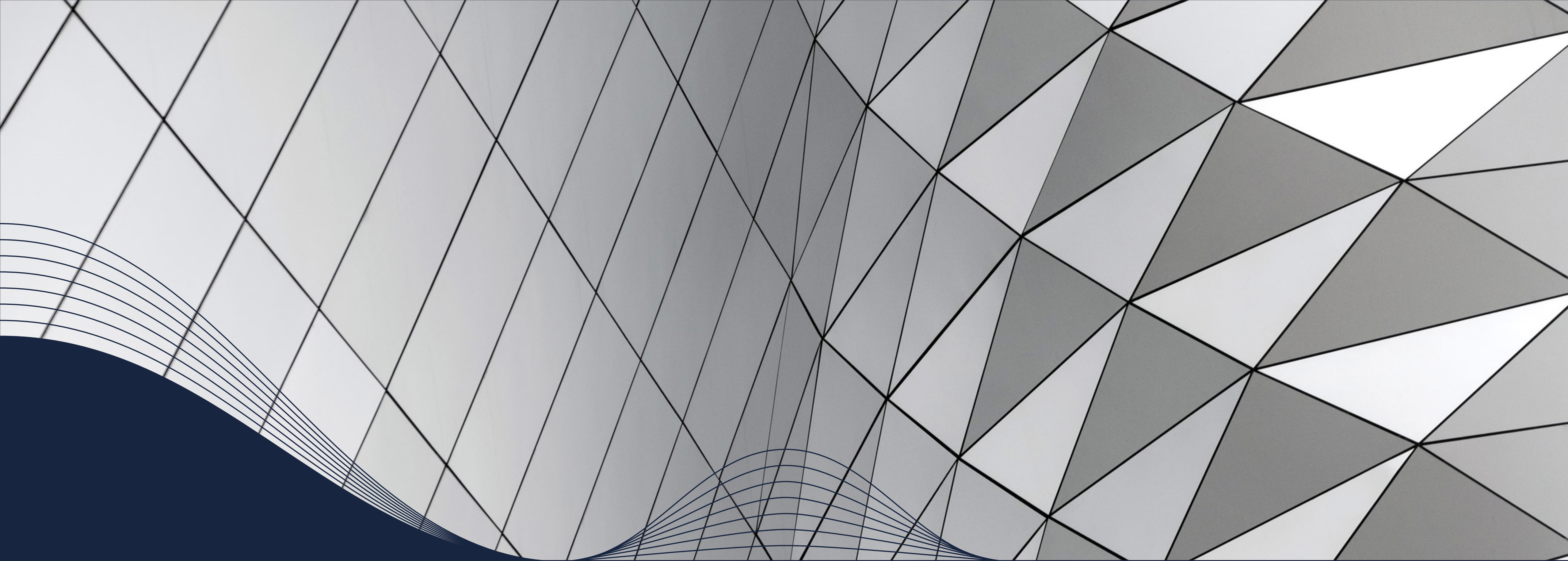
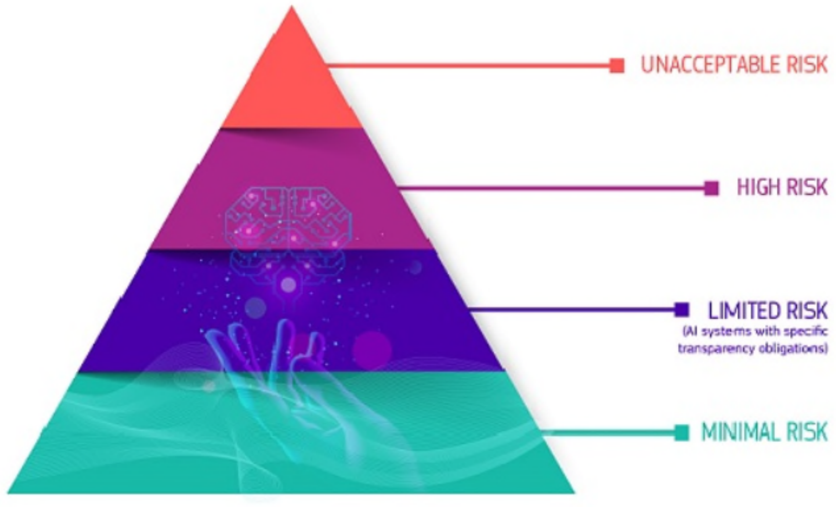


