OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Monthly Roundup

Giugno 2023

MONTHLY ROUNDUP

Giugno 2023

I principali aggiornamenti in materia di TMT & Data Protection del mese

---

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

Provvedimenti del Garante Privacy

- Fidelity Card: il Garante Privacy sanziona il Gruppo Benetton [Link]
- Garante: stop al web scraping per formare elenchi telefonici [Link]
- Garante privacy: illecite le email pubblicitarie senza consenso [Link]

Provvedimenti EDPB

- Guidelines 04/2022 on the calculation of administrative fines under the GDPR [Link]

PRINCIPALI AGGIORNAMENTI

- EDPB Guidelines on the calculation of administrative fines: a useful tool for assessing the economic risks of violations
- GDPR e PIPL: similitudini e differenze
- China released the first guidelines for the submission of the standard contract to transfer personal information outside the borders of the People's Republic of China

EDPB Guidelines on the calculation of administrative fines: a useful tool for assessing the economic risks of violations

During its latest plenary, on 24 May 2023, the European Data Protection Board ("**EDPB**") adopted a final version of the **Guidelines on the calculation of administrative fines following public consultation** (the "**Guidelines**"). These Guidelines aim to harmonise the methodology data protection authorities ("**DPAs**") use to calculate fines and include harmonised "starting points". Hereby, three elements are considered: (i) the categorisation of infringements by nature, (ii) the seriousness of the infringement and (iii) the turnover of a business.

The Guidelines set out a 5-step methodology, taking into account the number of instances of sanctionable conduct, possibly resulting in multiple infringements; the starting point for the calculation of the fine; aggravating or mitigating factors; legal maximums of fines; and the requirements of effectiveness, dissuasiveness and proportionality.

The content of the Guidelines and the related methodology had already been analysed, before the conclusion of the public consultation phase and the adoption of the final version, in a previous contribution available **here**.

Moreover, the final version of the Guidelines includes a **reference table summarising the methodology with a number of starting points for the calculation of fines**, illustrating the range for the starting amount based on three level of seriousness (low level, medium level and high level) correlating with the range for the starting amount after adjustment applied for the size of the company, as well as two examples of practical application, for illustration purposes only and to be read in conjunction with the Guidelines.

As also specified by the EDPB, the reference table shall also be read taking into consideration that the calculation of an administrative fine is no purely mathematical exercise, and that real life cases, practice and DPAs case law will inevitably lead to a further sharpening of the starting points included in the table.

To that end, the Guidelines mention that the table and the numbers therein remain under close review by the EDPB and will be adapted if needed and the numbers constitute the starting points for further calculation and not fixed amounts (price tags).

A useful tool for assessing the economic risks of violations of the data protection legislations

Compared to the 'pre-consultation' version of the Guidelines, the inclusion of a table intended to provide numerical indications on the possible determination of fine amounts may be a useful tool to enable data controllers to carry out appropriate **assessments - at least in economic terms - of the impact and risks related to possible breaches of data protection legislations**.

As part of the risk assessment process, including any personal data protection impact assessments required under Article 35 of the GDPR, the methodology used to evaluate the risk - in terms of value of data and information, impacts and likelihood of incidents, acceptable risk, residual risk, and countermeasures - could also be defined in terms of the possible economic impact within the business organisation.

In fact, analysing the economic impacts may make the risk analysis more realistic and may give it greater capacity to communicate with all the stakeholders of the corporate organisation who are in charge of carrying out and approving this assessment.

In addition, the economic impact of any administrative fines, which could potentially be imposed by the competent DPA and which can be determined - albeit not with mathematical precision - on the basis of the table made available by the EDPB, to be considered when defining the risk assessment process, can also be a useful tool for determining the sustainability of the risk treatment plan, also in light of the provisions of Article 32 of the GDPR. Article 32 of the GDPR provides, in fact, that "*taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement* ***appropriate technical and organisational measures to ensure a level of security appropriate to the risk***".

