Data Protection and Connected Cars

EU and France view

Christine (Yaotian) Chai

Aurilex Law Firm

Attorney-at-Law - Ph.D. in Law - CIPP/E

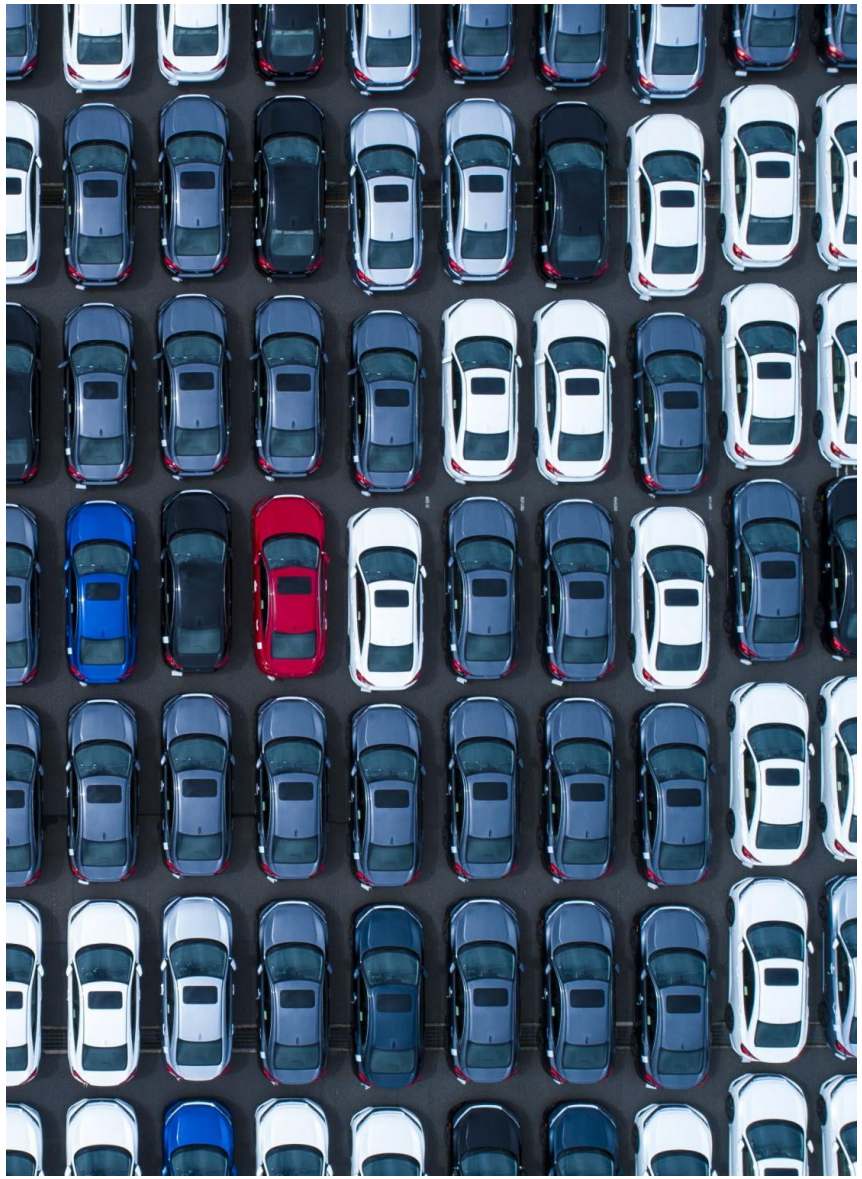
yaotian.chai@aurilex.com

Wechat:

14.03.2024

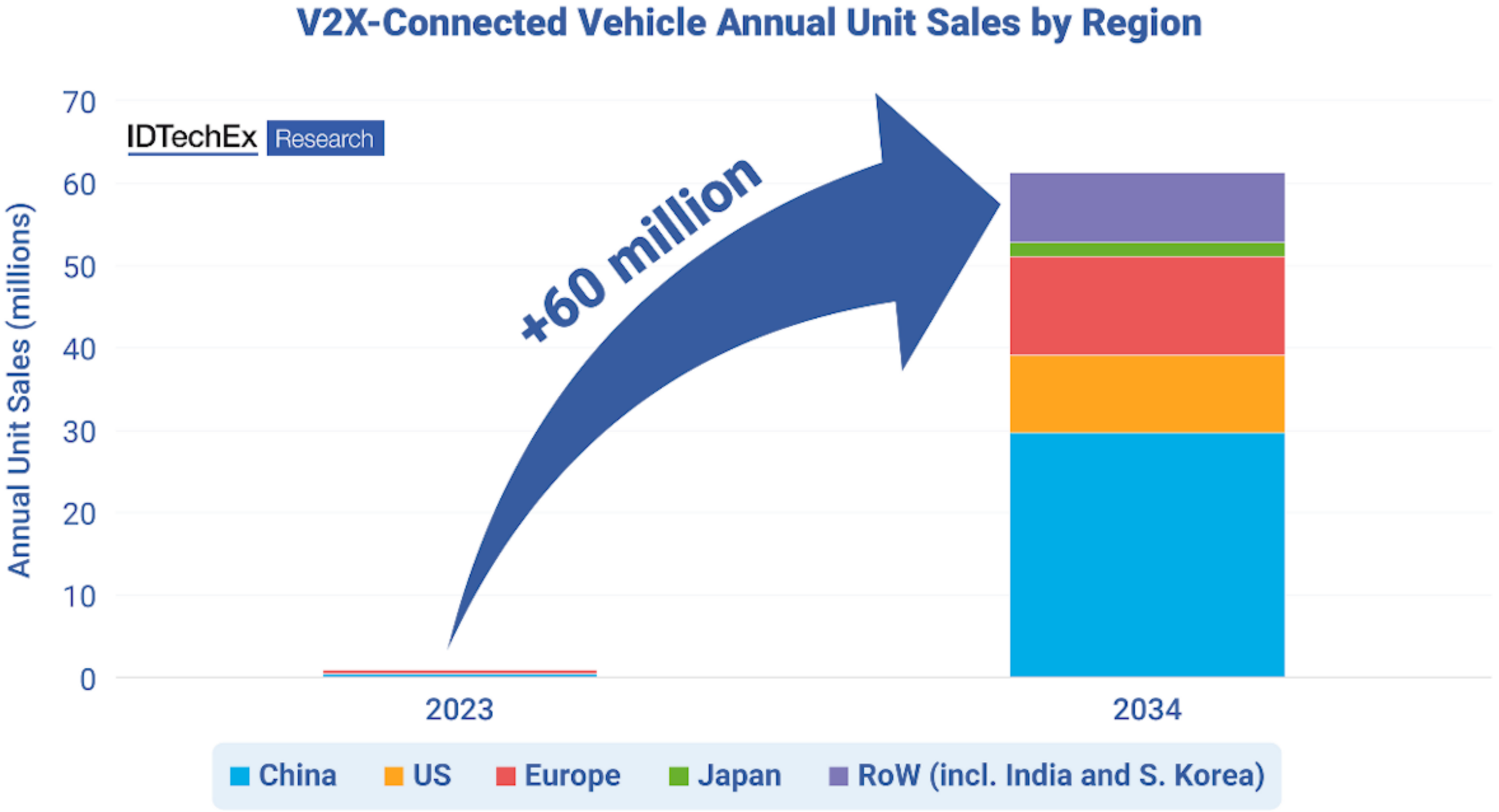
Outline

1. Introduction
2. Types of personal data in connected cars
3. Legal landscape in the EU and in France
4. Transfer of personal data outside the EU