AI Regulation and Data Compliance

EU AI Act proposal

A risk-based approach



Unacceptable risk
All AI systems considered a clear threat to the safety, livelihoods and rights of people will be banned, from social scoring by governments to toys using voice assistance that encourages dangerous behaviour.

High-risk AI systems will be subject to strict obligations before they can be put on the market:

- adequate risk assessment and mitigation systems;
- high quality of the datasets feeding the system to minimise risks and discriminatory outcomes;
- logging of activity to ensure traceability of results;
- detailed documentation providing all information necessary on the system and its purpose for authorities to assess its compliance;
- clear and adequate information to the user;
- appropriate human oversight measures to minimise risk;
- high level of robustness, security and accuracy.

Limited risk
Limited risk refers to AI systems with specific transparency obligations. When using AI systems such as chatbots, users should be aware that they are interacting with a machine so they can take an informed decision to continue or step back.

Minimal or no risk
The proposal allows the free use of minimal-risk AI. This includes applications such as AI-enabled video games or spam filters. The vast majority of AI systems currently used in the EU fall into this category.

EU AI Act proposal

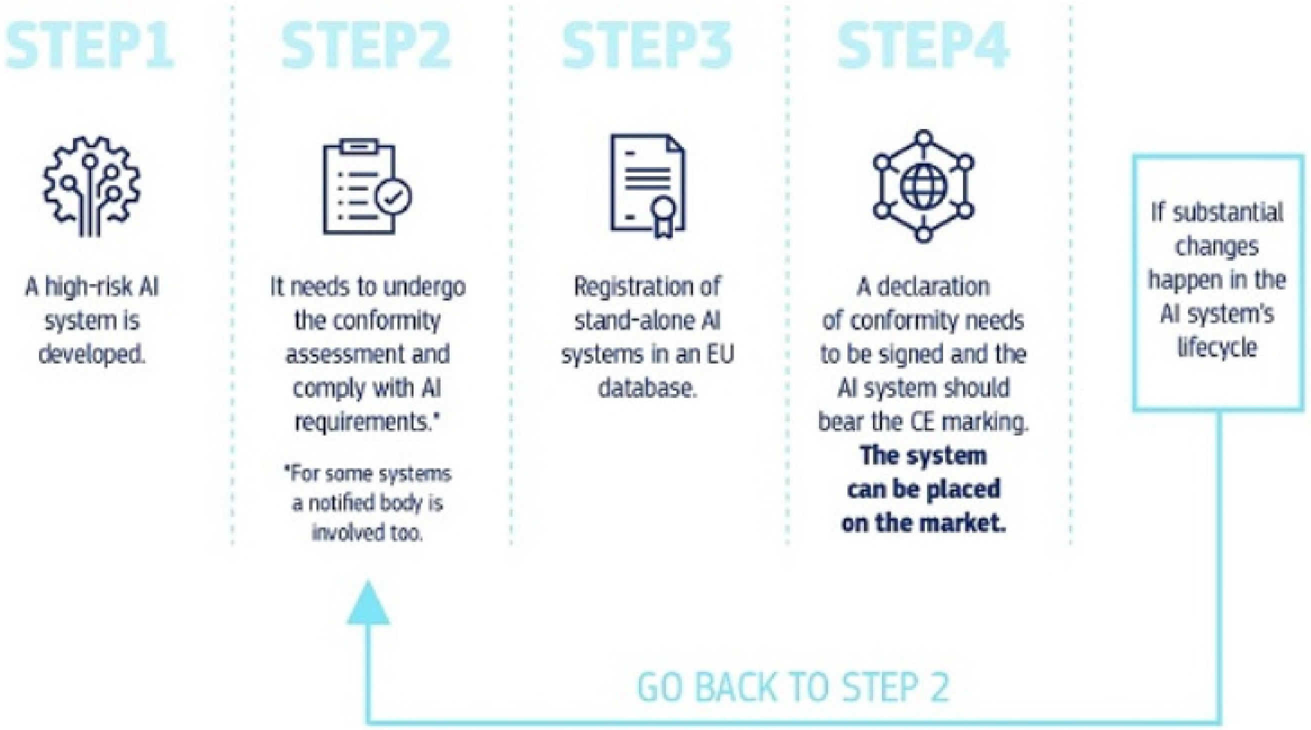
This Regulation applies to:

(a) providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country;

(b) users of AI systems located within the Union;

(c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union.

'Provider' means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge.



STEP1

A high-risk AI system is developed.

STEP2

It needs to undergo the conformity assessment and comply with AI requirements.*

*For some systems a notified body is involved too.

STEP3

Registration of stand-alone AI systems in an EU database.

STEP4

A declaration of conformity needs to be signed and the AI system should bear the CE marking. **The system can be placed on the market.**

If substantial changes happen in the AI system's lifecycle

GO BACK TO STEP 2

How does it all work in practice for providers of high risk AI systems?

EU AI Act proposal

The promotion of AI-driven innovation is **closely linked to the Data Governance Act, the Open Data Directive and other initiatives under the EU strategy for data**, which will establish trusted mechanisms and services for the re-use, sharing and pooling of data that are essential for the development of data-driven AI models of high quality.

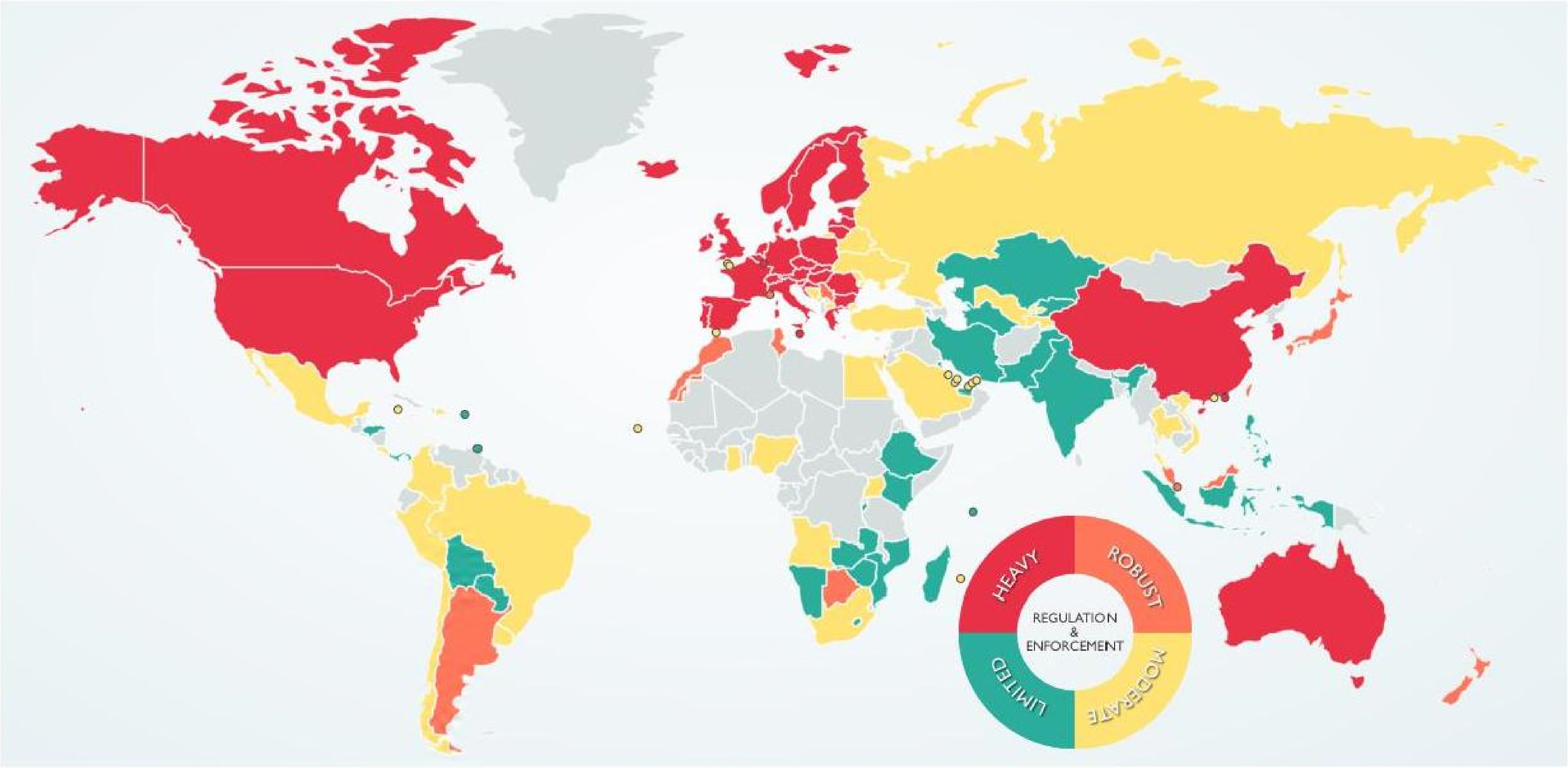
Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular

(a) the relevant design choices;
(b) data collection;
(c) relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation;
(d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent;
(e) a prior assessment of the availability, quantity and suitability of the data sets that are needed;
(f) examination in view of possible biases;
(g) the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed.

Training, validation and testing data sets shall

- be relevant, representative, free of errors and complete;
- take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, behavioural or functional setting within which the highrisk AI system is intended to be used;
- be subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued;

Data privacy heat map



Key personal data compliance obligations

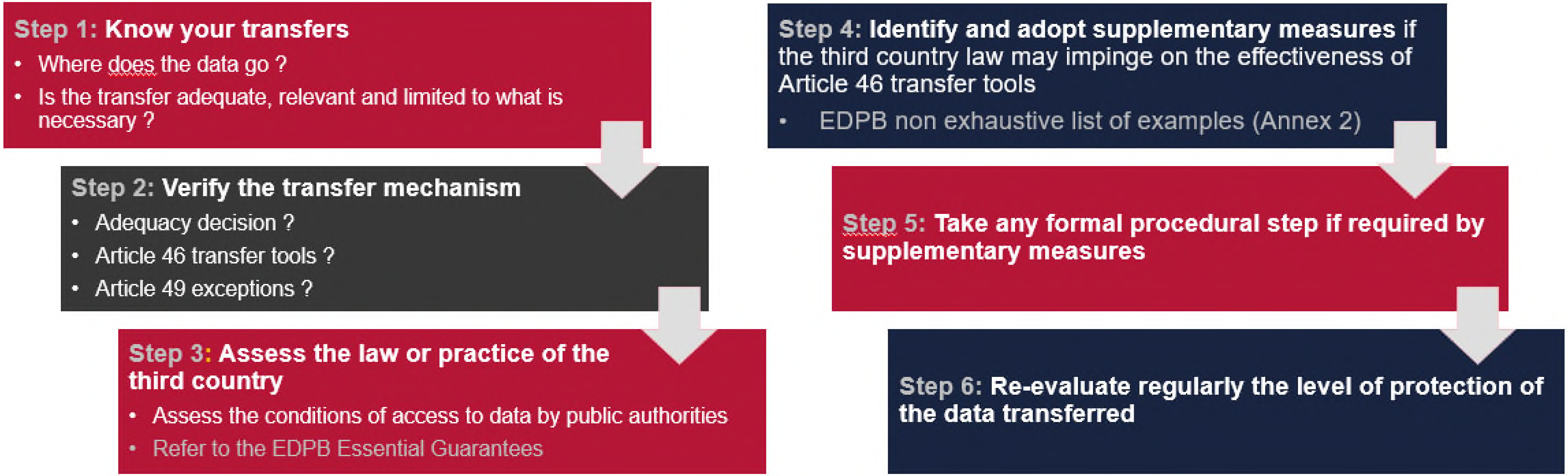
- Collection: privacy notices/consents
- Use
- Transfer and data recipients (C2C and C2P)
- **Cross-border data transfers and data localisation**
- Data minimisation/accuracy/retention
- Data subject rights
- Data breach notification
- Governance
- Data security

