TÜV SÜD America

Choose certainty.
Add value.

Are You Ready for the EU's General Data Protection Regulation?

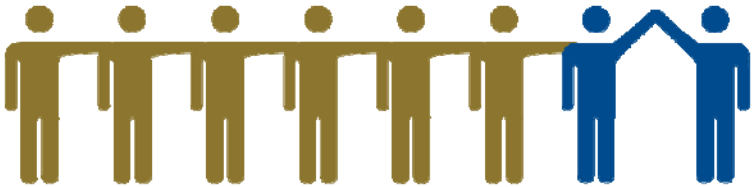
Presented by:
Martin Voelk, Senior Security Analyst
TÜV SÜD America
February 13, 2018

TÜV SÜD at a glance

150+
YEARS OF QUALITY, SAFETY & SUSTAINABILITY

1,000
LOCATIONS WORLDWIDE

€2.3
BILLION IN ANNUAL REVENUE



24,000
EMPLOYEES

43%
OF REVENUE OUTSIDE GERMANY

574,000
CERTIFICATES

100%
INDEPENDENT & IMPARTIAL

1-STOP
SOLUTIONS PROVIDER

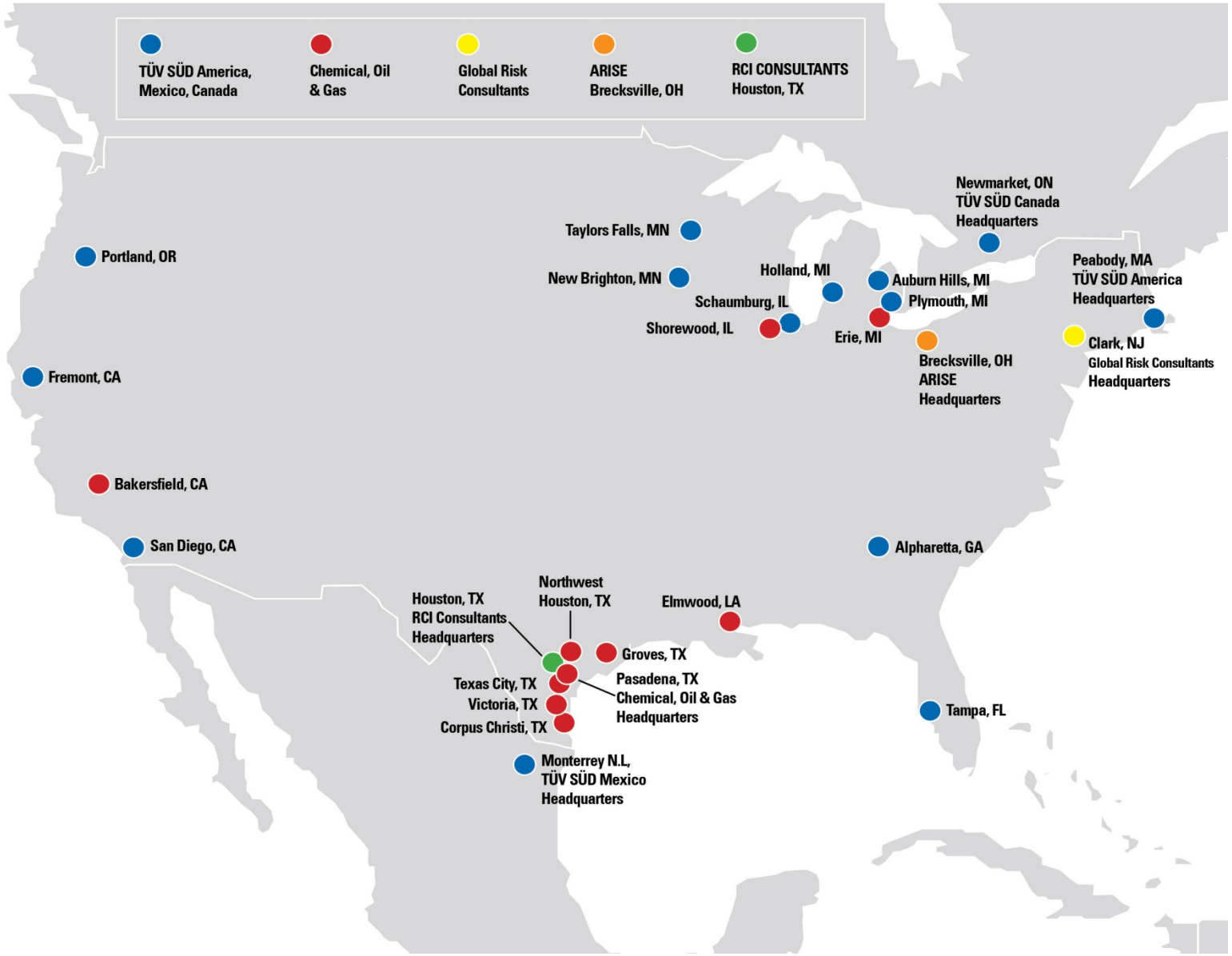
Note: Figures have been rounded off.

