OFFICIAL (ISC)² CHAPTER | BEIJING

请先扫码

Connect | Educate | Inspire | Secure

EU General Data Protection Regulation implementation

Presented by Yves LE ROUX
CISM,CISSP
EAC GDPR Task Force Chair
yleroux@eac.isc2.org

(ISC)2北京分会第15次安全沙龙 @京仪大酒店

Big thanks to：
会议室及晚宴赞助商：爱思考
巧克力赞助者：雪玲珑
现场志愿者：刘宇

OFFICIAL (ISC)² CHAPTER | BEIJING

The EAC GDPR Task Force (GDPR TF)

- Yves LE ROUX, (ISC)² EAC Co-Chair, Chair
- Samuel Berger (Germany) Senior Technical Director, AT&T, Chief Security Office
- Michael Christensen (Denmark) Freelance Compliance and InfoSec Consultant
- Ramon Codina (Spain)
- Albert Granyo (Spain)
- David Higgins (UK) Independent Consultant
- Alain Bensoussan and Olivianne Juès (France) Technology Attorneys
- Paul Lanois (Switzerland) Technology Attorney
- Santosh Krishna Putchala (India)
- Eric Tierling, (USA) Sr. Compliance Program Manager, Microsoft Corporation,
- Visia Tartaglione (USA) Information Security Consultant & Project Manager

OFFICIAL (ISC)² CHAPTER | BEIJING

GDPR TF Publications

- The (ISC)² EMEA Advisory Council GDPR Task Force has published:
  - overview of the basics
  - 12 Areas of Activity and their key supporting tasks

  Both documents are freely available @ http://blog.isc2.org/

OFFICIAL (ISC)² CHAPTER | BEIJING

EU General Data Protection Regulation (GDPR)

- The EU Commission presented its legislative proposal in January 2012 as replacement of Directive 95/46
- After negotiating with the EU Council, the draft GDPR has been adopted by the European Parliament-on April 14th 2016 and published on May 4th 2016 in the Official journal
- The regulation entered into force 20 days after its publication in the EU Official Journal.
- Its provisions will be directly applicable in all Member States two years after this date.

