OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Monthly Roundup

Febbraio 2023

MONTHLY ROUNDUP

Febbraio 2023

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

---

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

EU

- One-Stop-Shop case digest on right to object and right to erasure [Link]
- European Parliament resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework [Link]

Garante Privacy

- Decreto trasparenza e lavoro: le prime indicazioni del Garante [Link]
- Sanità: per le ricette transfrontaliere servono maggiori garanzie [Link]
- Telemarketing, Garante: il "no" dell'utente va registrato subito [Link]
- Cloud nella PA: le Autorità Ue chiedono il rispetto della privacy [Link]

PRINCIPALI AGGIORNAMENTI

- Clinical Trials Information System: it becomes mandatory for new clinical trial applications in the EU
- Privacy by design: adozione della ISO 31700
- Diritto all'oblio: cosa prevede la Riforma Cartabia
- Decreto Trasparenza: il Garante Privacy si esprime in merito agli obblighi introdotti in materia di protezione dei dati personali

---

Clinical Trials Information System: it becomes mandatory for new clinical trial applications in the EU

From 31 January 2023, all initial clinical trial applications in the European Union ("EU") must be submitted via the Clinical Trials Information System. The latter is now the single-entry point for sponsors and regulators of clinical trials for the submission and assessment of clinical trial data.

Clinical Trials Regulation: aims and benefits

On 31 January 2022, the European Regulation No. 536/2014 on clinical trials on medicinal products for human use (the "**Clinical Trials Regulation**") came into force, replacing the former Directive 2001/20/EC ("**Directive**") and the corrisponding national transposing legislation.

The Clinical Trials Regulation provided for a transition period:

- during the first year of implementation and until 30 January 2023, clinical trial sponsors could choose whether to apply to start a clinical trial via the CTIS or under the Directive;
- from **31 January 2023** onwards, clinical trial sponsors are required to apply to start a clinical trial via the Clinical trials Information System ("CTIS");
- from 31 January 2025, any trials approved under the Directive that continue to running will need to comply with the Clinical Trials Regulation and their sponsors must have recorded the related information in the CTIS.

The Clinical Trials Regulation aims to harmonise the processes of assessing and supervising clinical trials throughout the EU in order to facilitate the conduct of larger clinical trials in multiple EU Member States/European Economic Area ("**EEA**") countries and it aims to ensure that the EU provides an attractive and favorable environment for carrying out clinical research on a large scale, with high standards of public transparency and safety for clinical trial participants.

Prior to the implementation of the Clinical Trials Regulation, sponsors had to submit separate clinical trial applications to national competent authorities and ethics committees in each country in order to obtain regulatory approval to conduct a clinical trial. Furthermore, registration and the posting of results of the clinical trials were subject to separate processes.

With the implementation of the Clinical Trials Regulation – in order to obtain the approval to run a clinical trial in several European countries – sponsors can now submit one online application via the CTIS, This makes it more efficient both to carry out multinational trials and for EU Member States to evaluate and authorise such applications together.

However, running a clinical trial involves the processing of personal data and, therefore, beside the Clinical Trials Regulation, also the General Data Protection Regulation (EU) 679/2016 ("**GDPR**") shall apply. It should be noted that the Clinical Trials Regulation constitutes the sector-specific legislation with special provisions under a data protection perspective which, however, do not derogate from the provisions of the GDPR.

Moreover, considering that personal data are also processed by the Union institutions, bodies, offices and agencies, also Regulation (EU) 2018/1725 (s.c. European Data Protection Regulation, hereinafter "**EUDPR**") shall apply.

CTIS and personal data issues

In the context of a clinical trial (including the authorisation and supervision process), different actors may need to register personal data into CTIS, including sponsors, marketing authorisation applicants or holders, the European Commission, European Medicine Agency ("**EMA**"), EU Member States and EEA countries (the "**Parties**").