TÜV SÜD America Inc.

- TÜV SÜD America Inc., founded in 1987, is the North American subsidiary of TÜV SÜD AG.

- TÜV SÜD America Inc. provides complete services through its divisions:
  - Business Assurance
  - Product Service
  - Industry Service
  - Chemical, Oil & Gas
  - Global Risk Consultants (GRC)

TÜV SÜD America locations



Agenda

1. What is GDPR?
2. Objectives of GDPR
3. Who is affected by GDPR
4. Penalties for non-compliance
5. How can you make sure your organization is compliant?
6. Why chose TÜV SÜD?

Difference: Directives – Regulations, escape clauses, recitals

•GDPR:
REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and **repealing Directive** 95/46/EC (General Data Protection Regulation)

•EU Regulation which will be applicable directy in all EU Member States

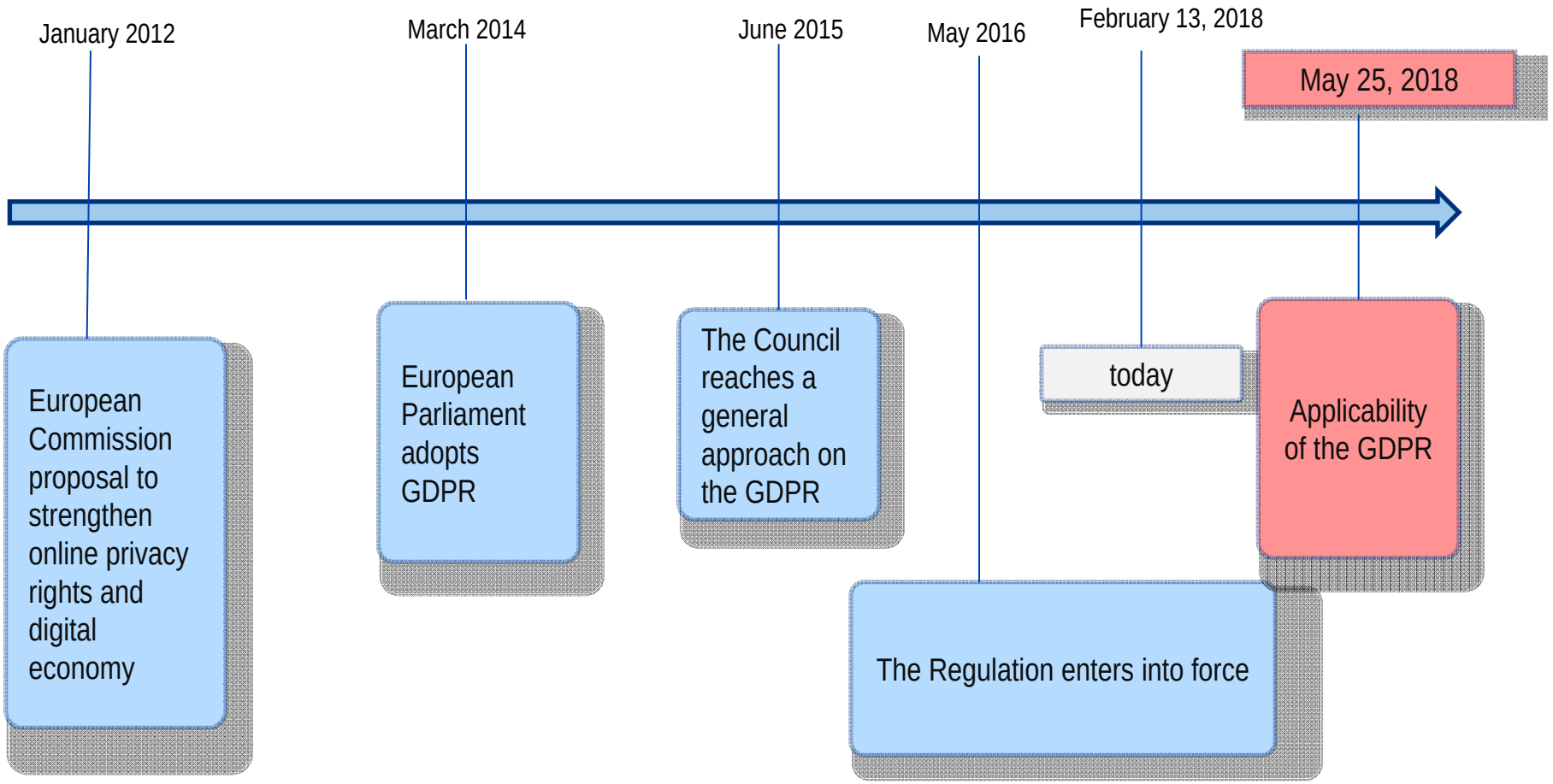
•Direct applicability → No need to implement national laws by the Member States (unlike the Directives)