OFFICIAL (ISC)² CHAPTER | BEIJING

Personal Data Traceability

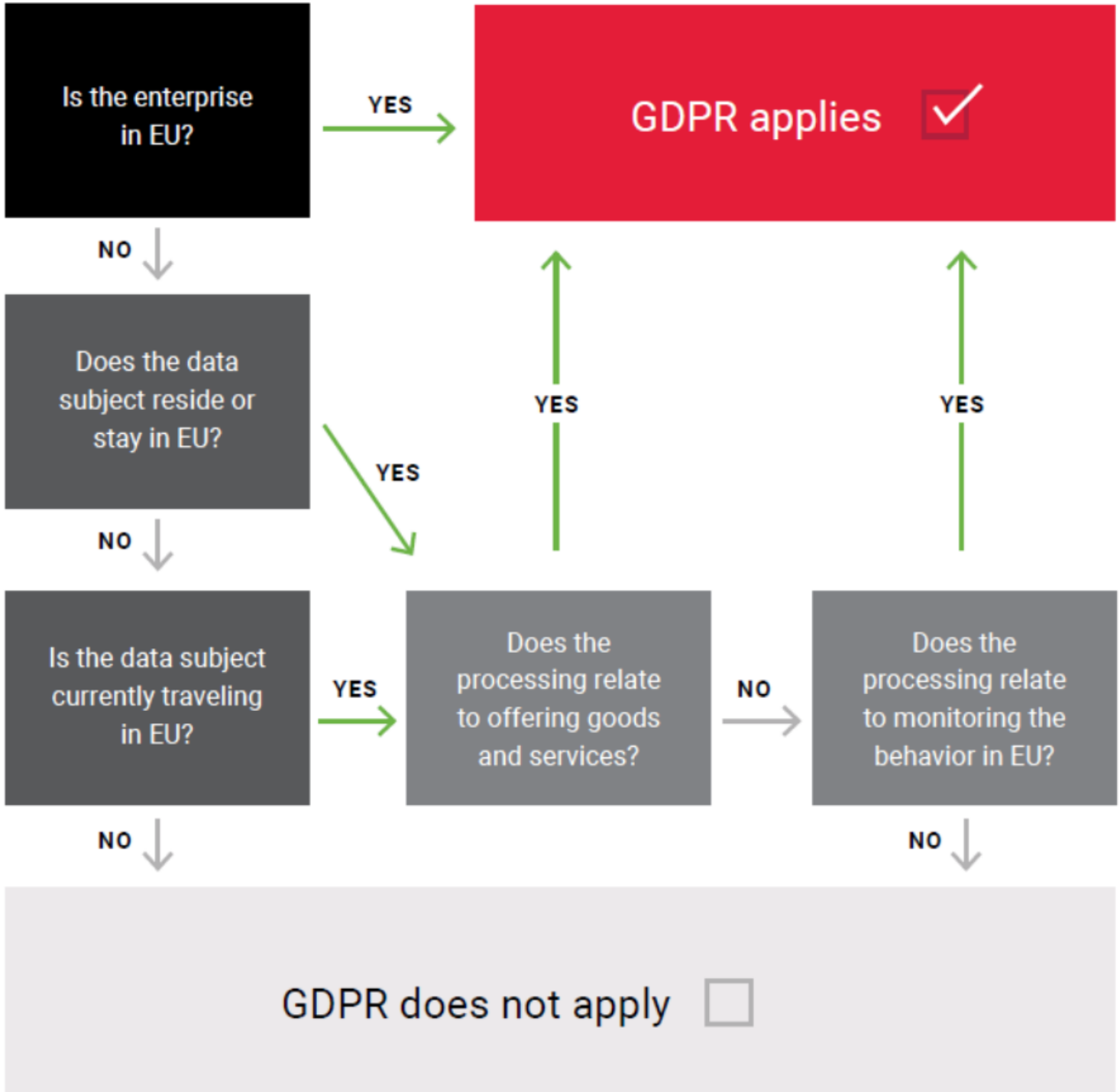
OFFICIAL (ISC)² CHAPTER | BEIJING

Personal Data definition

- ‘Personal Data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who **can be identified, directly or indirectly,** in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria.

OFFICIAL (ISC)² CHAPTER | BEIJING

Why GDPR may impact non EU companies?



OFFICIAL (ISC)² CHAPTER | BEIJING

Why GDPR may impact non EU companies?

- GDPR applies regardless of whether the processing takes place in the EU or not.

- Looking at the precedent slide, many non-EU businesses that were not clearly required to comply with the Directive will be required to comply with the Regulation

EU representatives for GDPR

- The non-EU resident controllers and processors who are obliged to comply with the GDPR must appoint representatives within the EU to be a point of contact for the EU personal data subjects and regulators for the purposes of enforcement of the GDPR

Exceptions to EU representatives

- Obligation to appoint an EU representative shall not apply to:
  - processing which is occasional, does not include, on a large scale, processing of special categories of data or processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons; or
  - a public authority or body.

International Data transfers

- GDPR allows for data transfers to countries whose legal regime is deemed by the European Commission to provide for an “adequate” level of personal data protection.
- In the absence of an adequacy decision, transfers are also allowed outside non-EU states under certain circumstances, such as by use of standard contractual clauses or binding corporate rules (BCRs).
- BCRs require approval from DPAs, but once such approval is obtained, individual transfers made under BCRs do not require further approval.
- Derogations are also permitted under limited additional circumstances.

International Data transfers

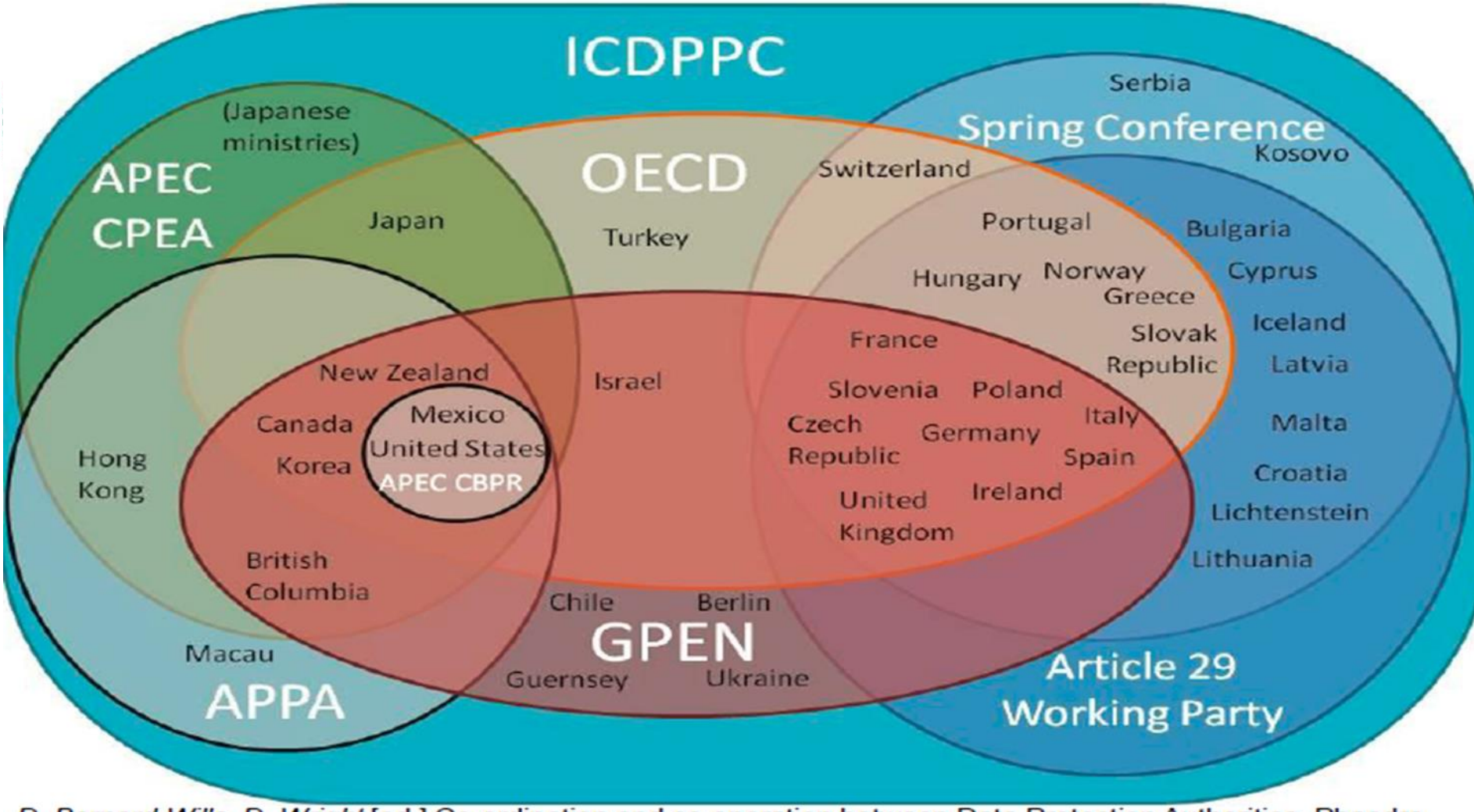
- In light of the increased penalties and the general media attention to non-compliance in the area of data protection, a multinational may be willing to audit its existing intra-group data transfer arrangements or consider developing binding corporate rules (BCR).