Therefore, for the purpose of determining the sustainability of the risk treatment plan, the following elements may be taken into account:

a) the cost of applying the identified countermeasures should not exceed the calculated risk;
b) the cost of the identified countermeasures should be proportionate to the investment possibilities;
c) the choice of countermeasures should favour those of an organisational nature, which are usually more sustainable;
d) the cost of applying countermeasures must take into account the resources actually available, including the resulting commitment of the persons involved in their adoption and implementation.

* * *

GDPR e PIPL: similitudini e differenze

Il **PIPL** è la prima legge cinese sulla protezione delle informazioni personali ed è entrata in vigore lo scorso 1° novembre 2021.

È la prima legge in Cina a completare il quadro della protezione dei dati personali. Altre leggi di riferimento sono la *Cybersecurity Law* entrata in vigore il 1° giugno 2017, la *Data Security Law* entrata in vigore il 1° settembre 2021, nonché tutti gli altri regolamenti e provvedimenti del **Cyberspace Administration of China** ("**CAC**").

Da un'analisi del testo normativo del PIPL si può notare certamente l'influenza del GDPR.

Nonostante il PIPL e il GDPR si somiglino in vari aspetti, si possono tuttavia riscontrare diverse disposizioni e obblighi che divergono dal Regolamento UE 2016/679 ("GDPR").

Ambito di applicazione della normativa

Analogamente a quanto previsto dal GDPR, il PIPL, all'art. 3, par. 2, estende il proprio ambito di applicazione anche al trattamento di dati personali effettuato extra territorialmente, a condizione che lo scopo del trattamento sia rivolto a persone fisiche situate nel territorio cinese, al fine di:

- fornire loro prodotti o servizi;
- analizzare o valutare il loro comportamento; o
- negli altri casi stabiliti da leggi o regolamenti amministrativi cinesi.

L'ambito di applicazione della legge cinese sembra ispirarsi al GDPR in quanto si applica a livello extraterritoriale alle aziende che offrono beni o servizi o monitorano i comportamenti degli interessati. L'ambito generale del PIPL, tuttavia, può essere più ampio poiché tale legge fornisce un'ampia discrezionalità alle autorità di regolamentazione cinesi per prescrivere ulteriori circostanze in cui essa è applicabile.

Una evidente influenza del GDPR si nota, inoltre, nell'obbligo per le imprese con sede al di fuori dalla Cina di nominare un rappresentante o di stabilire un ente nel territorio per assumersi la responsabilità nei confronti delle autorità cinesi laddove a tali imprese si applichi il PIPL per attività extraterritoriali.

L'articolo integrale è disponibile su Norme e Tributi - Il Sole 24 Ore.

* * *

China released the first guidelines for the submission of the standard contract to transfer personal information outside the borders of the People's Republic of China

In our previous articles, we analyzed the Measures for data export security assessment (available here), the Guidelines for the application of such Measures (available here) and the implementation rules for personal information protection certification (available here).

In this article we will analyze another condition that the personal information controller shall meet in case the company "truly" need to transfer personal information outside the borders of the People's Republic of China for business or other such requirements: the standard contract.

Specifically, this article introduces the Guidelines for the filing of the standard contract in order to transfer personal information outside the Chinese territory (1st version) (the "Guidelines", in Chinese "个人信息出境标准合同备案指南，第一版") issued by the Cyberspace Administration of China (the "**CAC**") the last 30th May 2023, right before the effective date (1st June 2023) of the Measures for Standard Contract of Cross-border Transfer of Personal Information (the "**Measures**", in Chinese "个人信息 出境标准合同办法", available here, only in Chinese).

The Guidelines contains specific indications about the materials to be submitted with the standard contract for cross-border transfer of personal information (the "**Chinese SCC**") and on the procedure to be followed by the controller. Moreover, the Guidelines address widely concerned issues such as how to conduct personal information protection impact assessment (the "**PIPIA**").

This article aims at helping companies (including European companies) on how use the Chinese SCC for cross-border transfer of personal information and to understand the filing procedure provided by the CAC, in case of entering into a contract, in accordance with the standard contract formulated by the CAC, with the foreign receiving party, stipulating and agreeing the rights and obligations of both parties.