•But: „escape clauses“: allow regulations in national law/ room for manoeuvre/ mandate for action

•For example in Germany:
Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (DSAnpUG-EU) of 30 June 2017, so called BDSG (amended version)

•Additional: recitals of the GDPR

History of the GDPR



Applicability of GDPR

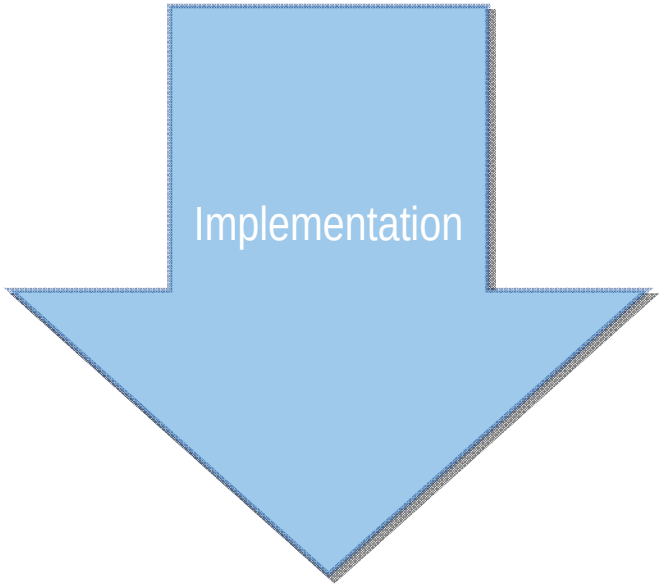
Article 99
Entry into force and application

(1)This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

(2) It shall apply from 25 May 2018.

Example for an escape clause for Germany

GDPR



BDSG (amended version)

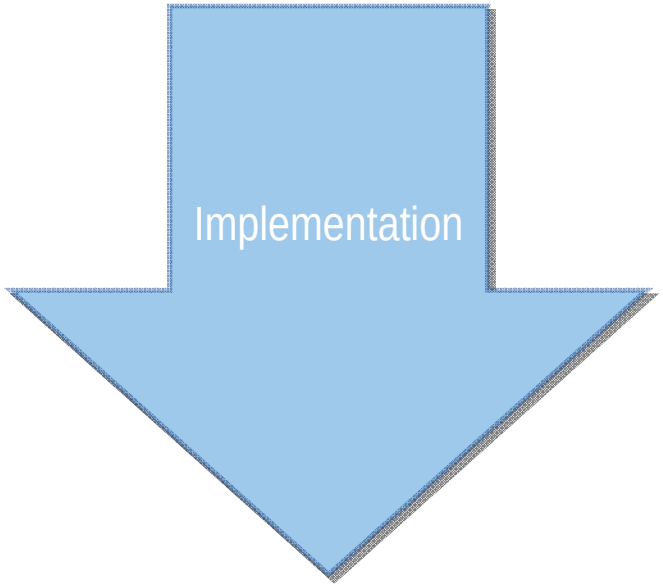
GDPR:

Article 88
Processing in the context of employment

(1) **Member States may, by law** or by collective agreements, **provide for more specific rules** to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context […].

Example for an escape clause for Germany

GDPR



BDSG (amended version)

BDSG (amended version):

Section 26
Data processing for employment-related purposes

(1)Personal data of employees may be processed for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract or to exercise or satisfy rights and obligations of employees' repre-sentation laid down by law or by collective agreements or other agreements between the employer and staff council. […]

It‘s all about personal data

Personal data

any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or Indirectly

- surename, first name
- address (private and business)
- contact details (e-mail, telephone number, private and business)
- personnel number
- Identity number
- banking information
- date of birth
- martial status
- salary
- IP-address
- license plate
- […]

Special categories of personal data

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person’s sex life or sexual orientation

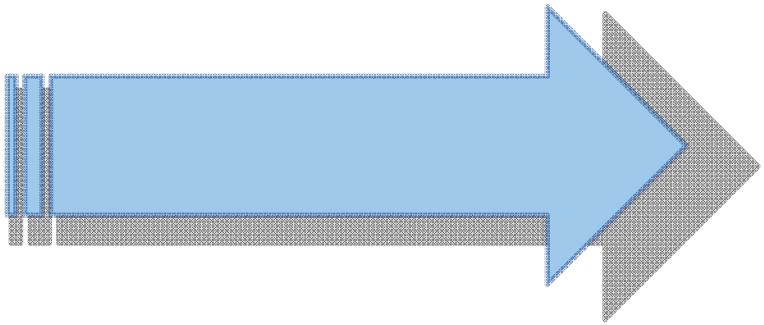
Agenda

1. What is GDPR?
2. Objectives of GDPR
3. Who is affected by GDPR?
4. Penalties for non-compliance
5. How can you make sure your organization is compliant?
6. Why chose TÜV SÜD?