Binding Corporate Rules (BCR)

- Binding Corporate Rules ("BCR") are internal rules (such as a Code of Conduct) adopted by multinational group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection.
- Once approved under the EU cooperation procedure, BCR provide a sufficient level of protection to companies to get authorisation of transfers by national data protection authorities ("DPA")
- More details in GDPR Article 47

Increased enforcement powers

- The GDPR introduces significant fines, including revenue based fines, which enables the DPAs to impose fines for some infringements of up to the higher of 4% of annual worldwide turnover and EUR20 million. Other specified infringements would attract a fine of up to the higher of 2% of annual worldwide turnover and EUR10 million.
- Global Privacy Enforcement Network (GPEN) comprise 64 privacy enforcement authorities in 47 jurisdictions around the world



D. Barnard-Wills, D. Wright [ed.] Co-ordination and co-operation between Data Protection Authorities. Phaedra Workstream 1 report, 2014, p. 136

OFFICIAL (ISC)² CHAPTER | BEIJING

Specific issues for non-EU Business

- Whether, taking into account its business model and the existing processes, it is in scope of the GDPR?
- What does it mean for the non-EU business to comply with the GDPR both in terms of restructuring the operations and on-going costs?
- How the cross-border intra-group personal data transfers are structured and whether any changes to these processes may be required?

Specific issues for non-EU Business

- Whether compliance with the GDPR can conflict with the need to continue to comply with the existing data protection rules in the home jurisdiction of the non-EU entity?
- Whether any restructuring of operations/business is necessary/feasible to ensure compliance/minimize compliance costs?
- Who should be appointed as a Representative, and what the arrangements with such Representative shall include?

OFFICIAL (ISC)² CHAPTER | BEIJING

Article 29 Working Party Guidelines

- Guidelines on the right to "data portability", wp242rev.01
- Guidelines on Data Protection Officers ('DPOs'), wp243rev.01
- Guidelines on The Lead Supervisory Authority, wp244rev.01
- Guidelines on Data Protection Impact Assessment (DPIA) wp248
- Draft Guidance on automated decision making and profiling wp251