In general terms, CTIS is a system that facilitate the exchange of information between the Parties, and specifically, throughout the lifecycle of a clinical trial, the interactions between clinical trial sponsors (researchers or companies that run a clinical trial and collect and analyse the data) and regulatory authorities in EU Member States and EEA countries.

Therefore, CTIS is structured as follows:

- the **sponsor's workspace**, which assists them with preparing and completing the clinical trial application and related documents to be submitted for evaluation;
- the **authority's workspace**, which enables EU Member States, EEA countries and the European Commission to use CTIS to oversee the conduct of clinical trials in the EU/EEA;
- a **search function within the public website**, which anybody can use to find detailed information on clinical trials conducted in the EU and EEA based on the information contained in CTIS.

Considering the involvement of the different Parties in clinical trials, the protection of personal data in CTIS is a joint responsibility. Therefore each Party is responsible for ensuring that personal data are processed according to the principles of the GDPR and EUDPR.

In this regard, following consultation by EMA, the European Data Protection Supervisor ("**EDPS**") confirmed [1] that, pursuant to Article 26 of the GDPR and Article 28 of the EUDPR, the Parties need to be qualified as "joint controllers" of the CTIS.

In order to comply with the obligations set forth by Article 26 of the GDPR, the EMA and the representatives of the Parties were engaged in drafting a Joint Controller Agreement ("**JCA**") which sets out the roles and responsibilities of the joint controllers in relation to the processing of personal data while using and interacting with CTIS. Moreover, the JCA sets out the measures that the Parties shall put in place in order to ensure the secure processing of personal data in CTIS and covers how the Parties must handle any personal data breaches.

Considering that JCA needs to be accepted by all joint controllers, it should be noted that, when accessing the CTIS for the first time, each user is required to confirm acceptance of the terms set out in the JCA.

The JCA also includes two annexes:

- "Annex I" provides a list of contact points for cooperation between the different Parties subject to the CTIS JCA and having access to the CTIS secure domain as applicable, and for data subjects in respect of queries, complaints and provision of information within the scope of the JCA;
- "Annex II" thereof provides a privacy notice regarding personal data processing in the CTIS.

Finally, it is important to note that each of the joint controller can act as an independent controller for the processing activities that can be performed without the cooperation of the other Parties (e.g. sponsors are independent data

[1] See EDPS Case Number C 2018-0642.

controllers in relation to data processing activities performed outside of CTIS and carried out within their organisation, whether related to clinical trials or not).

Privacy roles of the sponsor and the clinical trial centre

As clarified above, in any clinical trial there are multiple actors involved, each with their own scope of activities and specific responsibilities. However, while the role of the Parties within the CTIS is well defined, in the context of conducting clinical trials, neither the GDPR nor the Clinical Trials Regulation have brought clarity to the privacy roles of the subjects involved therein.

In this paper, the privacy roles of the sponsor and the trial centre will be examined in more detail.

The EDPB's Guidelines 07/2020 on the concepts of controller and processor in the GDPR ("**EDPB's Guidelines**"), throughout a specific example[2], consider that the trial centre and the sponsor, which have to draft together the study protocol, should be qualified, pursuant to Article 26 of the GDPR, as joint-controller, as they jointly determine and agree on the same purpose and the essential means of the processing.

On the contrary, in the event that the trial centre does not participate to the drafting of the protocol (it only accepts the protocol already elaborated by the sponsor), and the protocol is only designed by the sponsor, the trial centre should be considered as a processor and the sponsor as the controller for such trial.

Instead, at the national level, the "Guidelines for the Processing of Personal Data in the Context of Clinical Trials of Medicines - July 24, 2008" ("**Guidelines**") published by the Italian Data Protection Authority ("**Italian DPA**") provide that, trial centres and sponsor have separate responsibilities in the context of clinical trials and are, therefore, to be qualified as autonomous data controllers.