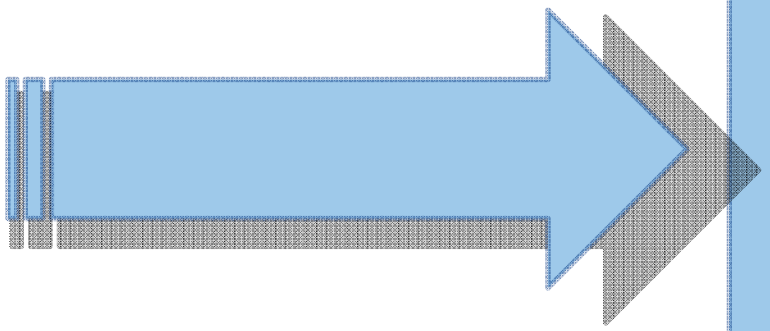
Need for action

Problems:

- Different level of data protection between the Member States
- Constant further development of the jurisdiction of the European Court of Justice regarding data protection



Need for action

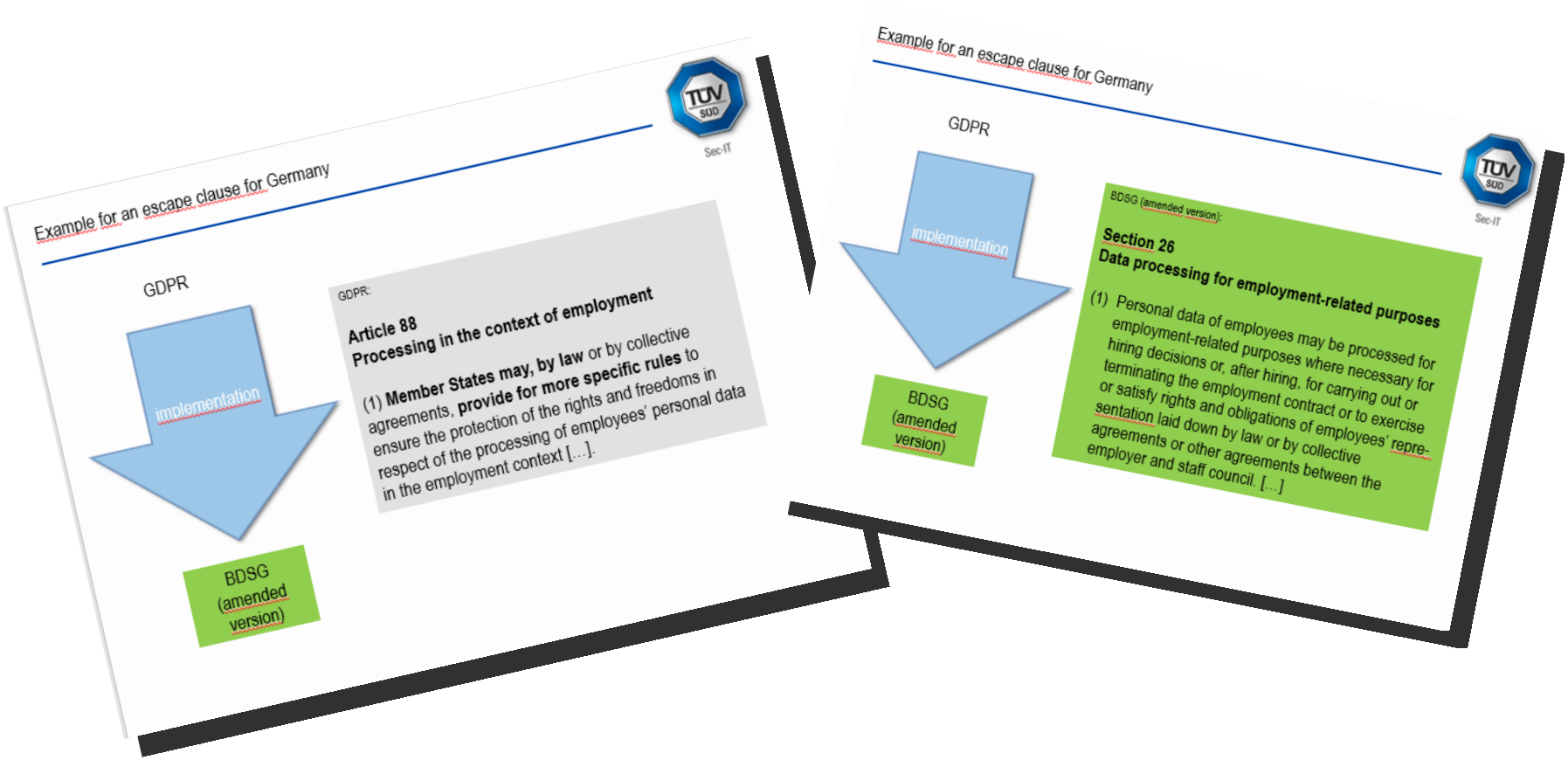


Objectives:

- Harmonise regulated legal matter
- Creation of equal economic conditions and equal terms of competition
- Ensure the free flow of personal data between the Member States
- Protection of fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data
- Ensuring a high level of the protection of personal data regarding the transfer to third countries

Need for action

But no full harmonisation because of the escape clauses!