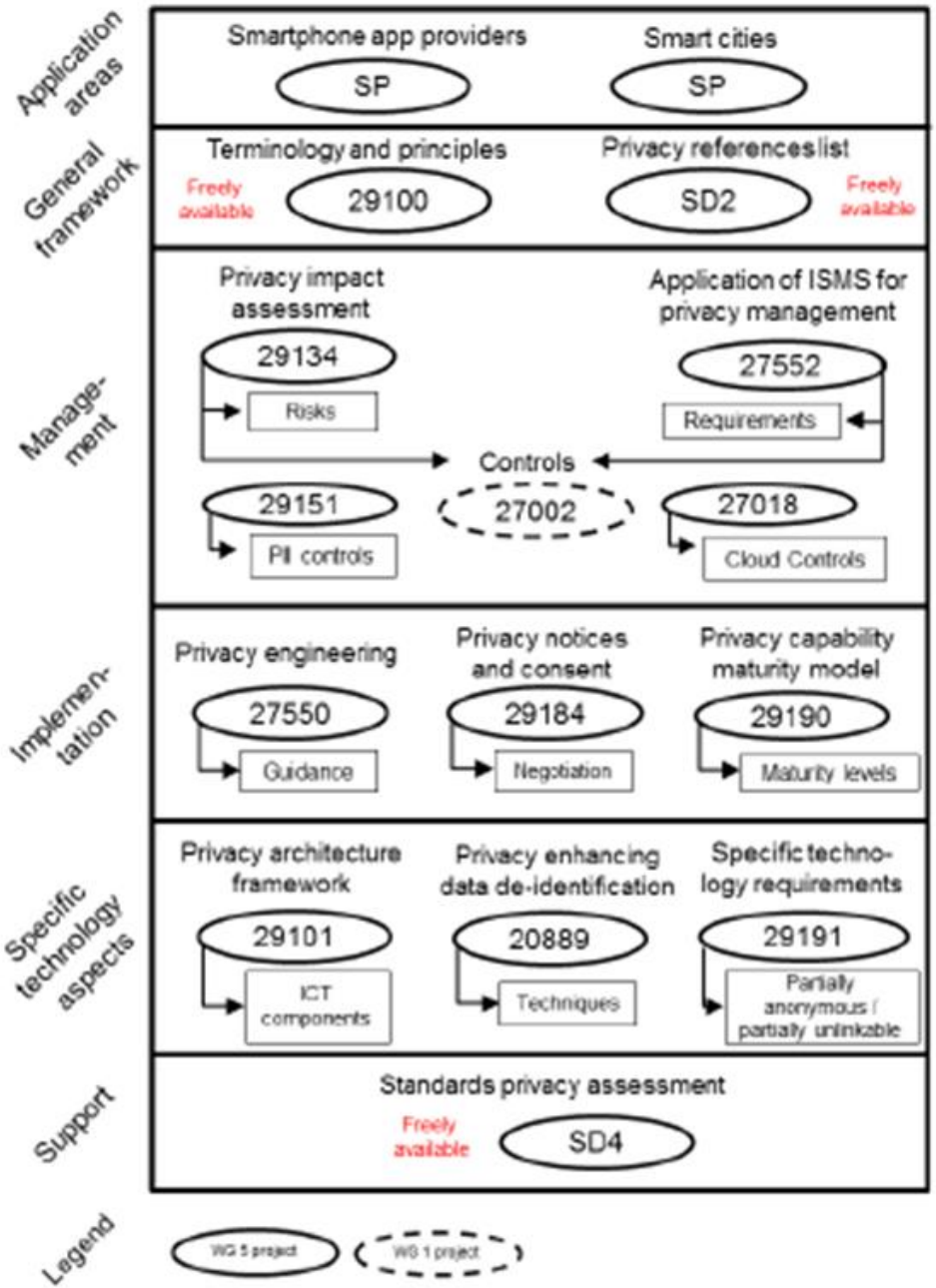
Involvement of the DPAs in standardization

- WP29 positions taken into account in ISO/IEC 29100 (Privacy terms and principles)
- Official liaison betweenWP29 and ISO
- Legitimity in information security in editing ISO/IEC 27001
- New projects: ISO/IEC 27009, ISO/IEC 29134, ISO/IEC 29151, ISO/IEC 27552, etc.

OFFICIAL (ISC)² CHAPTER | BEIJING

Involvement of the DPAs in standardization

- Following the ISO meetings, the liaison officer has informed WP29 during its plenary meetings on the key projects of ISO SC27 WG5,e.g.:
  - Enhancement to ISO/IEC27001 for privacy management (ISO/IEC27552)
  - Privacy Impact Assessment(PIA,ISO/IEC29134)
  - Privacy controls(ISO/IEC29151)
  - Privacy Enhancing Technologies for Data de-identification (ISO/IEC20889)
  - Online privacy notices and consent (ISO/IEC29184)


Application areas
Smartphone app providers
SP
Smart cities
SP
General framework
Terminology and principles
Freely available
29100
Privacy references list
SD2
Freely available
Management
Privacy impact assessment
29134
Risks
Application of ISMS for privacy management
27552
Requirements
Controls
29151
PII controls
27002
27018
Cloud Controls
Implementation
Privacy engineering
27550
Guidance
Privacy notices and consent
29184
Negotiation
Privacy capability maturity model
29190
Maturity levels
Specific technology aspects
Privacy architecture framework
29101
ICT components
Privacy enhancing data de-identification
20889
Techniques
Specific technology requirements
29191
Partially anonymous / partially unlinkable
Support
Standards privacy assessment
Freely available
SD4
Legend
WG 5 project
WG 1 project

