Gestione dei trasferimenti di dati tra UE e Cina

Con la progressiva digitalizzazione dei processi economici, le imprese operano sempre più spesso a livello internazionale, gestendo flussi di dati personali tra diverse giurisdizioni. In questo articolo ci focalizziamo in particolare sui trasferimenti di dati tra Unione europea (UE) e Repubblica Popolare Cinese (RPC), due sistemi – disciplinati rispettivamente dal Regolamento generale sulla protezione dei dati (GDPR) e dalla Legge sulla protezione delle informazioni personali (PIPL) – che, pur condividendo l'obiettivo comune di tutelare i dati personali degli individui, presentano differenze significative nelle modalità di applicazione.
Comprendere come queste due normative si intrecciano è quindi fondamentale per le organizzazioni che trasferiscono dati tra l'UE e la RPC.

Principi comuni, sistemi differenti
A un primo sguardo, il GDPR e la PIPL sembrano avere diverse similitudini. Entrambe hanno portata extraterritoriale, applicandosi anche a trattamenti svolti al di fuori del proprio territorio quando riguardano dati personali di cittadini europei o cinesi.
Tuttavia, gli approcci delle due normative differiscono: il GDPR si fonda sul principio di accountability del titolare del trattamento e sulla supervisione da parte di autorità indipendenti, mentre il PIPL riflette un modello maggiormente incentrato sulla governance dei dati, in linea con il quadro regolatorio della RPC in materia di sicurezza e sovranità dei dati.

Trasferimento transfrontaliero di dati personali
Ai sensi del GDPR, il trasferimento di dati personali al di fuori dell'UE è possibile solo nel rispetto delle condizioni stabilite nel Capitolo V del Regolamento. Tra questi rientrano:

- una decisione di adeguatezza della Commissione europea, che riconosce al Paese di destinazione un livello di tutela sostanzialmente equivalente a quello europeo;
- l'adozione di garanzie appropriate, come le Clausole contrattuali standard (SCCs) o le Norme vincolanti d'impresa (BCRs);
- oppure, in via eccezionale, alcune deroghe specifiche, come il consenso esplicito.

Poiché attualmente non esiste una decisione di adeguatezza tra l'UE e la RPC, i trasferimenti di dati tra UE e Cina si basano generalmente sulle SCCs, precedute da

una valutazione d'impatto sul trasferimento (TIA). Tale documento valuta se la normativa locale – in particolare in materia di accesso ai dati da parte delle autorità governative – possa compromettere il livello di tutela previsto dal GDPR.

Un esempio emblematico in tal senso è rappresentato dagli Stati Uniti, che negli anni hanno affrontato diverse criticità in materia di trasferimenti di dati personali.

La Corte di giustizia dell'UE (CGEU), infatti, con le note sentenze Schrems I e Schrems II, ha infatti invalidato le precedenti decisioni di adeguatezza proprio a causa delle criticità legate all'accesso dei dati da parte delle autorità statunitensi.

In tal senso, nonostante l'adozione del nuovo EU–US Data Privacy Framework, il dibattito sull'effettivo livello di protezione dei dati negli Stati Uniti resta tuttora aperto, a conferma della complessità che caratterizza la disciplina dei trasferimenti transfrontalieri di dati.

La PIPL, al contrario, adotta un approccio differente. Qualsiasi azienda che trasferisca informazioni personali al di fuori della Cina può essere tenuta, sulla base di specifici parametri e soglie, a:

- sottoporsi a una valutazione di sicurezza da parte della Cyberspace Administration of China (CAC);
- sottoscrivere e depositare un contratto standard presso la CAC; o
- ottenere una certificazione da parte un ente accreditato.

Tuttavia, in alcuni casi possono trovare applicazione esenzioni o procedure semplificate. Ad esempio, alcuni trasferimenti di dati infragruppo effettuati per finalità di gestione delle risorse umane o di amministrazione interna possono non essere soggetti alle disposizioni previste per il trasferimento di dati.

Inoltre, per alcune categorie di operatori – in particolare per chi gestisce infrastrutture informatiche critiche (CII) o tratta grandi quantità di dati – permane l'obbligo di localizzazione dei dati. Ciò significa che le informazioni personali devono essere conservate all'interno del territorio cinese, salvo specifiche circostanze.

Implicazioni pratiche per le imprese multinazionali

Per i gruppi multinazionali che operano in entrambi i mercati, conciliare i requisiti del GDPR e della PIPL può risultare complesso.

