The General Data Protection Regulation (Regulation 2016/679 – GDPR)

Rokas
International Law Firm

7th AIDA Europe Conference, Warsaw, Poland, 12 & 13 April 2018
"De-Mystifying InsurTech: a Legal and Regulatory View"

1. Introduction

Rokas
International Law Firm

➢Police Directive (2016/680) => with transposition deadline on

6 May 2018

ONE CONTINENT – ONE (?) LAW

➢Aims at unified law and uniform interpretation and implementation

BUT

➢Many derogations in favor of national laws

(EXTRA-)TERRITORIAL SCOPE

- Processing by establishments within the EU; **AND**
- Processing by establishments outside the EU, **IF** related to:
  - the offering of goods or services to data subjects in the EU; or
  - the monitoring of their behaviour takes place within the EU.

The GDPR does not come alone:

Hard law:

✓The Police Directive (Directive (EU) 2016/680)

✓NIS Directive (Directive (EU) 2016/1148) with transposition date **9 May 2018**

✓Proposal for Regulation on Privacy and Electronic Communications (ePrivacy Regulation)

✓EU Commission's Decisions

✓National implementing laws & regulation

Soft law:

✓Working Party 29 Guidelines/ Opinions/Recommendations

✓National Authorities guidance

✓Case-law

✓Precedent under the Data Protection Directive (95/46/EC)

2. Main points of focus

Rokas
International Law Firm

LEGITIMATE PROCESSING

Legal basis:

✓Data subject's consent

✓Performance of a contract / Preparation of a contract

✓Controller's legal obligation

✓Data subject's or third party's vital interest

✓Task carried out in the public interest/ in the exercise of public authority

✓Legitimate interest pursued by the controller

General principles:

✓Lawfulness and fairness

✓Transparency

✓Purpose limitation

✓Data minimization

✓Accuracy

✓Storage limitation

✓Integrity and confidentiality

✓Accountability

DATA CONTROLLER'S OBLIGATIONS

Processing activity

✓Safety measures

✓Technical & Organisational measures

✓Privacy by design & by default

✓Data breach notification

✓Data transfers

✓Cooperation with National Authority

Internal organisation

✓Privacy & Data Protection Policy

✓Data Protection Officer (DPO)

✓Data Protection Impact Assessment (DPIA)

✓Records of Processing Activities

✓Procedures in case of exercise of data subjects' rights

✓Procedures in the even of data breach

Relation with data processor

✓Contract or other legal act with minimum content

✓Processing on documented instructions of the controller

✓Limitations on sub-processors

✓Administrative liability on the controller

✓Civil liability to compensation

Accountability is a core new principle of the GDPR, meaning that the data controller shall

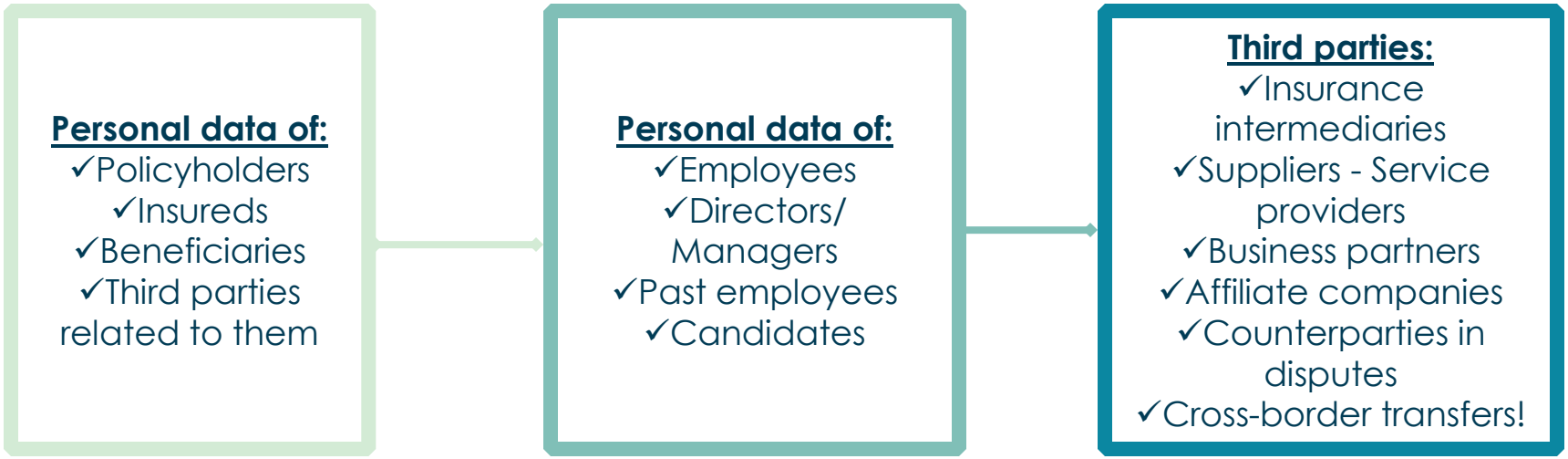
- be responsible for, and
- be able to prove

compliance with all GDPR requirements.