Agenda

1. What is GDPR?
2. Objectives of GDPR
3. Who is affected by GDPR?
4. Penalties for non-compliance
5. How can you make sure your organization is compliant?
6. Why chose TÜV SÜD?

Material scope

GDPR applies to

GDPR does not apply to

Material Scope

Processing of personal data

- Automated

- Non-automated processing of personal data which are stored or are to be stored in a filing system

Processing of personal data

- By a natural person in the course of a purely personal or household acitvity

- By competent authorities (prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security)

Territorial scope

Territorial Scope

Controllers in the European Union (EU)

–any person who operates **from an establishment within in the EU**

–regardless whether the processing itself takes place within the EU

–establishment implies the effective and real exercise of activity through stable arrangements

–not the determining factor: legal form of the stable arrangement (whether through a branch or a subsidiary with a legal personality)

–not relevant: data subject has a job or habitual residence in a third country or is a foreign national

–**example:** GDPR (+) if US company with an (independent or dependent) establishment in the EU processes personal data in the context of the activities of the European establishment

Territorial scope

Territorial Scope

Controllers resident outside the European Union (EU)
if the processing activities are related to

–**offering goods or services**, irrespective of whether a payment of the subject is required, to such data subjects in the EU

- insufficient: accessibility of a website in the EU, of an e-mail-address of of other contact details
- sufficient: use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the EU

– the **monitoring of data subject's behaviour** as far as their behaviour takes place within the EU

- e.g. tracking on the internet including potential subsequent use of personal data processing techniques

- **representative** in the EU (without legal prejudice to legal actions initiated against controller or processor)
  - shall be designated in writing
  - shall be established in one of the Member States where the data subjects are
  - contact point for supervisory authorities and data subjects

Territorial scope

Norm Addressees	
Controller	**Processor**
natural or legal person, authority, agency or other body who either alone or with others decides on the purpose and the means of processing of personal data	natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Agenda

1. What is GDPR?
2. Objectives of GDPR
3. Who is affected by GDPR?
4. Penalties for non-compliance
5. How can you make sure your organization is compliant?
6. Why chose TÜV SÜD?

Principles relating to processing of personal data (Article 5)

Lawfulness, fairness and transparency	• Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
Purpose limitation	• Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes […].
Data minimisation	• Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Principles relating to processing of personal data (Article 5)

Accuracy	• Personal data shall be accurate and, where necessary, kept up to date […].
Storage limitation	• Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed […].
Integrity and confidentiality	• Personal data shall be processed in a manner that ensures appropriate security of the personal data […].

More important requirements (without limitation)

Privacy by design

- The controller shall implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles.

Privacy by default

- The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

Data Protection Officer (DPO)

- The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

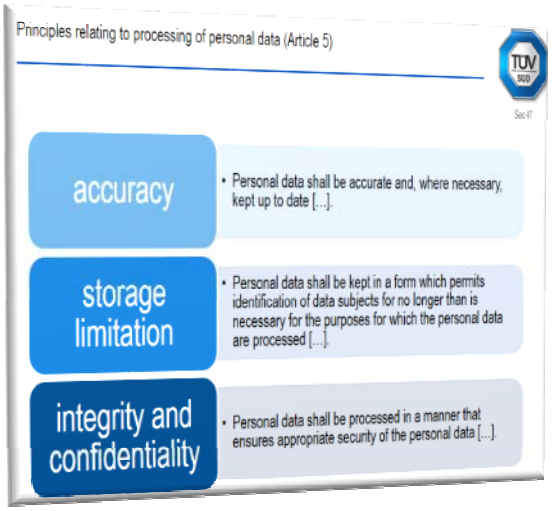
More important requirements (without limitation)

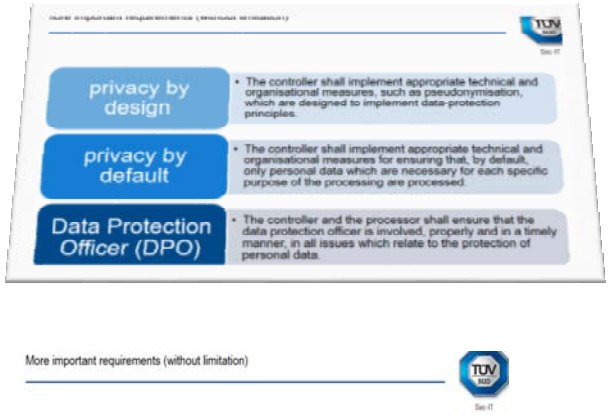
Rights of the data subjects	• Right to be forgotten • Information and access to personal data • Right to data portability […]
Processor	• Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller […].
Records of processing activities	• Each controller and each processor and, where applicable, the controller's/ processor's representative, shall maintain a record of processing activities under its responsibility […].