EU and UK: Schrems II Case and SCCs

The EDPB Guidelines

10 November 2020 - EDPB adopts recommendations on supplementary measures - submitted to public consultation

6-step process to help assessing third countries' laws and identifying supplementary measures



Step 1: Know your transfers

- Where does the data go ?
- Is the transfer adequate, relevant and limited to what is necessary ?

Step 2: Verify the transfer mechanism

- Adequacy decision ?
- Article 46 transfer tools ?
- Article 49 exceptions ?

Step 3: Assess the law or practice of the third country

- Assess the conditions of access to data by public authorities
- Refer to the EDPB Essential Guarantees

Step 4: Identify and adopt supplementary measures if the third country law may impinge on the effectiveness of Article 46 transfer tools

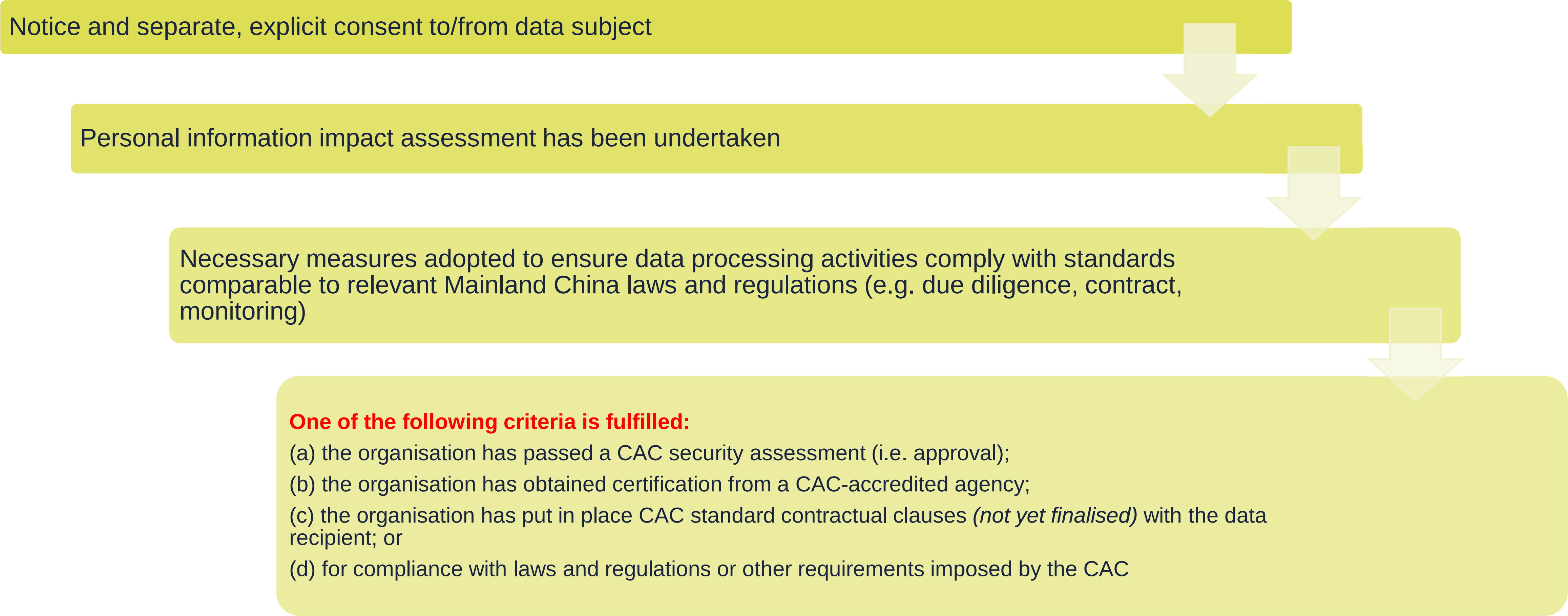
- EDPB non exhaustive list of examples (Annex 2)