3. GDPR and Insurance

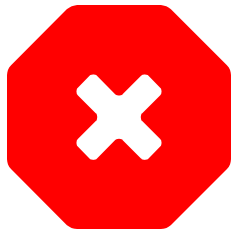
Rokas
International Law Firm

The insurance company's activity entails numerous data processing aspects:



The GDPR affects the insurance company's operations and internal organisation.

FREQUENT (INDICATIVE) COMPLIANCE GAPS



- Non-compliance with **consent requirements**: e.g. consents are not specific for each individual processing purpose
- Third party **Data Processors**: no written agreements or agreements are not in line with the GDPR
- **Data subjects' rights**: the internal procedures do not ensure effective exercise of the data subjects' rights
- The **purpose and storage limitation principles** may have to be updated; e.g. no provision or process for timely destruction of data
- **Lack** of clear and documented **notices** to consumers and to employees: e.g. no reference to the processing purposes, or to the retention period
- **Lack of legal basis** for the processing, e.g. of prospective agents' data in order to examine their solvency

(INDICATIVE) COMPLIANCE ACTION PLAN

- ✓ Ensure that the **consent forms** are in line with the GDPR provisions and the WP 29 Guidelines on consent; in old consents, request new consent!
- ✓ **Privacy notices to consumers and to employees**: review, amend and ensure that they comply with the GDPR and the WP 29 Guidelines on transparency
- ✓ **Data Processors**: amend any existing agreements or draft and execute new ones which shall contain the minimum terms provided in the GDPR
- ✓ Conduct **privacy trainings** to employees/officers involved in processing actions
- ✓ Review the data categories being collected and ensure that only the ones absolutely necessary for the processing purposes will be processed; stop collecting any **unnecessary data**
- ✓ If the processing activities include **profiling**: make sure that the relevant GDPR requirements are met; WP 29 Guidelines on automated-decision making can provide significant guidance

GDPR and Insurance Corporate Governance (1)

The GDPR adds on the corporate governance obligations of the insurance undertakings under the Solvency II and the IDD rules.

- **Appoint Data Protection Officer (DPO):** seems to be obligatory for insurance companies (see WP 29 Guidelines and FAQs)

- **Multi-national insurance groups and cross-border transfers of data:**
  - Designation of the lead supervisory authority in the EU (see relevant WP 29 Guidelines)
  - Data transfers to third countries become problematic (expected new decisions and guidance on SCCs, BCRs, new concerns on the adequacy of the Privacy Shield)

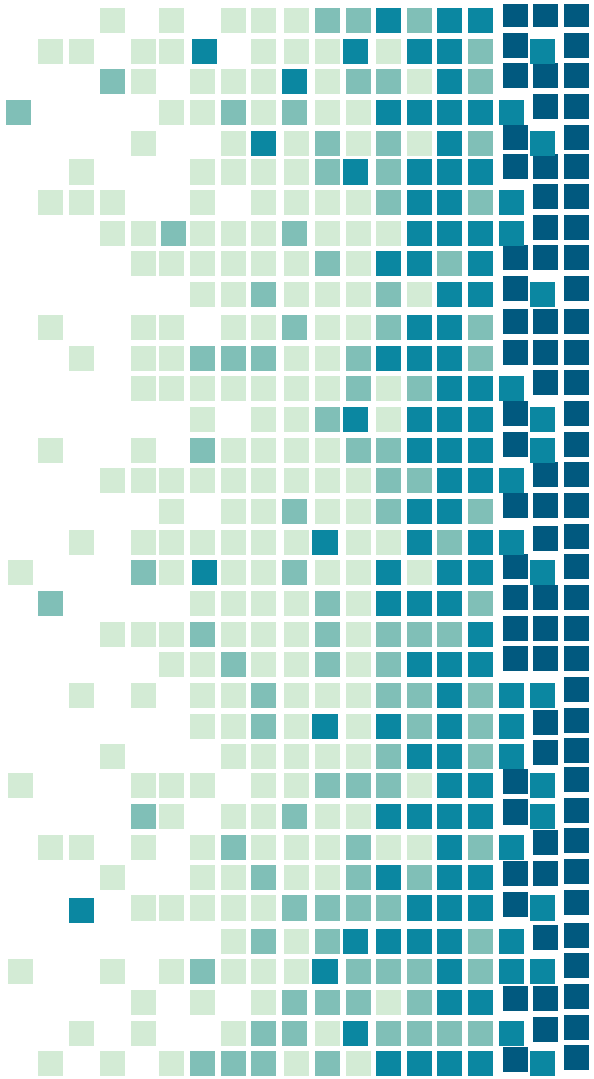
GDPR and Insurance Corporate Governance (2)

➢ **Data Protection Impact Assessment (DPIA):** GDPR and WP 29 Guidelines render it obligatory

➢**Internal Privacy and Data Protection Policies** to be amended:

- Procedures to ensure the effective exercise of data subjects' rights – particularly right to data portability (WP 29 Guidelines)
- Procedures in the event of data breach; guidance by WP 29 Guidelines
- Provide for classified access to data records (?)

