OBSERVAR
focus on success

European General Data Protection Regulation (GDPR)

OBSERVAR – the modular eGRC* Suite to achieve privacy compliance

*(*enterprise Governance, Risk and Compliance)*

© Observar AG, Lindenstrasse 10, CH-6340 Baar / Zug, www.observar.ch

OBSERVAR
focus on success

Agenda GDPR

© Observar AG, Lindenstrasse 10, CH-6340 Baar / Zug, www.observar.ch

OBSERVAR
focus on success

Why is GDPR relevant for you

You are a company which…

1

- offers goods or services to individuals in the EU
- or monitors their behaviour within the EU
- and processes and/or stores personal data of employees or customers

…GDPR requires from you

2

✓ Accountability
- evidence that GDPR privacy rules effective 25 May 2018 are complied with

✗ If not, fines can be levied
- up to 4% of Group sales

3

OBSERVAR – Simplify your work

- Web-based solution supports you with work-flows as well as automatic reminder, alert and change request messages, plus provides evidence that GDPR privacy rules are complied with

© Observar AG, Lindenstrasse 10, CH-6340 Baar / Zug, www.observar.ch

OBSERVAR
focus on success

What is new for you

One single GDPR legal framework within the European Union brings…

More obligations for companies

- Accountability, Evidence showing compliance with privacy rules
- Data breach notification to supervisory authorities within 72h
- Data protection impact assessment (DPIA) for ‘risky’ processing activities
- Inventory of personal datapools and record of processing activities

More rights to data subjects

- Explicit consent required to process personal data, no ‚bundling‘
- Right of information and access
- Rights to object, rectify and erasure
- Right of portability and restriction of processing

© Observar AG, Lindenstrasse 10, CH-6340 Baar / Zug, www.observar.ch

OBSERVAR
focus on success

How to achieve GDPR privacy compliance

Steps to succeed:

0	**Basic settings**	…Corporate legal & management structure, currencies, users, control catalogues, notification settings, Web-solution with LDAP for MSSQL database
1	**Data inventory**	…list all personal data pools with description of purpose, processing activities, responsibilities, location etc.
2	**Risk identification & -assessment**	…classification for each data pool& processing activities, description of level of controls
3	**Controls to ensure compliance**	…for risk management purposes select controls, define work-flows to be able to document level of ‘ Soll’ and ‘ Ist’ in GDPR compliance
4	**Confirmations as evidence for compliance**	…as evidence for executed controls, incl. reporting of discrepancy messages(self-assessment with integrated audit function)

© Observar AG, Lindenstrasse 10, CH-6340 Baar / Zug, www.observar.ch

OBSERVAR
focus on success

How can OBSERVAR support you

….with its modular eGRC Suite

0 Basic settings	**MASTER module**	▪ Corporate legal & management structure, currency, users ▪ Control catalogue to ensure compliance, notification settings ▪ WEB-solution with LDAP for MSSQL database
1 Data inventory **2 Risk identification and assessment**	**Data Inventory module**	▪ Capturing personal datapools, processing activities, location & responsibilities ▪ Risk identification and assessment through questionnaires and rating system ▪ Special attention required for ‘risky’ processing activities (DPIA)
3 Controls to ensure compliance **4 Confirmations as evidence for compliance**	**GDPR Compliance module**	▪ Risk management by selecting relevant controls from control catalogue (180), Implementation through design of work-flows with assignment of repsonsibilities and selection of periodicality ▪ Reminder- and execution messages, gap analysis, as evidence of data privacy compliance