GDPR Task Force Action Plan

BEIJING

GDPR Task Force Action Plan

1. Insure the support from the board & business units
2. Establish inventory of personal information held
3. Privacy Notice & Information
4. Individuals' rights
5. Data subjects' access requests
6. Data protection impact assessments (DPIA)
7. Consent
8. Children
9. Personal data breaches
10. Security of data processing & data protection by design
11. Data protection governance
12. International data transfers

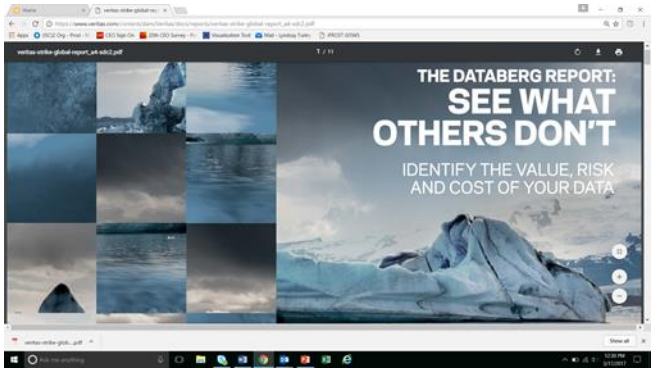
OFFICIAL (ISC)² CHAPTER | BEIJING

Stakeholder Support: Board & Business units

- Decision makers and key people in your organisation must be aware of their accountability and appreciate the impact GDPR is likely to have so that they can identify areas and processes that will need to change
- Implementation could require significant resources, especially for larger and more complex organisations.

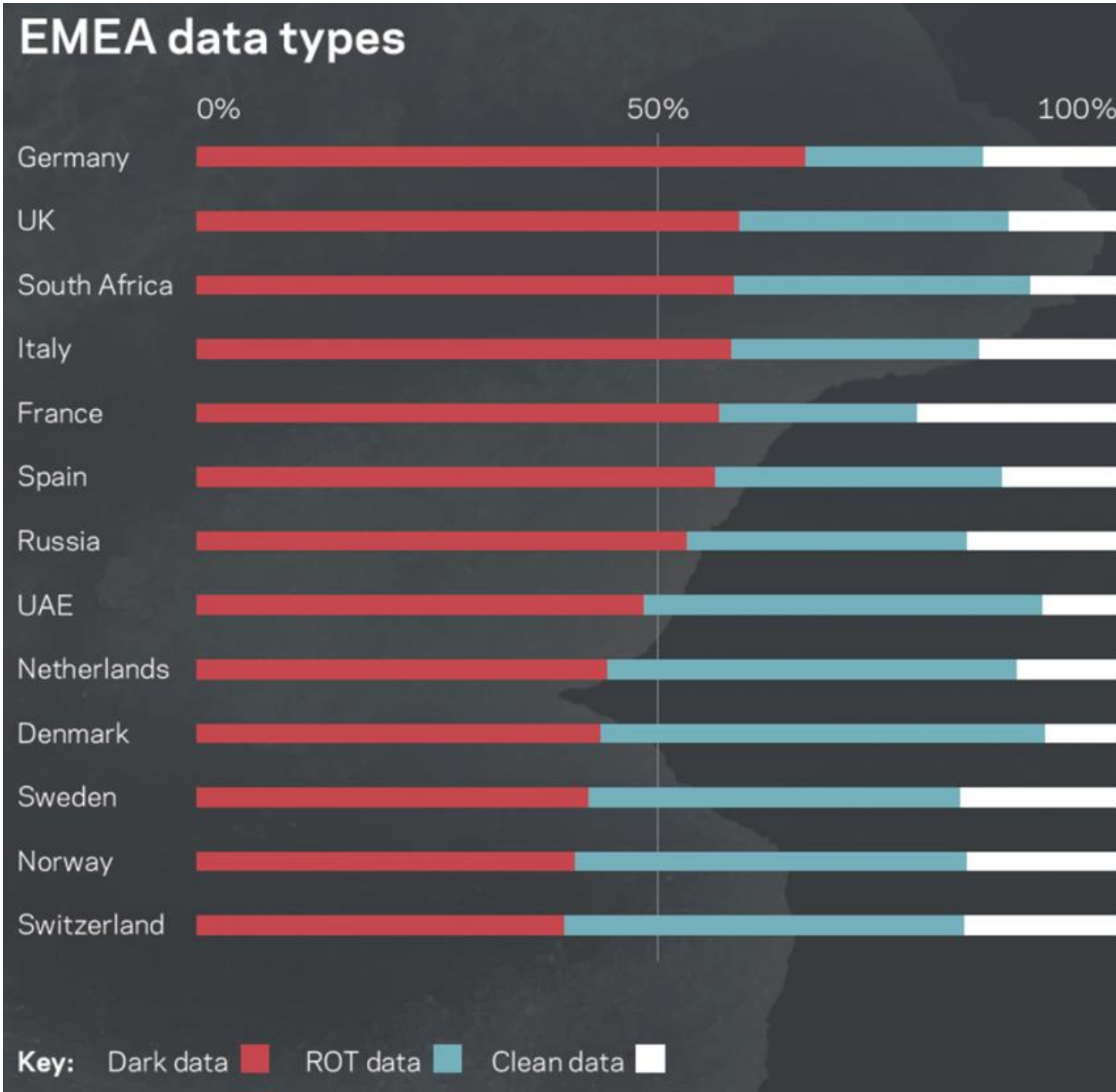
Inventory of the personal Information you hold