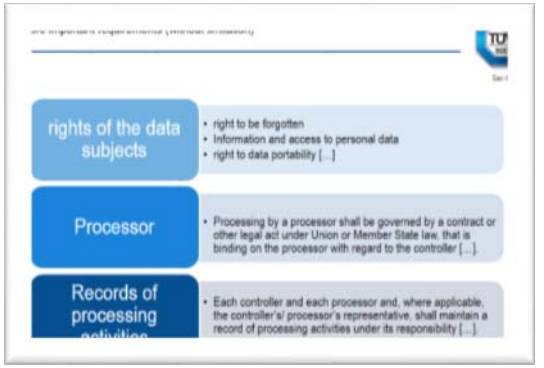
More important requirements

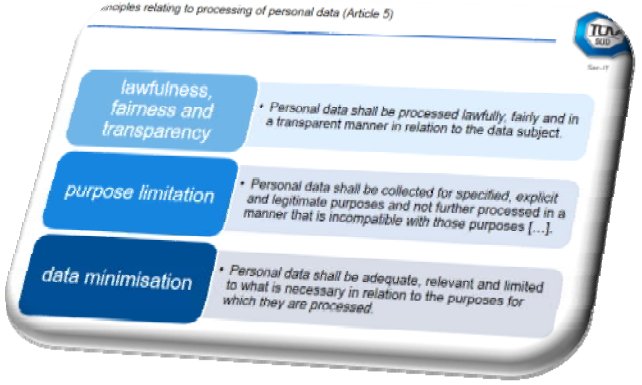
Accountability

The controller shall be responsible for, and be able to demonstrate compliance with, Article 5 paragraph 1









Penalties

Each supervisory authority shall ensure that the imposition of administrative fines […] shall in each individual case be **effective**, **proportionate** and **dissuasive**.

Penalties

up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Right to compensation and liability

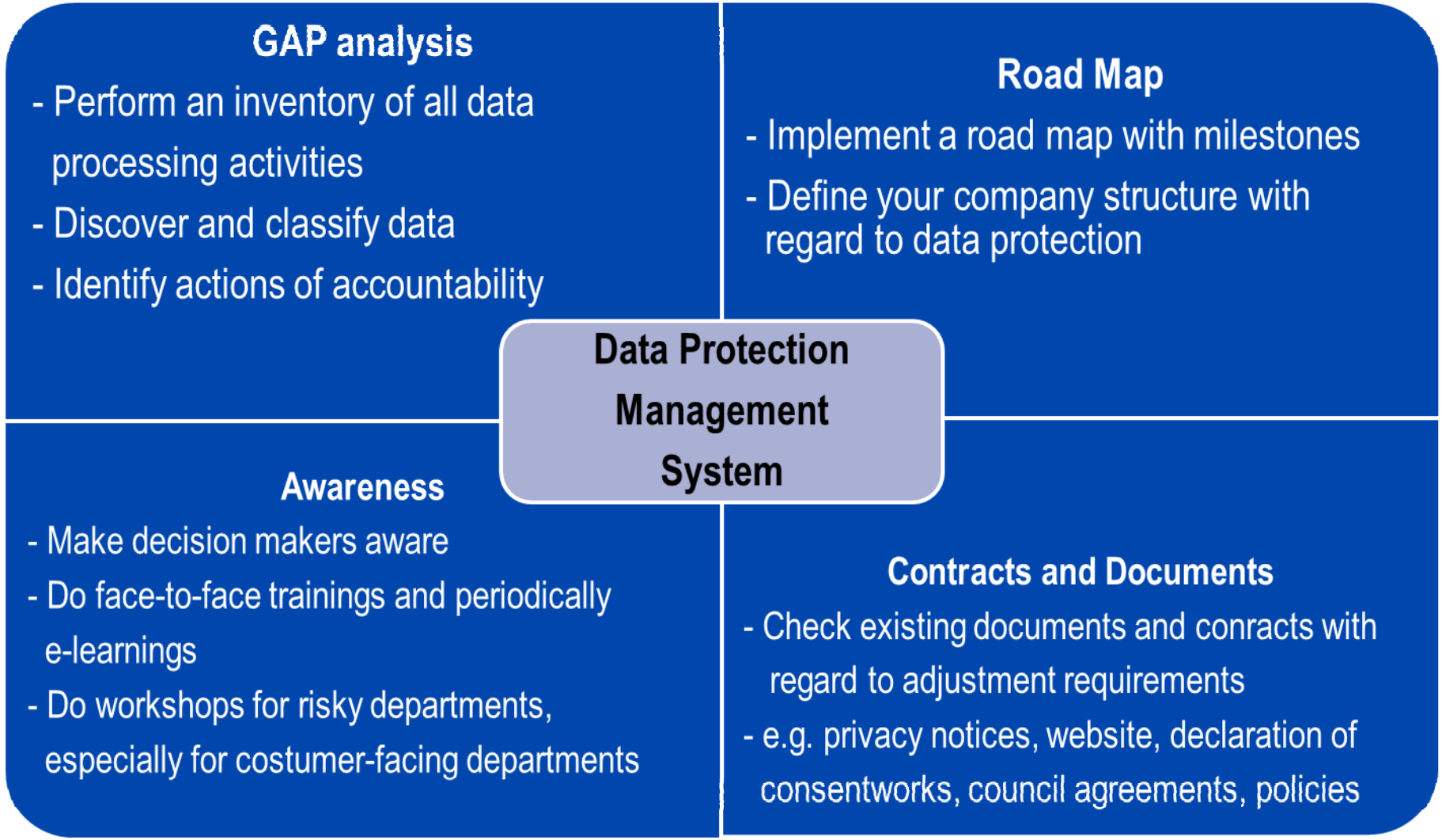
Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive **compensation from** the **controller or processor** for the damage suffered.