1. Introduction

- The Europe-connected cars market revenue by the end of **2021** was **US$ 10.2 Billion**.
- The Europe-connected cars market is expected to reach **US$ 49.7 Billion** by **2032**.
- By **2025**, partial and conditional automation vehicles are expected to account for **over 50% of new vehicle sales** in China.
- By **2025**, **more than 470 million connected vehicles** are expected to be on the roads of Europe, the United States and China.
- China is set to add **30 million** new connected vehicles to the road every year by **2034.**

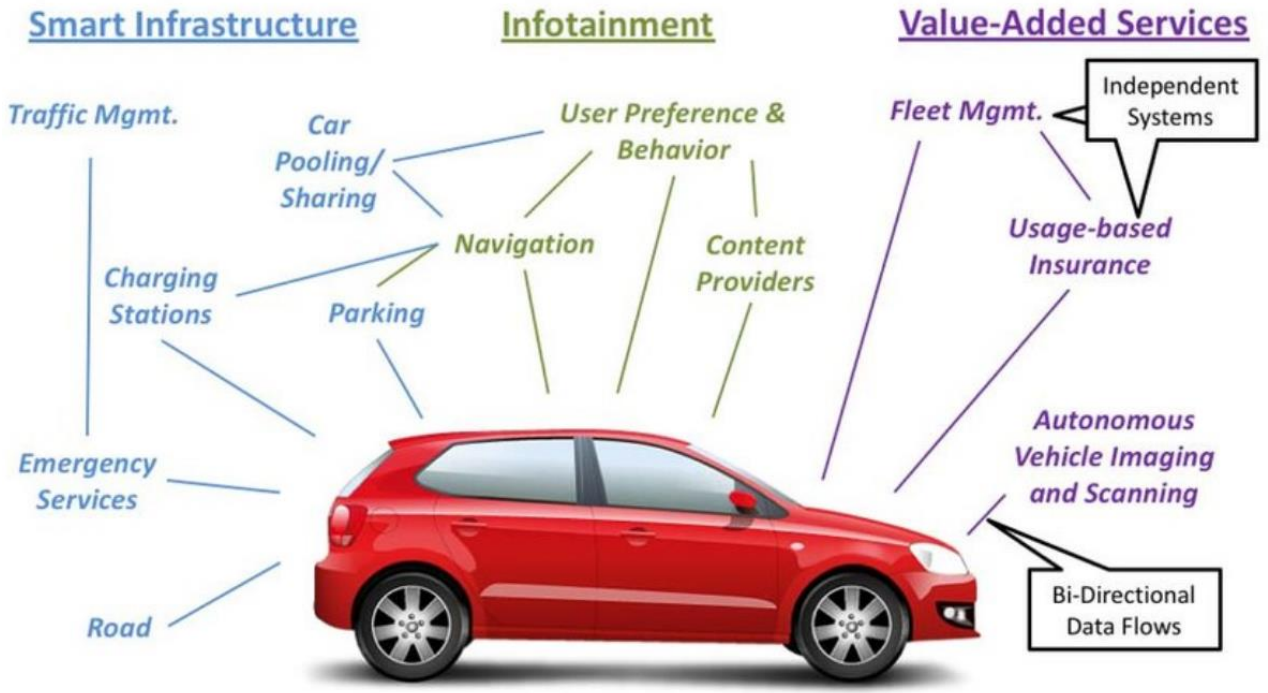


Annual V2X-Connected Vehicle Unit Sales are expected to exceed 60 million units by 2034. Source: IDTechEx

To whom belongs the personal data in connected cars?

2. Types of personal data in connected cars

- vehicle condition
- geolocation
- life on board
- journeys made
- places regularly visited
- driving style
- driver’s eye movements, pulse, biometric data…



Categories of personal data

- Reveal life habits of data subjects
- Place of work, residence
- Leisure
- Religion
- Sexual orientation
- Data minimization: when the movement detection is sufficient, no need of localization.