- You should document
  - what personal data you hold
  - where it came from and
  - who you share it with



- Presenting a real a challenge for companies: Databerg Research by Vanson Bourne for Veritas Technologies LLC: https://www.veritas.com/content/dam/Veritas/docs/reports/veritas-strike-global-report_a4-sdc2.pdf

OFFICIAL (ISC)² CHAPTER | BEIJING



OFFICIAL (ISC)² CHAPTER | BEIJING

Privacy Notice & Information

- You must give notice that:
  - Provides details of the grounds that are used to justify processing
  - highlights that consent may be withdrawn, the existence of the data subject rights (see action 4) and the right to lodge a complaint with the Supervisory Authority, and
  - is concise, transparent, intelligible and in an easily accessible form using clear and plain language.

Individuals' rights

The main rights for individuals under the GDPR will be:

- access to their personal data,
- to have inaccuracies corrected,
- to have information erased,
- to object to the processing of personal data for direct marketing purposes,
- to prevent automated individual decision-making and profiling, and
- data portability.

Individuals' rights

- GDPR introduces two new rights:
  - The right to be forgotten.
    - This right basically allows individuals to request the deletion of personal data, and, where the controller has publicized the data, to inform other controllers to also comply with the request.
  - The right to data portability
    - This right basically requires controllers to provide personal data to the data subject in a commonly used format and to transfer that data to another controller if the data subject so requests.

Individuals' rights

Data subjects are entitled under GDPR to a number of rights with regard to automated profiling:

- Some – like notice and access – require procedures similar to non-profiling data processing.
- Others– like the right to object, halt the profiling, and/or avoid profiling-based decisions –require special attention and set processes for compliance.

Data subjects' access requests

- Data subjects will have a right to request a copy of their personal data undergoing processing. They may also request:
  - the purpose of processing, the period of time for which data will be stored, any recipients of the data, the logic of automated decision-making, including profiling, and the envisaged consequences of any such processing.
- The controller must take the appropriate action "without undue delay" or at the latest within a month of the request

Data Protection Impact Assessments (DPIA)

- The GDPR introduces Data Protection Impact Assessments (DPIA) as a means to identify and deal with high risks, notably to the privacy rights of individuals when processing their personal data.
- The DPIA requirement is linked to processing "likely to result in a high risk for the rights and freedoms of natural persons," taking into account "the nature, scope, context and purposes of the processing."

Data Protection Impact Assessments (DPIA)

- Individual DPAs have authority to publish guidance on the kinds of processing operations that require a DPIA and those that do not, and these individual guidance documents might differ from country to country.

Consent

- Consent must be “freely given, specific, informed and unambiguous.”
- Consent has to be specific to the processing operations. The controller cannot request open-ended or blanket consent to cover future processing.
- GDPR requires the data subject to make a statement or clear affirmative action removing the possibility of “opt-out” consent or the interpretation of silence, inactivity, and pre-ticked boxes as a means of providing consent.

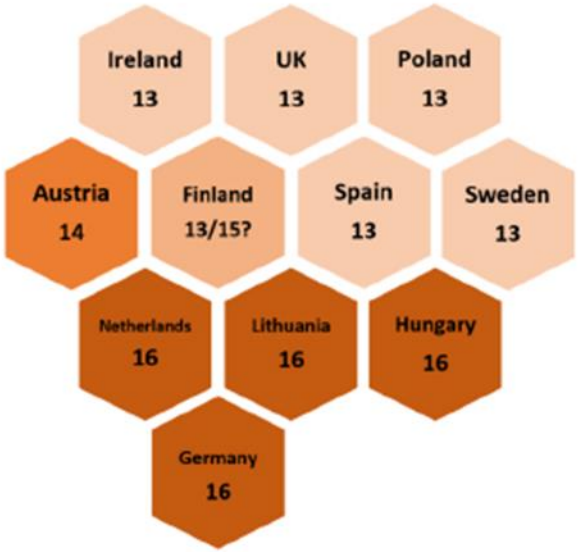
Consent

- GDPR allows member states to enact laws that restrict the processing of some categories of data even if the data subject explicitly consents.
- The data controller bears the burden of demonstrating that consent was obtained lawfully.

