data as soon as consent is expired or invalidated.

Anonymise extracted data, anonymise whole entities in systems together with consents, automated anonymization when consent is expired or invalidated. Automated anonymization is driven by business rules (e.g. customers can anonymize only certain data, data are automatically anonymized when there is no valid consent connected to data, etc.).

2017 – 05.01

**NESS Czech s.r.o.** | V Parku 2335/20, 148 00 Praha, Czech Republic | tel.: +420 244 026 400 | e-mail: nesscz@ness.com | www.nesstech.com