Location data

- Sensitive data in the sense of Art. 9 GDPR
- Data security
- The number of authentication attempts should be limited.
- Encryption of the data stored in the vehicle.
- The raw data used to make up the biometric template and for user authentication are processed in real time without ever being stored, even locally.

Biometric data

- Data indicating that the vehicle crossed a white line, the instantaneous speed of a vehicle combined with precise location data, etc.
- Safeguard provided by Art. 10 of the GDPR: Any comprehensive register of criminal convictions shall be kept only under the control of official authority

Data relating to traffic violations

3. Legal lanscape in the EU and in France

3.1. EDPB Guidelines on connected vehicles (March 2021)

Aimed at: car manufacturers, providers of corresponding services, motor vehicle insurers.

Consent remains the essential legal basis for the processing of vehicle data.

Sensible personal data: position data, biometric data and data that provide information about possible violations of the law, should only be possible in very restrictive conditions.

Privacy by design: The GDPR requirements should be taken into account already at the stage of development of the corresponding technologies.

High standards of IT security in the connected vehicle

3.2 2017 CNIL compliance pack for connected vehicles and personal data

- **Scenario 1 "IN => IN"**: data collected in the vehicle remains in the vehicle without being transmitted to the service provider.
- Example: an eco-driving solution that processes data directly in the vehicle to display eco-driving advice in real time on the on-board computer.
- **Scenario no. 2 "IN => OUT**": data collected in the vehicle is transmitted externally to provide a service to the person concerned.
- Example: "Pay as you drive" contract with an insurance company.
- **Scenario no. 3 "IN => OUT => IN"**: data collected in the vehicle is transmitted to the outside world to trigger an automatic action in the vehicle.
- Example: dynamic "Infotrafic" with calculation of a new route following an incident on the road

2017 CNIL compliance pack for connected vehicles and personal data

All data that can be linked to an identified or identifiable natural person, in particular via the number plate or the vehicle's serial number, is personal data protected by the French Data Protection Act and the GDPR. For example, data relating to journeys made, the state of use of parts, the dates of roadworthiness tests, the number of kilometers driven or driving style is personal data when it can be linked to a natural person.

A "privacy by design" approach to data protection should be favoured. This can take the form of setting up easily configurable dashboards, so as to guarantee that users have control over their data.

The CNIL is encouraging players to opt for the IN => IN scenario, which involves data being processed locally, in the vehicle, without being transmitted to the service provider.

Compliance Club on connected vehicles and mobility

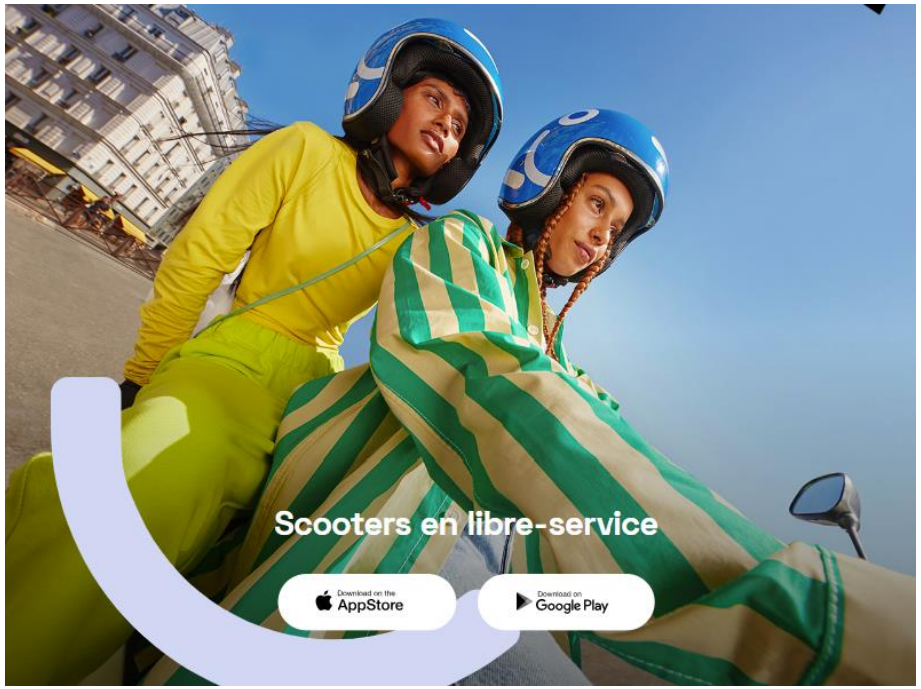
On 1 March 2023, the CNIL launched a "compliance club" dedicated to connected mobility, designed to provide a forum for players in the sector to discuss the challenges of data collection by "intelligent" vehicles. It is intended to provide "concrete and appropriate responses" to the challenge of "reconciling innovation and the protection of privacy".