Step 5: Take any formal procedural step if required by supplementary measures

Step 6: Re-evaluate regularly the level of protection of the data transferred

Managing Mainland China cross-border data transfer rules

Most organisations may transfer or access **most** personal data outside of Mainland China if:



Notice and separate, explicit consent to/from data subject

Personal information impact assessment has been undertaken

Necessary measures adopted to ensure data processing activities comply with standards comparable to relevant Mainland China laws and regulations (e.g. due diligence, contract, monitoring)

One of the following criteria is fulfilled:

(a) the organisation has passed a CAC security assessment (i.e. approval);

(b) the organisation has obtained certification from a CAC-accredited agency;

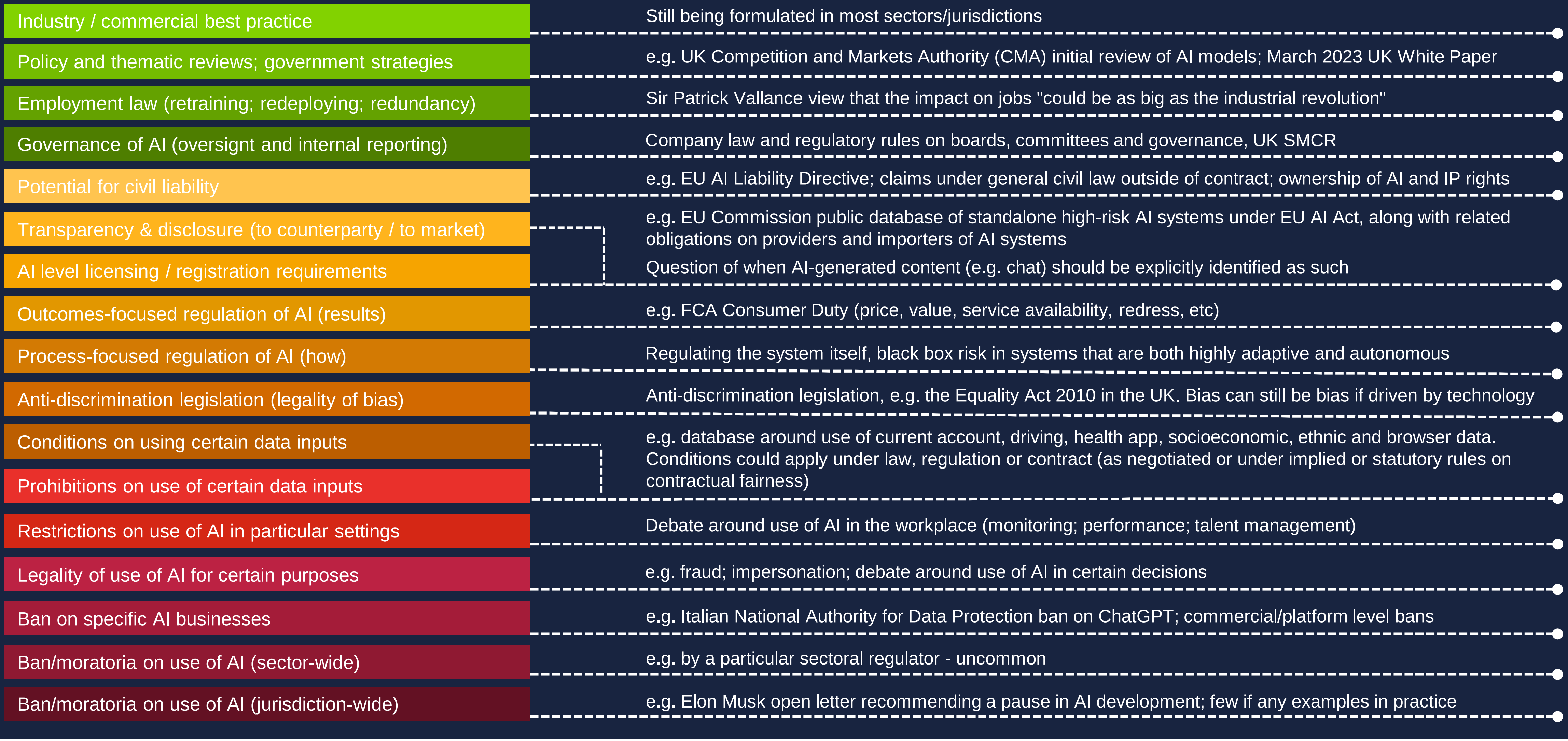
(c) the organisation has put in place CAC standard contractual clauses *(not yet finalised)* with the data recipient; or