Le imprese devono coordinare il proprio modello organizzativo privacy, le procedure interne, le informative privacy e così via, gestendo al contempo i rapporti contrattuali che si estendono su più giurisdizioni e i potenziali rischi di accesso ai dati da parte delle autorità pubbliche. Allo stesso modo, devono considerare il rischio di violazioni dei dati personali, anche nel contesto dei trasferimenti transfrontalieri di dati, e

garantire l’adozione di misure tecniche e organizzative adeguate a prevenirne o mitigarne gli effetti.
Spesso ciò comporta la creazione di sistemi di compliance paralleli, con processi documentali e adempimenti distinti per ciascun ordinamento.

Nonostante le loro differenze, GDPR e PIPL mostrano una convergenza crescente attorno a valori come trasparenza, accountability e sicurezza.
Per le multinazionali, essere già conformi a uno dei due framework può costituire una base solida per adeguarsi anche all’altro. I principi di privacy by design, liceità del trattamento e governance dei dati stanno infatti diventando standard globali condivisi. Anche in un quadro normativo complesso, un approccio proattivo e integrato può fare la differenza. Il supporto di professionisti in entrambe le giurisdizioni consente alle imprese di operare in modo conforme, sicuro e competitivo su scala internazionale.

Managing EU–China Data Transfers

With the progressive digitalization of economic activities, companies increasingly operate on an international level, managing personal data flows across multiple jurisdictions.

In this article, we focus specifically on data transfers between the European union (EU) and the People's Republic of China (PRC) – two legal systems, governed respectively by the General Data Protection Regulation (GDPR) and the Personal Information Protection Law (PIPL) – which, while sharing the common goal of protecting individuals' personal data, differ significantly in their implementation and enforcement approaches. Understanding how these two frameworks interact is therefore essential for organizations transferring data between the EU and the PRC.

Converging principles, diverging systems

At first glance, the GDPR and the PIPL seem to share many similarities. Both GDPR and PIPL have extraterritorial reach, applying to processing activities outside their territories when the personal data of EU or Chinese individuals is involved.
However, their approaches differ: the GDPR is based on the data controller's accountability and supervisory oversight, while the PIPL reflects a model more centered on data governance, consistent with PRC's regulatory framework on data security and sovereignty.

Cross-border data transfer

Under the GDPR, the transfer of personal data outside the EU is only possible in compliance with the conditions set out in Chapter V of the Regulation. These include:

- a formal adequacy decision by the European Commission, confirming that the destination country ensures a level of protection essentially equivalent to the EU's;
- appropriate safeguards, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs);
- or, in exceptional cases, specific derogations, such as explicit consent.

As there is currently no adequacy decision between the EU and the PRC, data transfers between the EU and PRC generally rely on SCCs, preceded by a Transfer Impact Assessment (TIA). This document evaluates whether local laws – particularly

those on government access – could compromise the protection granted to EU personal data.

A pivotal case in this regard is the United States, which over the years has faced several challenges concerning the transfer of personal data.

The Court of Justice of the European Union (CJEU), through the well-known Schrems I and Schrems II judgments, invalidated the previous adequacy decisions due to concerns related to the access of personal data by U.S. public authorities.

In this sense, despite the adoption of the new EU–US Data Privacy Framework, the debate over the actual level of data protection in the United States remains open, confirming the inherent complexity of the cross-border data transfer regime.

The PIPL, on the other hand, takes a different approach. Any company transferring personal information outside China may be required, based on specific parameters and thresholds, to:

- undergo a security assessment by the Cyberspace Administration of China (CAC);
- sign and file a standard contract to the CAC; or
- obtain certification from an approved entity.

However, certain exemptions or simplified procedures may apply. For example, some intra-group data transfers carried out for HR management or internal administrative purposes may not be subject to the provisions for data transfers.

Moreover, for certain categories of operators – such as those managing Critical Information Infrastructure (CII) or handling large volumes of data – data localization remains mandatory. This means that personal information must be stored within China, unless specific circumstances apply.

Practical implications for multinational companies

For multinational groups active in both markets, aligning GDPR and PIPL requirements can be challenging.

Companies must coordinate their privacy organizational model, internal procedures, privacy notices, and so on, while also managing contractual chains across jurisdictions and addressing potential government-access risks. They should likewise consider the risk of data breaches, including those that may occur in the context of cross-border data transfers, and ensure that adequate technical and organizational measures are in place to mitigate such events.

This often leads to the creation of dual compliance frameworks, with distinct documentation and obligations in each region.

However, despite their differences, GDPR and PIPL show a growing convergence around transparency, accountability, and security.

Therefore, for multinational companies, achieving compliance in one framework can significantly facilitate alignment with the other. The principles of privacy-by-design, lawful processing, and robust governance are increasingly universal. Even within a complex regulatory framework, a proactive and integrated approach can make a real difference. The support of professionals familiar with both jurisdictions enables companies to operate in a compliant, secure, and competitive manner on an international scale.