OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Monthly Roundup

Dicembre 2022

MONTHLY ROUNDUP

Dicembre 2022

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

---

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

- **EU – USA Data Privacy Framework**

- European Commission starts the process to adopt adequacy decision for the EU-USA Data Privacy Framework [Link]

- Questions & Answers: EU-U.S. Data Privacy Framework, draft adequacy decision [Link]

- **EU**

- Digital Rights and Principles: Presidents of the Commission, the European Parliament and the Council sign European Declaration [Link]

- Artificial Intelligence Act: Council has adopted its common position ("general approach") [Link]

- **Garante Privacy**

- Il Garante Privacy ha sanzionato una regione italiana dichiarando illecito il controllo di metadati delle e-mail di dipendenti [Link]

- Social network delle chat vocali sanzionato per 2 milioni di euro: numerose le violazioni riscontrate dal Garante Privacy [Link]

PRINCIPALI AGGIORNAMENTI

- China: CAC announces implementation of personal information protection certification
- EU-US Data Privacy Framework: la bozza di decisione di adeguatezza della Commissione Europea
- Adozione del Regolamento DORA: la resilienza digitale e la gestione del rischio informatico del settore finanziario
- CNIL recall: the rules applying in case of communication to third parties of customers' lists for commercial purposes

China: CAC announces implementation of personal information protection certification

In our previous articles, we analyzed the Measures for Data Export Security Assessment and the Guidelines for the application of such Measures.

In order to guide controllers of personal information to comply with the Personal Information Protection Law (the "**PIPL**"), which came into effect as of 1st November 2021, and to carry out cross-border data transfer activities, the Cyberspace Administration of China ("**CAC**") and the State Administration of Market Regulation ("**SAMR**"), the last 18th November 2022, issued the Implementation Rules for Personal Information Protection Certification (in Chinese "个人信息保护认证实施规则", briefly "**Certification Rules**").

The Certification Rules contain the implementation rules about the process that controllers of personal information shall carry out to obtain the certification for certifying the collection, storage, use, processing, transmission, provision, disclosure, deletion, and cross-border transfer of personal information.

Pursuant to the Certification Rules, controllers shall comply:

- for collection, use and processing of personal information, with the requirements of GB/T 35273 Information Security Technology Personal Information Security Specifications (in Chinese "信息安全技术 个人信息安全规范")[1]; and, additionally
- for cross-border data transfer, also with the Security Certification Specifications for Handling Cross-Border Transfer of Personal Information (in Chinese: "个人信息跨境处理活动安全认证规范")[2].

Moreover, the Certification Rules outline requirements for on-site audits, the technical evaluation and approval of certification results, post-certification supervision, as well as certification period of validity, specifying that the certification process is divided into different steps:

1. the certification agency shall determine the documents and materials that the controller shall submit;
2. the controller shall submit all the required documents and materials to the certification agency and the latter, after a review of the submitted materials, shall give feedback to the controller;
3. the certification agency determines the certification plan on the basis of the certification materials submitted by the controller, including the type and quantity of personal information, the

[1] GB/T 35273 Information Security Technology Personal Information Security Specifications is a document that specifies the principles and security requirements for the collection, storage, use, sharing, transfer, public disclosure and deletion of personal information. The document is applicable to personal information processing activities carried out by all kinds of organizations and can also be used by competent authorities, third party assessment agencies and other organizations to supervise, manage and evaluate personal information processing activities.

[2] Specifications for Security Certification of Cross-Border Processing of Personal Information is a practice guideline that propose basic principles and requirements for the security of cross-border processing of personal information, as well as the protection of the rights and interests of personal information subjects. On this regard, the National Information Security Standardisation Technical Committee of China ("TC260") issued, on 16th December 2022, its revised practice guidelines for Specifications for Security Certification of Cross-Border Processing of Personal Information, following public consultations.

scope of processing activities involved, and the information of the technical verification agency;

4. the technical verification agency shall carry out the technical verification, according to the certification plan, and issue a report to the certification agency and to the controller;

5. the certification agency shall conduct on-site audit and issue a report to the controller;

6. the certification agency shall conduct a comprehensive evaluation on the basis of the certification materials, technical verification report, on-site audit report and other relevant materials and information, and take the final decision. In case the requirements are met, the certification agency will issue the certification. On the other side, where the requirements are not satisfied, the certification agency can require a rectification by the controller, within a time limit;

7. after the issue of the certification, the certification agency may conduct continuous supervision of the certified controller. Where the certification agency identified irregularities, the certification can be revoked.