Application Scope

As well as the Measures, the Guidelines specify that the Chinese SCC mechanism can be adopted by the controller of personal information who intends transfer data overseas where the following circumstances shall be met simultaneously:

- is not designated as a critical information infrastructure operator ("**CIIO**");
- has processed personal information of less than 1 million individuals;
- has not provided or does not intend to provide abroad personal information of more than 100,000 individuals accumulatively since January 1st of last year; and
- has not provided or does not intend to provide abroad sensitive personal information of more than 10,000 individuals accumulatively since January 1st of last year.

Controllers cannot split the amount of personal information in order to adopt another mechanism and therefore mislead the requirements provided by the Chinese legislation to transfer personal information (such as pass a cross-border transfer security assessment conducted by the CAC).

Submission procedure

As provided in the Measures, the Chinese SCC and other materials shall be submitted to the cyberspace administration at the provincial level (the "**local CA**") within 10 working days after the Chinese SCC enters into effect.

The Guidelines clarifies that the submission shall be done by the delivery of written materials and by sending the electronic versions of the materials. In the future, it seems quite likely that online filing platforms will be opened. This is actually happening, for example, with the security assessment like in Suzhou (Jiangsu Province) where they opened an online channel for notifying security assessment for cross-border transfer of personal information.

Upon receipt of the submitted materials, the local CA will complete the examination of the materials within 15 working days and notify the result of the submission. The scenario will be different:

- in case of approval, the registration number will be issued to the applicant;
- in case of refusal, the applicant will receive a notice including the reasons of the rejection;
- in case of supplement, the local CA require to the applicant to supplement the materials. The supplement and the re-submission of the materials shall be completed within 10 working days.

Materials

On the basis of the Measures, the Guidelines further specifies that the following materials shall be submitted:

- a photocopy stamped with the official seal of the unified social credit code certificate (i.e., business license);
- a photocopy stamped with the official seal of the ID card of the legal representative of the company;
- a photocopy stamped with the official seal of the ID card of the person in charge of application for the submission;
- an original of the power of attorney for the person in charge of application for the submission;
- an original of the letter of commitment;
- an original of the standard contract of cross-border transfer of personal information;
- an original of the PIPIA report conducted by the CAC.

In addition to the Chinese SCC, the Guidelines also includes templates of the power of attorney for the person in charge, the letter of commitment and the PIPIA report.

Moreover, it is worth mentioning that the PIPIA shall be completed within **3 months** prior to the date of the submission and no significantly change must have occurred at the date of the submission.

Regarding the Chinese SCC, it is necessary to bear in mind that, in principle, the terms of the Chinese SCC cannot be modified. The contracting parties can agree to add other clauses, but they cannot be in conflict with the Chinese SCC content.

Controllers are responsible for the authenticity of the materials submitted, and those who submit false materials will be held legally responsible for the corresponding legal responsibilities.

Re-submission procedure

In specific circumstances occurs during the validity period of the contract, the Guidelines provides that a re-submission shall be done. In particular, a new PIPIA shall be conducted, and Chinese SCC shall be supplemented or re-signed and submitted.

Those specific circumstances are:

- changes in the purpose, scope, type, sensitivity, method, and storage location of the personal information to be exported or in the purpose or method of processing personal information by the overseas recipient, or extension of the storage period of personal information;
- changes in the legislation and regulations on the protection of personal information in the country or region where the overseas recipient is located, that may affect the rights and interest of the personal information subjects; or
- any other circumstances that may affect the rights and interests of the personal information subjects.

The local CA shall review the re-submitted materials within 15 working days.

The announcement and the Guidelines are both available **here**, only in Chinese.

* * *

Per maggiori informazioni, potete contattare:

Carlo Impalà
Partner e Responsabile Dip. TMT e Data Protection
(Carlo.Impala@MorriRossetti.it)

OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Morri Rossetti
Piazza Eleonora Duse, 2
20122 Milano

MorriRossetti.it
Osservatorio-dataprotection.it