(d) for compliance with laws and regulations or other requirements imposed by the CAC

BUT certain (personal and non-personal) data must nonetheless stay in China…

Law, regulation and AI

Types of legal restrictions and their navigability



Industry / commercial best practice	Still being formulated in most sectors/jurisdictions
Policy and thematic reviews; government strategies	e.g. UK Competition and Markets Authority (CMA) initial review of AI models; March 2023 UK White Paper
Employment law (retraining; redeploying; redundancy)	Sir Patrick Vallance view that the impact on jobs "could be as big as the industrial revolution"
Governance of AI (oversight and internal reporting)	Company law and regulatory rules on boards, committees and governance, UK SMCR
Potential for civil liability	e.g. EU AI Liability Directive; claims under general civil law outside of contract; ownership of AI and IP rights
Transparency & disclosure (to counterparty / to market)	e.g. EU Commission public database of standalone high-risk AI systems under EU AI Act, along with related obligations on providers and importers of AI systems Question of when AI-generated content (e.g. chat) should be explicitly identified as such
AI level licensing / registration requirements	
Outcomes-focused regulation of AI (results)	e.g. FCA Consumer Duty (price, value, service availability, redress, etc)
Process-focused regulation of AI (how)	Regulating the system itself, black box risk in systems that are both highly adaptive and autonomous
Anti-discrimination legislation (legality of bias)	Anti-discrimination legislation, e.g. the Equality Act 2010 in the UK. Bias can still be bias if driven by technology
Conditions on using certain data inputs	e.g. database around use of current account, driving, health app, socioeconomic, ethnic and browser data. Conditions could apply under law, regulation or contract (as negotiated or under implied or statutory rules on contractual fairness)
Prohibitions on use of certain data inputs	
Restrictions on use of AI in particular settings	Debate around use of AI in the workplace (monitoring; performance; talent management)
Legality of use of AI for certain purposes	e.g. fraud; impersonation; debate around use of AI in certain decisions
Ban on specific AI businesses	e.g. Italian National Authority for Data Protection ban on ChatGPT; commercial/platform level bans
Ban/moratoria on use of AI (sector-wide)	e.g. by a particular sectoral regulator - uncommon
Ban/moratoria on use of AI (jurisdiction-wide)	e.g. Elon Musk open letter recommending a pause in AI development; few if any examples in practice

DLA Piper AI Report

To help our clients create value from AI, DLA Piper have undergone market research across multiple sectors and locations to showcase the varying attitudes and maturity levels in implementing AI, exploring the balance between AI value creation and ethical values, focussing on how organizations can leverage AI responsibly, safely and commercially. The report will be released in September and clients can pre-register now.

For further information, please contact:

Amanda Ge, Of Counsel
DLA Piper Beijing

E: amanda.ge@dlapiper.com

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication. This may qualify as “Lawyer Advertising” requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

DLA PIPER