UBEEQO fined 175 000 euros by CNIL on 21/07/2022

- During the rental of a vehicle by a private individual, UBEEQO collected data relating to the geolocation of the rented vehicle **every 500 meters** when the vehicle was in motion, **when the engine was switched on and off** or **when the doors were opened and closed**. In addition, the company kept a log of some of the geolocation data collected, for an excessive length of time.
- Violation of the **principle of minimization of data**
- Violation of the **principle of storage of personal data for a reasonable period**
- Violation of the **obligation of providing information**

CITYSCOOT fined 125 000 euros by CNIL on 28/03/2023

- In 2020, the CNIL focused some of its controls on a number of priority areas of everyday concern to the French, including **geolocation** for local services.
- During the inspection of CITYSCOOTER, the CNIL noted that during the rental of a scooter by a private individual, the company collected **data relating to the geolocation of the vehicle every 30 seconds**.
- In addition, the company kept a record of these journeys.
- Violation of the data minimization principle
- Failure to inform users and obtain their consent before recording and reading information on their personal equipment



4. Transfer of personal data outside the EU

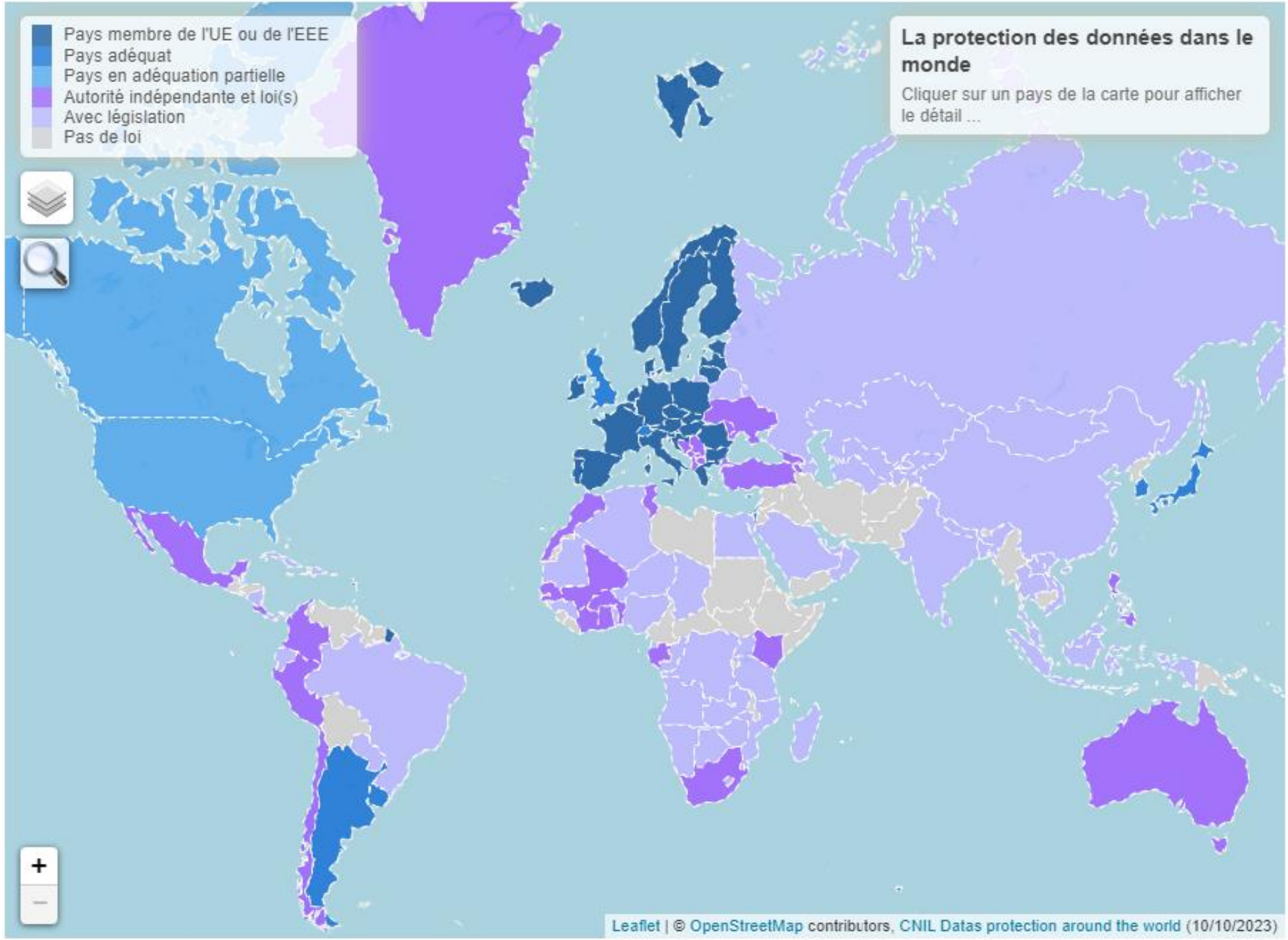
The cross-border flow of personal data requires one of the following conditions to be met:

Transfer inside the EU/EEA.

European Commission recognizes the country's level of personal data protection as equivalent to that of the EU（Adequacy decision， Art. 45 GDPR ）。

Guarantees: BCR, Standard Contractual Clauses, Certification (Art. 46, 47 GDPR）。

Explicit consent of the data subject to the transfer of his/her personal data in the event that he/she is informed of the risk of lack of equivalent decisions and appropriate safeguards（Article 49-1 a) GDPR）。