The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage.

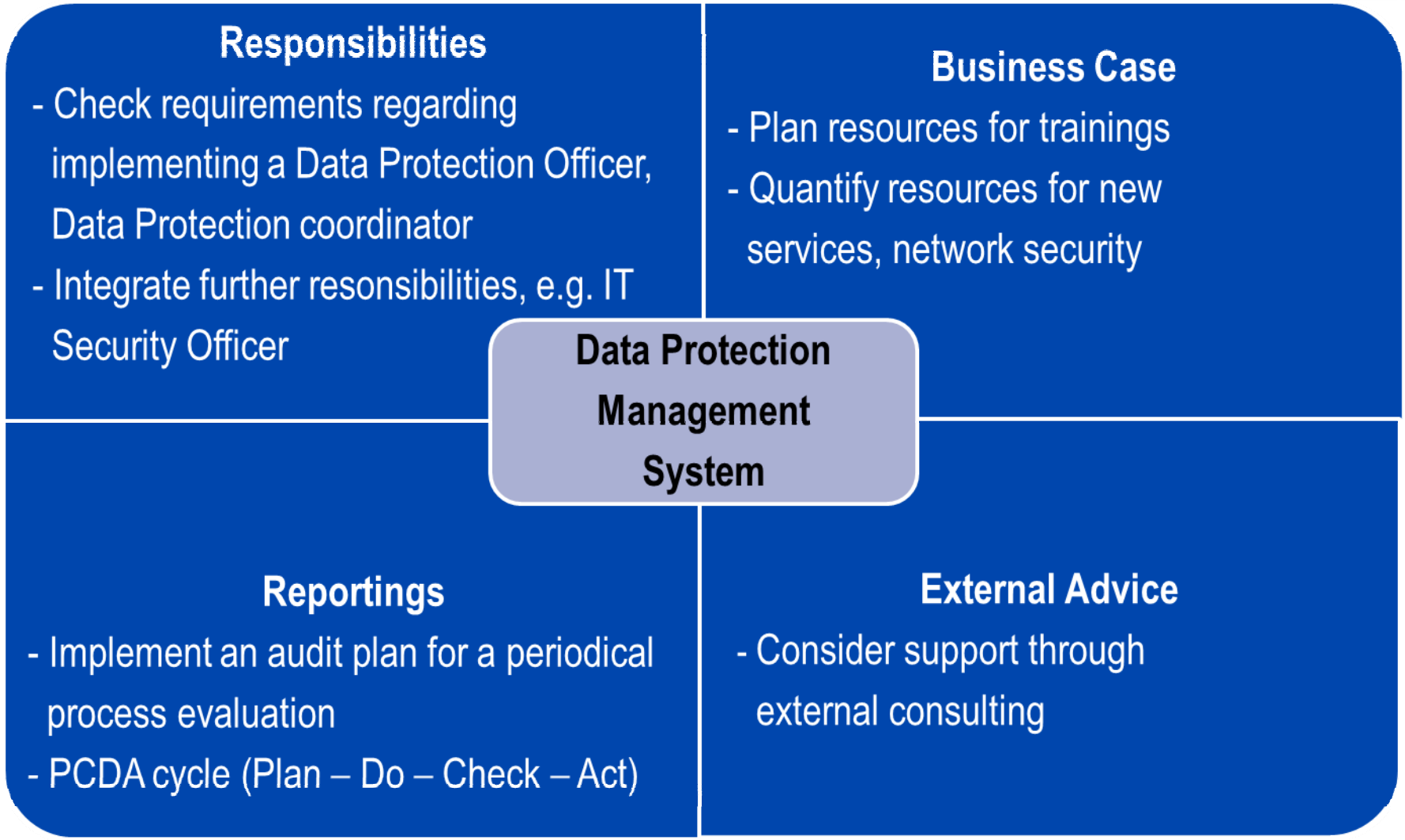
Agenda

1. What is GDPR?
2. Objectives of GDPR
3. Who is affected by GDPR?
4. Penalties for non-compliance
5. How can you make sure your organization is compliant?
6. Why chose TÜV SÜD?