© Observar AG, Lindenstrasse 10, CH-6340 Baar / Zug, www.observar.ch

OBSERVAR
focus on success

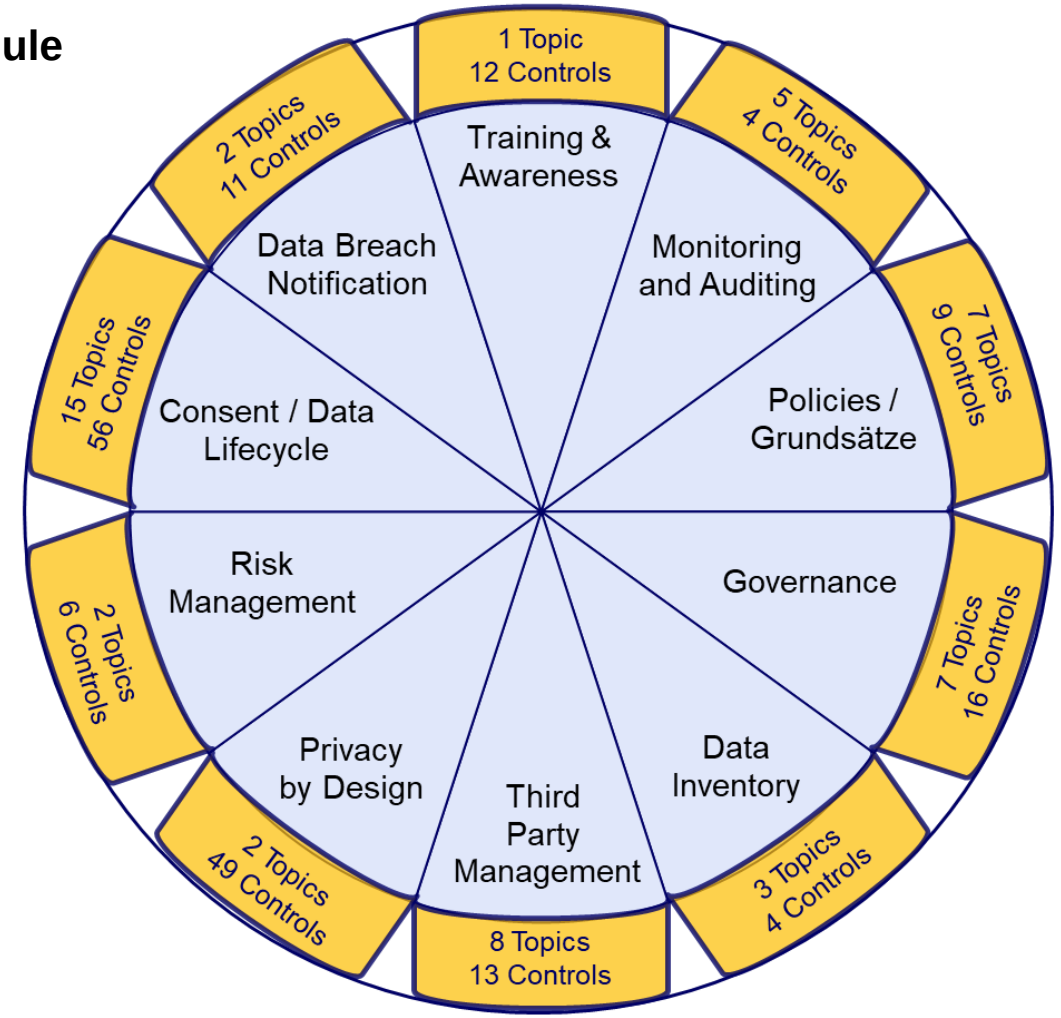
3 Compliance-Massnahmen
4 Bestätigungen als Nachweis
GDPR Compliance Modul