According to the Certification Rules, the certification shall be valid for 3 years and it is renewable if the requirements are still satisfied.

The certified controller shall use the relevant certification mark (as provided in the Certification Rules) in advertisements and other publicity in accordance with relevant regulations, and shall not mislead the public. You can read the notice here and the implementation rules here, both only available in Chinese

* * *

EU-US Data Privacy Framework: la bozza di decisione di adeguatezza della Commissione Europea

In un nostro precedente articolo, abbiamo parlato dell'*Executive Order* firmato dal Presidente degli Stati Uniti, Joe Biden, lo scorso 7 ottobre.

A seguito di tale *Executive Order*, la Commissione europea ("**CE**") aveva pubblicato dei Q&A di chiarimento con indicazione degli step successivi all'adozione dell'Executive Order, annunciando altresì l'inizio della predisposizione di una bozza di decisione di adeguatezza.

In conseguenza di quanto sopra, il 13 dicembre la CE ha avviato il processo per l'adozione di una decisione di adeguatezza, ai sensi dell'art. 45 del Regolamento UE 2016/679 ("**GDPR**"), per i trasferimenti UE-USA, pubblicando il progetto di decisione di adeguatezza (disponibile e scaricabile alla fine del presente articolo).

Il progetto di decisione di adeguatezza rispecchia la valutazione della CE in merito al quadro giuridico statunitense. Nella sua valutazione, la CE conclude affermando che, dal punto di vista normativo, gli Stati Uniti garantiscono un livello adeguato di protezione dei dati personali trasferiti dall'UE alle imprese statunitensi.

Il progetto di decisione di adeguatezza è stato trasmesso all'*European Data Protection* Board ("*EDPB*"), che ora dovrà fornire il suo parere.

I successivi step

A seguito del rilascio del parere da parte dell'EDPB:

- la CE dovrà chiedere l'approvazione da parte di un comitato composto da rappresentanti degli Stati membri dell'UE;
- il Parlamento europeo ha il diritto di controllo sulle decisioni di adeguatezza;
- una volta completata la procedura di adozione, la CE potrà procedere all'adozione della decisione finale di adeguatezza.

Entro un anno dall'adozione della decisione di adeguatezza, la CE, unitamente alle Autorità di controllo europee e alle autorità statunitensi competenti, valuterà il funzionamento del nuovo EU-USA Data Privacy Framework, verificando la piena attuazione e l'efficace funzionamento di tutte le misure volte a rafforzare le garanzie a tutela della protezione dei dati personali e delle libertà civili degli interessati adottate dagli Stati Uniti. Il nuovo EU-USA Data Privacy Framework sarà soggetto a revisioni periodiche.

La decisione di adeguatezza, laddove adottata, potrebbe risolvere il problema del trasferimento di dati personali dall'UE verso gli Stati Uniti, sorto a partire dalla nota sentenza della Corte di Giustizia dell'UE "*Schrems II*" che ha invalidato il c.d. "*Privacy Shield*" (ovvero la precedente convenzione USA-UE in materia di trasferimento di dati personali).

Tuttavia, allo stato attuale non è possibile determinare quando la decisione di adeguatezza finale verrà effettivamente adottata ed entrerà in vigore.