Data Management



Data Management



Agenda

1. What is GDPR?
2. Objectives of GDPR
3. Who is affected by GDPR?
4. Penalties for non-compliance
5. How can you make sure your organization is compliant?
6. Why chose TÜV SÜD?

Why choose TÜV SÜD?

One-stop solution

TÜV SÜD offers a wide variety of IT Certification and IT Security Services.

World wide network

Our global business network allow us to serve your local business operations.

Added business value

We identify your vulnerabilities with specific and clear recommendations for actions.

Quality experts

TÜV SÜD auditors and experts have high levels of qualification and years of hands-on experience.

Additional benefits

Compliance Assessments / Gap Analysis

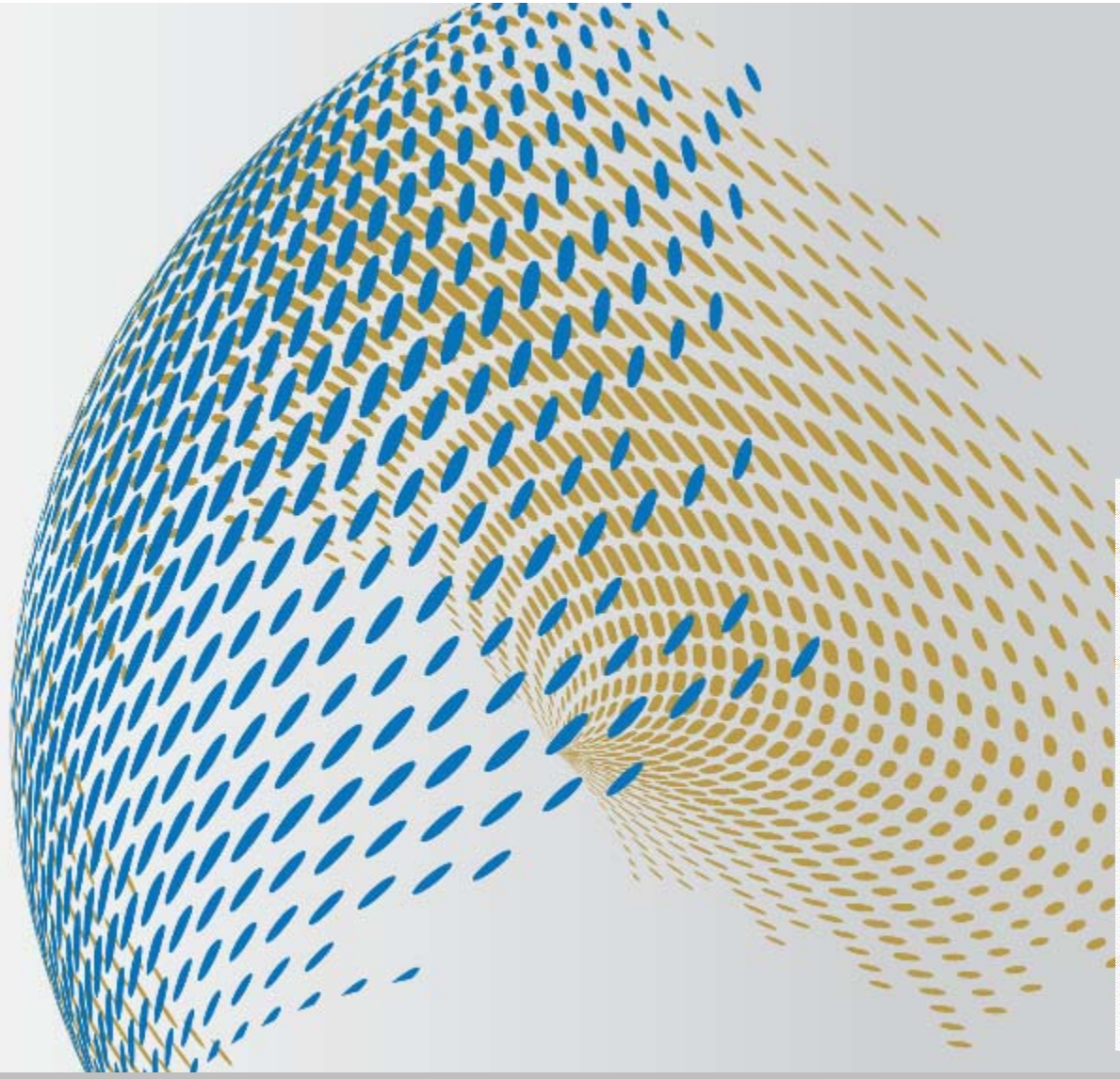
Mitigation

Ongoing monitoring

In-house or Live online Training

DPO preparedness

Discover the advantages of partnering with TÜV SÜD America



Contact us:
www.tuv-sud-america.com
info@tuvam.com

Follow us on social media:

instagram.com/tuvsud

linkedin.com/company/tuv-sud

twitter.com/tuvsud

youtube.com/tuvsudgroup