in detail(I/II) –

Based on GDPR Compliance module

Control catalogue with

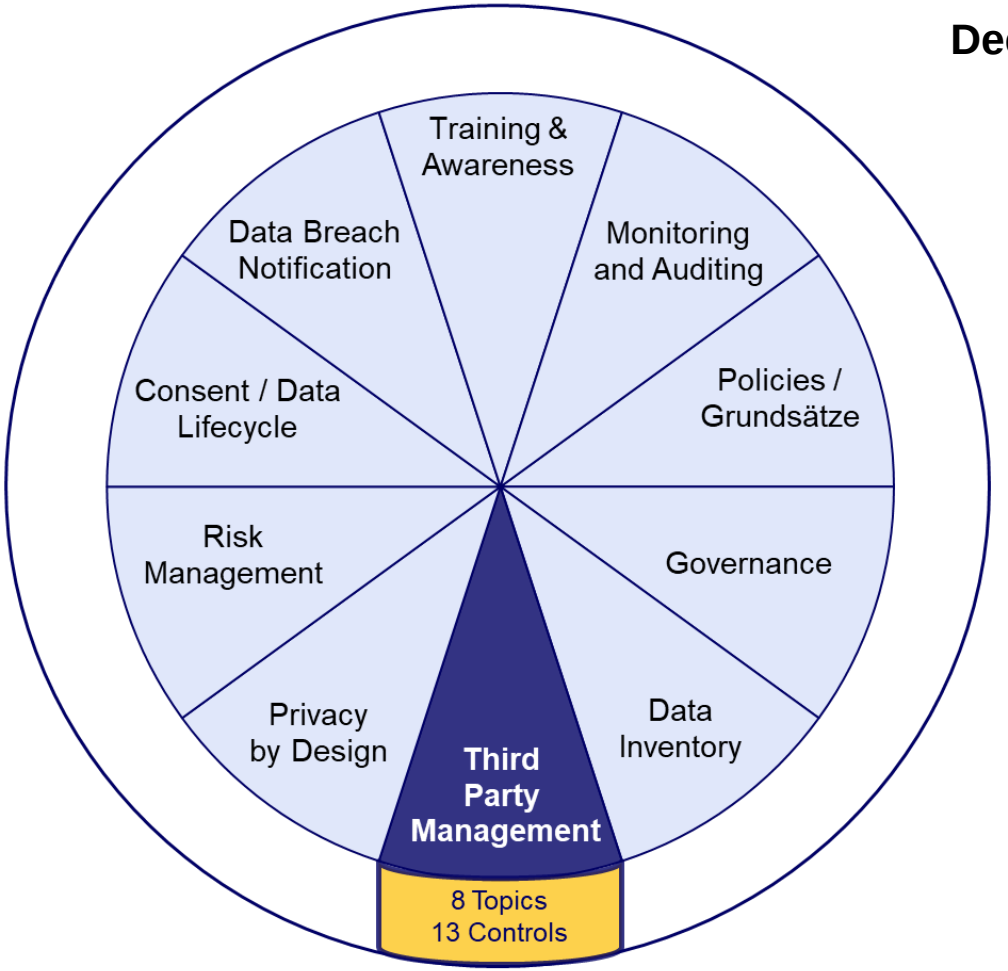
- 10 categories
- 52 topics (GDPR articles related)
- 180 relevant controls (assigned to GDPR articles)



© Observar AG, Lindenstrasse 10, CH-6340 Baar / Zug, www.observar.ch

OBSERVAR
focus on success

in detail(II/II) –



Deep Dive – «Third Party Management»

GDPR article	8 topics (articles) with 13 relevant controls
28	Processor
29	Processing under the authority of the controller or processor
44	General principle for transfers
45	Transfers on the basis of an adequacy decision
46	Transfers subject to appropriate safeguards
47	Binding corporate rules
48	Transfers or disclosures not authorised by Union law
49	Derogations for specific situations

© Observar AG, Lindenstrasse 10, CH-6340 Baar / Zug, www.observar.ch

OBSERVAR
focus on success

More to consider for GDPR privacy compliance

Steps to comply with more legal requirements…

5	**Data Protection Impact Assessment**	…mandatory after identifying ‘risky’ processing activities
6	**Data Breach Notification**	…mandatory to notify Supervisory Authorities within 72h after detection

…with the help of OBSERVAR eGRC modules

5 Data Protection Impact Assessment	**Data Protection Impact Assessment (DPIA) module**	▪ As a consequence of identiffying ‘risky’ processing activities ▪ Going forward – mandatory for changes in processing activities ▪ Notification to Supervisory Authoritiies in case of ‘high risk’
6 Data Breach Notification	**Data Breach Notification module**	▪ Capturing of data breaches with alarm message to data protection officer,.ensures tracking & documentation to Supervisory Authorities ▪ Capturing of measures to remedy and for ‘follow-up’ purposes

