

# European, Chinese and US regulatory approaches to personal data transfer and monetization

April 19, 2021

## GDPR, PIPL and CCPA

In October 2020, China unveiled its Personal Information Protection Law (“**PIPL**”), the draft of a set of rules aimed at regulating privacy law.

PIPL is meant to complete China’s regulatory framework on privacy, which was launched with the 2016 Cybersecurity Law. China, like other major world powers, is fully aware that “information is power” and to be up to date as situations develop, means for them to be able not only to react quickly but also to control the nature of the information.

PIPL looks like a “little sister” to EU Regulation 2016/679 (“**GDPR**”). Is it perhaps that China ran for cover after the Schrems II ruling? The EU court’s decision, in fact, is not only of concern for its immediate effects on data flows to the United States, but also for its repercussions in other third countries too, such as China. In order to assess whether China is a country with sufficient guarantees of adequacy (i.e. with an essentially equivalent level of protection of personal data to that guaranteed within the EU), market players are being asked to carry out an analysis that should really be carried out by regulatory authorities. Hence, the absence of ad-hoc privacy legislation may be a deterrent for data transfers to China. One may thus wonder whether this rush to create a “Mandarin GDPR” is more like a rush to avert a blockage of data transfers.

The **CCPA**, or California Consumer Privacy Act, is a piece of legislation adopted by the State of California in 2018. Similar to the GDPR, the CCPA’s scope of application also extends beyond the territorial limits of the Golden State. However, determining whether or not the information collected falls within its scope may be much more complicated for businesses, given that the definition of “resident” set out in the legislation is very broad and includes any individual who is in California for other than temporary or transitory purposes, and any individual domiciled in California who is momentarily or transitorily out of the state. While the CCPA represents a first step in the process of bringing California’s legislation closer to the European matrix, the state’s data protection legislative framework is to be further strengthened with the entry into force of the California Privacy Rights Act of 2020 (“**CPRA**”), scheduled for January 2023.

## Data transfer and monetization for legislators: Europe, China and the US compared

There is one aspect that, in particular, reveals what the economic interests that lie behind the processing of personal data may be, and that is their transfer for monetization purposes: i.e., the possibility to share data relating to data subjects as an asset with an economic value. In principle, the limits to the exploitation of personal data for economic

purposes will show to what the extent a market is inclined to validate the economic interests of its players, even at the risk of compressing fundamental rights such as the right to privacy, But how inclined are the above mentioned regulations to allow the economic exploitation of personal data?

## GDPR: a restrictive approach

The most frequent use of personal data for monetization purposes is normally linked to marketing purposes (possibly throughout profiling); in this case, generally, the data subject's consent is required.

Having said that, we should answer the question: is it possible to process personal data for monetization per se? Two main – and opposing – interpretations of GDPR can be found: according to some, the right to the protection of personal data cannot be conceived as a transferable asset in exchange for a consideration, given it is a fundamental right; according to others, however, the data could well be associated with an economic value, on the basis of the fact that the very Article 1(3) of GDPR provides that “the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data”. So far, the Italian Data Protection Authority (“**Garante**”) does not seem very fond of such a liberal thesis – and the same goes for the European Data Protection Board (“**EDPB**”), which in its Guidelines 2/2019 has highlighted that “[...] personal data cannot be considered as a trade-able commodity”.

In light of these considerations, even if we were to agree to the more restrictive approach, a distinction ought to be made: It is one thing to offer an economic consideration to the data subject in exchange for his/her personal data - in this case, since the right to privacy is a fundamental right, it seems logical to expect that the data subject cannot freely dispose of it outside of the possibilities allowed by law; it is another thing to treat personal data (as long as they are lawfully put on the market) as assets that can henceforth circulate and be given an economic value.

## PIPL: a work-in-progress approach

Under its Article 24, the PIPL seems to convey that the transfer of data to third parties normally requires the data subject's consent. The question arises as to whether the transfer can also be based on other legal grounds. While the PIPL appears very protective and restrictive as far as data circulation is concerned, on the other hand the rationale behind this remains unclear. With China being an economic power-house, it is curious to say the least that it adopts such a restrictive approach on free movement of data, thus reducing the potential of such an economic resource.

## CCPA: an opt-out centered mechanism

Among the most delicate aspects of California's data protection regulation is undoubtedly the 'sale' of personal data. But what is the real meaning of the term 'sale'? The definition provided by the CCPA itself includes any activity of “selling, renting, releasing, disclosing, disseminating, making available, transfer-ring, or otherwise communicating orally, in writing or by electronic or other means, a consumer's perso-nal information by the business to another business or a third party for a monetary or other valuable consideration”. It is evident that the scope of it is very broad, and it basically includes any communication of personal data carried out in exchange for any kind of “valuable consideration”.

If we think of digital marketing, for example, sharing personal data for the purpose of buying or selling a personalized advert would certainly constitute a “sale” under the CCPA. The approach thereby adopted seems thus to reflect the overseas approach, which is typically focused on the profit gained from pro-TECTING private property.

On the other hand, and poles apart with respect to the GDPR provisions, the CCPA adopts an opt-out based

approach, giving the customer the right to ask companies to stop selling his/her personal data. In the wake of this, companies are required to make available a “Do not sell my personal information” link. In addition, the CCPA limits temporarily the validity of the consumer’s choice to 12 months, after which the company may ask him/her again to provide his/her authorization to sell his/her personal data. This approach too is very different from the one adopted by the European regulators – including the UK ICO and the Garante – according to which a communication sent to the data subject for the purposes of requesting his/her consent to receive commercial communications is usually considered a commercial communication itself.

Do you have more questions, or do you want to share your thoughts on this article? Contact our Dentons Italy TMT Team at [tmtbites.italy@dentons.com](mailto:tmtbites.italy@dentons.com), and do not forget to sign up to our TMT Bites Newsletter and to follow us!

This article has been co-authored by Fabia Cairoli ([Fabia.Cairoli@dentons.com](mailto:Fabia.Cairoli@dentons.com)) and Flavia Messina ([Flavia.Messina@dentons.com](mailto:Flavia.Messina@dentons.com))

## Your Key Contacts



**Fabia Cairoli**

Associate, Milan

D +39 02 726 268 00

M + 39 347 28 61 698

[fabia.cairoli@dentons.com](mailto:fabia.cairoli@dentons.com)



**Flavia Messina**

Associate, Milan

D +39 02 726 268 00

[flavia.messina@dentons.com](mailto:flavia.messina@dentons.com)