* * *

Adozione del Regolamento DORA: la resilienza digitale e la gestione del rischio informatico del settore finanziario

Lo scorso 28 novembre, il Consiglio dell'Unione europea ha annunciato l'adozione del *Digital Operational Resilience Act* (il c.d. Regolamento DORA, che unitamente alla Direttiva NIS2 e al *Cyber Resilience Act*, costituisce l'insieme di iniziative europee relative alla sicurezza digitale), il quale va a incrementare le misure di sicurezza a favore della resilienza e della sicurezza informatica del settore finanziario, assicurando che gli operatori coinvolti siano in grado di prevenire nonché, eventualmente, reagire alle minacce informatiche.

Il Regolamento DORA individua i requisiti da rispettare e gli adempimenti da porre in essere, relativi alla *cybersecurity*, da parte delle aziende che operano, inter alia, nel settore finanziario, bancario e assicurativo, nonché dai fornitori di servizi di cripto-asset e di servizi strumentali considerati critici.

Tra le principali novità introdotte dal Regolamento DORA si segnalano gli obblighi di:

- predisposizione di un quadro di gestione e di controllo interno che garantisca una gestione efficace e prudente di tutti i rischi informatici;
- utilizzo e aggiornamento di sistemi, protocolli e strumenti di TIC (tecnologie dell'informazione e della comunicazione) idonei, affidabili, dotati di capacità sufficiente per elaborare i dati e resilienti.

Gli operatori dovranno adeguarsi entro 24 mesi dalla data di entrata in vigore del Regolamento DORA e l'adeguamento dovrà essere effettuato in conformità del principio di proporzionalità: i soggetti, nella valutazione e dimostrazione del corretto livello di requisiti implementati, dovranno quindi tenere in considerazione specifici fattori.

* * *

CNIL recall: the rules applying in case of communication to third parties of customers' lists for commercial purposes

On December 5th, 2022, the French Data Protection Authority (known as "*Commission Nationale de l'Informatique et des Libertés*", hereinafter "**CNIL**") published a reminder of the rules applying in case of communication of customers' lists to third parties for commercial purposes.

In these cases, the CNIL reminds that such communications are not prohibited by the Regulation (EU) 2016/679 ("**GDPR**"), but must be done in compliance with specific obligations.

In particular, communication of customers' lists to third parties can take place when:

- personal data have been collected – from the beginning – in compliance with the GDPR;
- personal data were collected for commercial purposes. On this regard, for example, CNIL excludes the communication of personal data kept for administrative purposes;
- personal data are active[3]; and
- the customers have given their consent or have not objected to the communication of their personal data to third parties for commercial purposes. Without the consent or in case of objection, the relevant personal data must be deleted before the communication of the customers' list to the purchaser.

Moreover, the purchaser must ensure that the rights of data subjects are respected and, specifically, the purchaser shall:

- provide specific information to the data subjects at the time when personal data are obtained and, in any case, at latest within one month, also indicating from which source the personal data were originated (i.e., the name of the company that has communicate the personal data, unless this information has already been provided);
- be able to demonstrate that it has the data subjects' informed consent for commercial purposes.

Regarding the informed consent, it is possible to distinguish two different situations:

- the data controller has already obtained the consent on behalf of the purchaser. On this regard, if, at the time of data collection, the identity of the purchaser was already included in the list of the recipients of the personal data, the

[3] According to the CNIL recommendations, customers' personal data collected for commercial purposes may be kept for a period of three years after the end of the commercial relationship or after the last contact by the customer.

purchaser may directly contact the data subjects who have consented to the communication of their personal data for commercial purposes;

- the data controller has not obtained the consent on behalf of the purchaser. In this case, the purchaser shall inform the data subjects and collect their consent before sending them commercial communication.

In any case, the purchaser must respect the rights of data subjects (such as the right of data subjects to withdraw the consent, at any time, or to express their refusal to receive new communications) and, in general, all the obligations provided by the GDPR (e.g., principle of the accountability, data retention periods, security of processing, etc.).

* * *

Per maggiori informazioni, potete contattare:

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

LinkedIn

Morri Rossetti

Osservatorio

OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Morri Rossetti
Piazza Eleonora Duse, 2
20122 Milano

MorriRossetti.it
Osservatorio-dataprotection.it