Children

- GDPR introduces specific protections for children who are identified as “vulnerable individuals” and deserving of “specific protection”. This applies to children under the age of 16, unless a Member State has made provision for a lower age limit (lowest age limit is 13).

- Where online services are provided to a child and consent is relied on as the basis for the lawful processing of his or her data, consent must be given or authorised by a person with parental responsibility for the child.



Personal Data breaches

- A “personal data breach” is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”
- In the event of a personal data breach, as a general rule, data controllers must notify the supervisory authority.

Personal Data breaches

- Notice must be provided “without undue delay and, where feasible, not later than 72 hours after having become aware of it.” If notification is not made within 72 hours, the controller must provide a “reasoned justification” for the delay.
- Moreover, in most cases, data controller will have to communicate the personal data breach to the data subject, without undue delay.

Personal Data breaches

A notification to the authority must “at least”:

- describe the nature of the personal data breach, including where it is possible the number and categories of data subjects and personal data records affected;
- provide the data protection officer’s contact information;
- “describe the likely consequences of the personal data breach”; and
- describe how the controller has addressed or proposes to address the breach, including any mitigation efforts

Security of data processing & Data Protection by Design

- Controllers and processors are required to "implement appropriate technical and organizational measures" taking into account "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."

Security of data processing & Data Protection by Design

Specific suggestions for what kinds of security actions might be considered “appropriate to the risk,” including:

- The pseudonymisation and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

OFFICIAL (ISC)² CHAPTER | BEIJING

Security of data processing & Data Protection by Design

- Controllers and processors that adhere to either an approved code of conduct or an approved certification mechanism (e.g. ISO 27001) may use these tools to demonstrate compliance with the GDPR's security standards

Security of data processing & Data Protection by Design

- GDPR codifies both the concepts of privacy by design and privacy by default.
- A data controller is required to implement appropriate technical and organisational measures both at the time of determination of the means for processing and at the time of the processing itself in order to ensure data protection principles such as data minimisation are met.
- Any such privacy by design measures may include, for example, pseudonymisation or other privacy-enhancing technology.

Security of data processing & Data Protection by Design

- GDPR takes a flexible, risk based, approach to privacy by design.
- In implementing privacy by design a data controller is expected to take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the likelihood and severity of risks to the rights and freedoms of natural persons posed by the processing of their personal data.

Data Protection Governance

- GDPR requires all organisations to implement a wide range of measures to reduce the risk of contravening GDPR requirements and to prove that they take data governance seriously.
- Accountability measures include: Data Protection Impact Assessments, audits, policy reviews, keeping records of processing activities and (potentially) appointing a Data Protection Officer a (“DPO”)
- For those organisations which have not previously designated responsibility and budget for data protection compliance these requirements will impose a heavy burden.

Data Protection Governance

Controllers and processors are free to appoint a DPO but the following must do so:

- Public authorities (with some minor exceptions);
- Any organisation whose core activities require:
  - "regular and systematic monitoring" of data subjects "on a large scale"; or
  - "large scale" processing of sensitive data or criminal records;
- Those obliged to do so by local law (countries such as Germany are likely to fall into this category).

OFFICIAL (ISC)² CHAPTER | BEIJING

Data Protection Governance

DPO tasks include:

- Informing and advising the controller or processor and its employees of their obligations to comply with the GDPR and other data protection laws.
- Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, training data processing staff, and conducting internal audits.
- Advising with regard to data protection impact assessments when required and monitoring its performance.
- Working and cooperating with the controller's or processor's designated supervisory authority and serving as the contact point for the supervisory authority on issues relating to the processing of personal data.
- Being available for inquiries from data subjects on issues relating to data protection practices, withdrawal of consent, the right to be forgotten, and related rights.

International Data transfers

- For organisations active in multiple EU countries, GDPR provides for a system of co-operation and consistency procedures that has been coined as the ‘one stop shop’ mechanism.
- if your organisation conducts “cross-border data processing”, GDPR will require you to work primarily with the supervisory authority based in the same Member State as your main establishment.

International Data transfers

Situations can arise where more than one lead authority can be identified

- A bank has its corporate headquarters in Frankfurt, and all its banking processing activities are organised from there, but its insurance department is located in Vienna.
- *If the establishment in Vienna has the power to decide on all insurance data processing activity and to implement these decisions for the whole EU, then the Austrian supervisory authority would be the lead authority in respect of the cross-border processing of personal data for insurance purposes, and the German authorities would supervise the processing of personal data for banking purposes, wherever the clients are located*.