4. What to expect?



Rokas
International Law Firm

Insurance-oriented follow-up on GDPR

InsurTech & GDPR

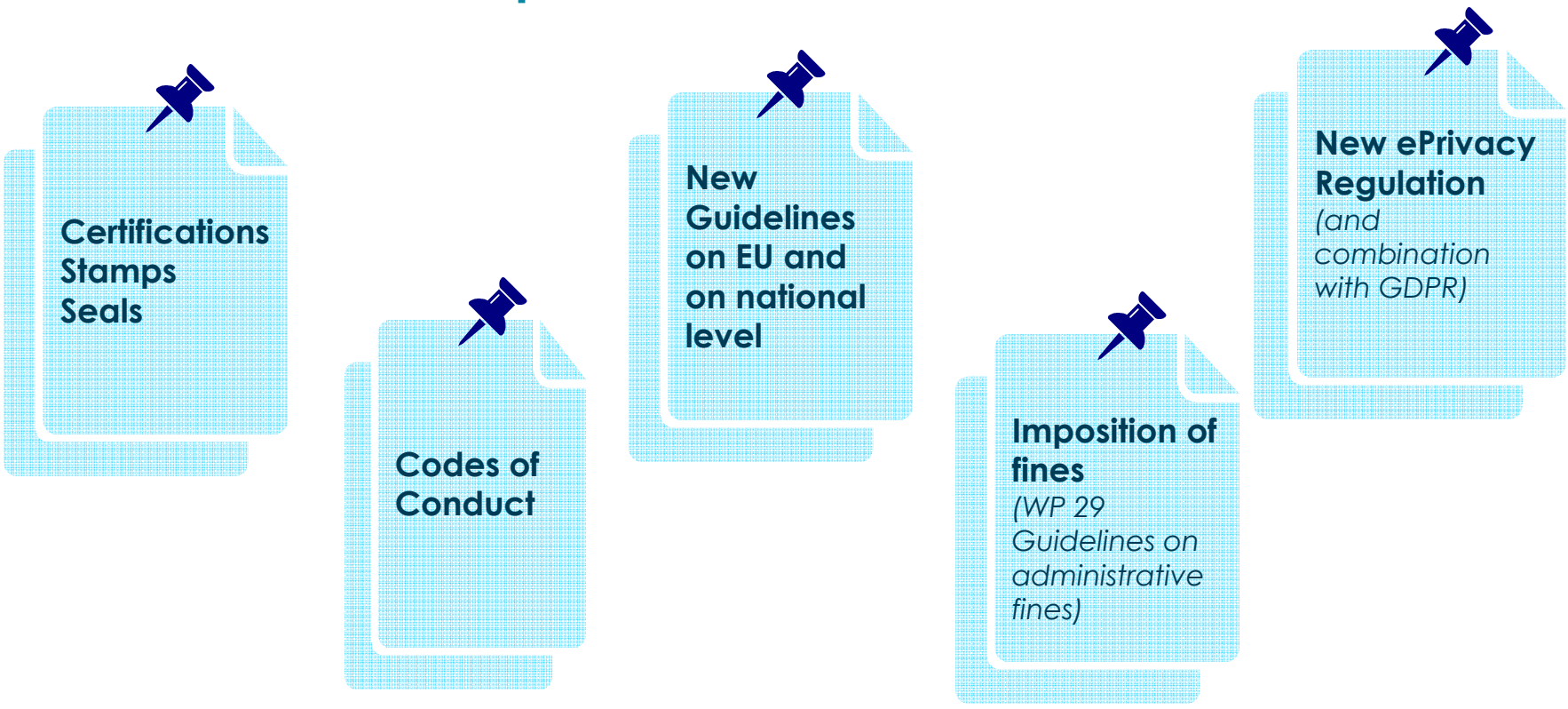
Blockchain - Virtual Currencies & GDPR

Cross-border issues:
- ✓Lead supervisory authority
- ✓Consistency mechanism
- ✓Cooperation mechanism
- ✓Role of EDPB

Third country transfers:
- ✓Adequacy decisions
- ✓New SCCs
- ✓New BCRs

National laws:
- ✓Derogations
- ✓Restrictions
- ✓Implementation

General GDPR Implementation issues



THANK YOU

Viktoria Chatzara
Senior Associate at ***Rokas*** **Law Firm**
v.chatzara@rokas.com

Rokas
International Law Firm

7th AIDA Europe Conference, Warsaw, Poland, 12 & 13 April 2018
"De-Mystifying InsurTech: a Legal and Regulatory View"