Pays membre de l'UE ou de l'EEE
Pays adéquat
Pays en adéquation partielle
Autorité indépendante et loi(s)
Avec législation
Pas de loi
La protection des données dans le monde
Cliquer sur un pays de la carte pour afficher le détail ...
+
−
Leaflet | © OpenStreetMap contributors, CNIL Datas protection around the world (10/10/2023)

New legal framework for data flows out of the EU

- The European Data Protection Board published on 10 November 2020 two guidelines on compliance with cross-border flows of personal data in the EU:

  - **Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data** (effective 18 June 2021): is used to test whether there are relevant safeguards in place for the flow of personal data out of the EU to ensure that there is no reduction in the level of protection of personal data. The appendix to the guideline lists additional technical or organisational measures that can be taken if the data flows do not maintain the same level of protection as in the EU.

  - **Recommendations 02/2020 on the European Essential Guarantees for surveillance measures**: for testing whether the legislation of destination countries affects the effectiveness of data flow safeguards.

New legal framework for data flows out of the EU

- The European Commission's new standard contractual clauses, which enter into force on 24 June 2021, are divided into two sets, namely data processing agreements between data controllers and processors in the EU, and data processing agreements for the flow of personal data out of the EU.
- From 27 December 2022 onwards, the use of the old Standard Contractual Clauses no longer guarantees an equivalent level of protection.

Thank you for your attention!

Christine (Yaotian) Chai
yaotian.chai@aurilex.com