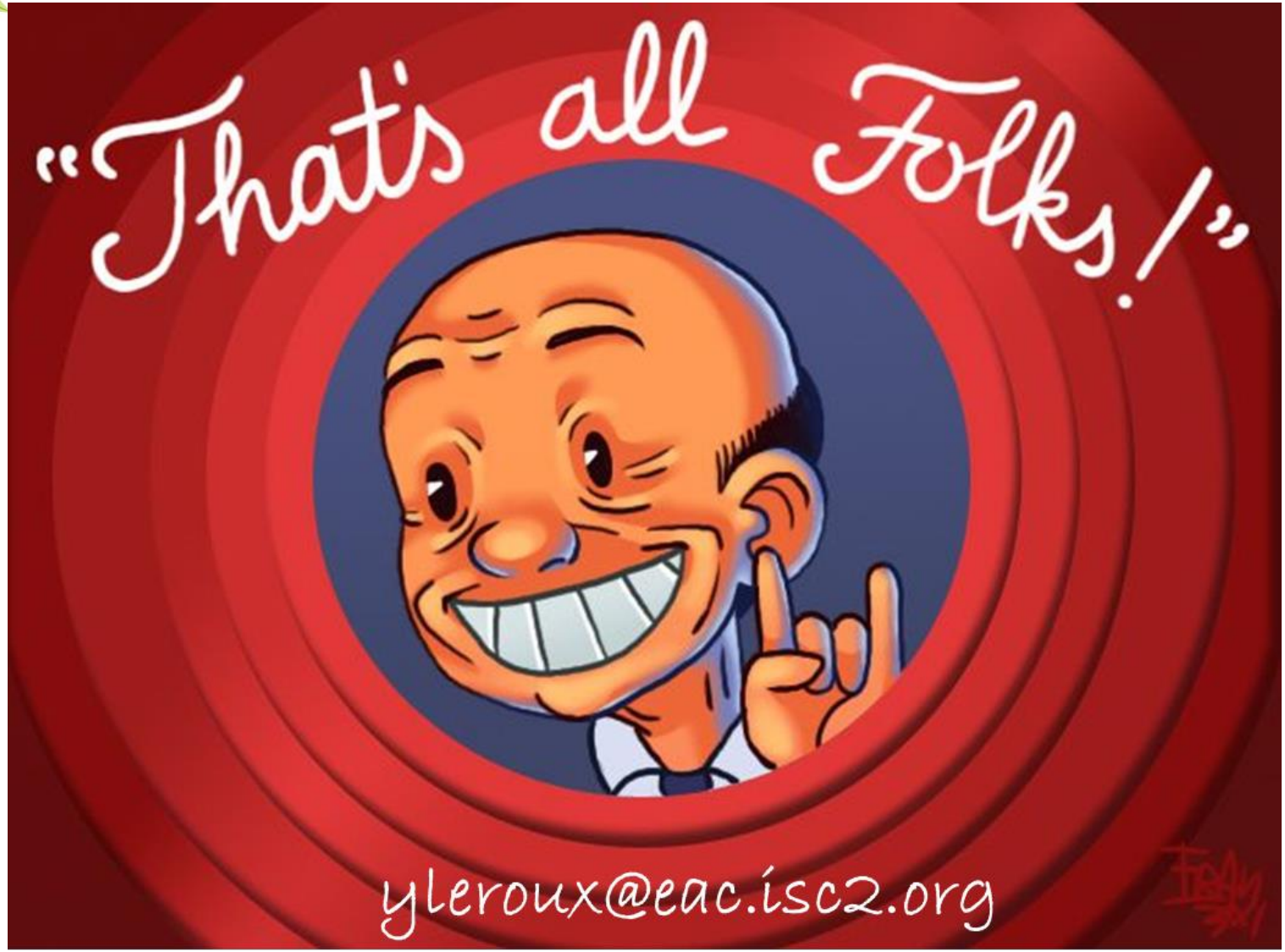
International Data transfers

- GDPR allows for data transfers to countries whose legal regime is deemed by the European Commission to provide for an “adequate” level of personal data protection.
- In the absence of an adequacy decision, transfers are also allowed outside non-EU states under certain circumstances, such as by use of standard contractual clauses or binding corporate rules (BCRs).
- BCRs require approval from DPAs, but once such approval is obtained, individual transfers made under BCRs do not require further approval.
- Derogations are also permitted under limited additional circumstances.

International Data transfers

Organisations operating internationally outside the EEA should:

- review and map their international data flows, including:
  - intra-group data flows
  - extra-group data flows where a EEA group company controller is exporting to a controller or processor outside of the EEA
  - extra-group data flows where a non-EEA group company is importing as a processor or controller
  - consider what existing data transfer mechanisms are in place and whether these continue to be appropriate. Countries that are currently white listed remain so until a Commission review finds otherwise (Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, Uruguay and New Zealand)
  - consider whether BCRs or PBCRs would be a viable option for intra-group data transfers
  - consider putting in place a process for responding to requests for information from non-EEA litigants, regulators or law enforcement agencies and ensure that relevant staff are made aware of such a process
- Ensure export obligations flow down through subcontractor chains and across to other controllers where required



OFFICIAL (ISC)² CHAPTER | BEIJING