© Observar AG, Lindenstrasse 10, CH-6340 Baar / Zug, www.observar.ch

OBSERVAR
focus on success

What makes OBSERVAR solution for GDPR unique

MASTER module

Data Inventory module

GDPR Compliance module

Data Protection Impact Assessment (DPIA) module

Data Breach Notification module

Benefits of a modular eGRC-WEB-based solution

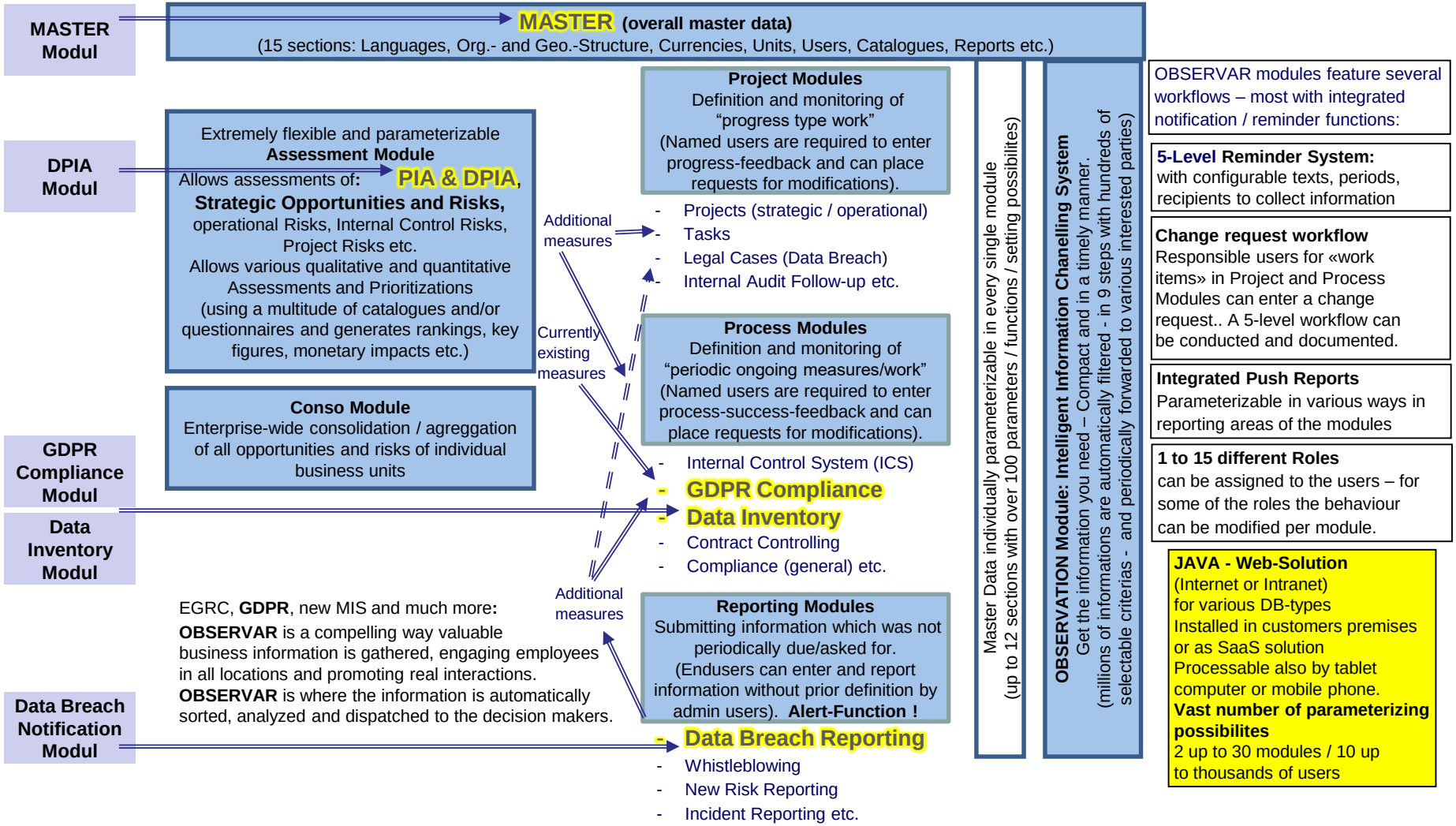
- Dynamic with integrated change management (no static excel or word files)
- For each client need customisable
- Minimal time required to install
- Skalable in terms of numbers of users & modules
- Minimal training required for users
- Integrated compliance awareness
- Evidene of compliance via a system solution, documents notifications and action
- Integrated audit trail

© Observar AG, Lindenstrasse 10, CH-6340 Baar / Zug, www.observar.ch

*technical/ process oriented outline

OBSERVAR
focus on success

Outline* eGRC-WEB-based solution



© Observar AG, Lindenstrasse 10, CH-6340 Baar / Zug, www.observar.ch

OBSERVAR
focus on success

your OBSERVAR partner

Hermann Bissig

Professional skills

Swiss Certified Public Accountant
Data Protection Officer

Email: hermann.bissig@observar.ch
Cell phone: + 41 (0)79 757 48 11

© Observar AG, Lindenstrasse 10, CH-6340 Baar / Zug, www.observar.ch