In fact:

- on the one hand, the sponsor (i) does not collect data directly, (ii) does not interact with "enrolled" subjects, and (iii) carries out processing operations through its monitors;
- on the other hand, the trial centre (i) is not subjected to any subordination, (ii) accepts the sponsor's protocol by agreeing with the latter on certain aspects, (iii) performs the trial in organizational autonomy although in compliance with the protocol, (iv) provides the privacy notice, (v) independently decides to employ collaborators that it deems qualified and is accountable for their performance, (vi) allows the sponsor's collaborators access to the original medical records of the subjects involved in the trial in order to carry out the monitoring activities, and (vii) manages and keeps such records under its own responsibility.

In view of the above, it follows that the trial centre and the sponsors should, for the reasons outlined by the Italian DPA, be considered as two autonomous data controllers regardless of whether or not they have jointly drafted the trial protocol.

Conclusion

The joint-controllership's approach (which is common especially in other European countries) should not be deemed as the suitable solution applicable aprioristically to all clinical trials without any distinction. This is due to the circumstance that data controllers shall comply,

[2]The example mentions the case in which a health care provider (the investigator) and a university (the sponsor) decide to launch together a clinical trial with the same purpose. They collaborate together to the drafting of the study protocol (i.e. purpose, methodology/design of the study, data to be collected, subject exclusion/inclusion criteria, database reuse (where relevant) etc.

pursuant to Articles 5(2) and 24 of the GDPR. In this specific case, the Accountability principle should require the parties to carry out a specific assessment, supported by documentation, of their privacy roles, taking into account the flow of personal data in the context of clinical trials.

In particular, it should be noted that "joint-controllers" jointly determine the purposes and means of processing. In the context of clinical trials, however, the purposes pursued by the clinical trial centre (i.e., patient care purposes) and the sponsor (i.e., scientific research purposes) are substantially different, even if they share a protocol.

Finally, it is worth noting that while the Guidelines are still applicable, they are dated, and new EDPB guidelines, updated in light of the provisions of the Clinical Trials Regulation, are expected.

* * *

Privacy by design: adozione della ISO 31700

In data 8 febbraio 2023, l'*International Organization for Standardization* [3] ("**ISO**") adotterà lo standard ISO 31700, che fornisce a tutti i titolari del trattamento requisiti e indicazioni sulle corrette modalità di implementazione del principio di *privacy by design*.

Privacy by design

Il principio di *privacy by design*, unitamente a quello di *privacy by default*, viene introdotto dall'art. 25 del Regolamento (UE) 2016/679 ("**GDPR**"). Tale principio impone ai titolari del trattamento l'obbligo, fin dalla progettazione, di mettere in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati personali. In particolare, si tratta di ridurre al minimo il trattamento di dati personali, mediante specifiche misure tecniche e organizzative (ad es. attraverso la pseudonimizzazione).

Il concetto di *privacy by design* è stato, tuttavia, coniato, prima dell'entrata in vigore del GDPR, da Ann Cavoukian, *privacy commissioner* canadese, verso la fine degli anni '90.

Lo scopo della Cavoukian era quello di garantire che la privacy fosse tenuta in considerazione durante l'intero processo di sviluppo di nuove tecnologie e prodotti, a partire dalla progettazione, e non soltanto in una fase successiva alla stessa.

In particolare, il concetto era stato coniato e sviluppato a seguito di un aumento della quantità di dati personali raccolti, conservati e comunicati da parte degli enti e delle società, nonché in conseguenza dell'incremento di episodi di data breach e violazioni della normativa in materia di protezione dei dati personali.

I principi su cui si basa la *privacy by design* sono i seguenti:

1. valutazione dei rischi a partire dalla fase di progettazione, prevenendo il verificarsi degli

[3] L'ISO è un'organizzazione mondiale che definisce standard e norme tecniche. Essa svolge funzioni consultive per l'UNESCO e per l'ONU. L'ISO è composto da 167 organismi nazionali di standardizzazione. Ad oggi, l'ISO ha adottato più di 24.000 standard, tra cui l'ISO 27001 che descrive le best practice per i sistemi di gestione della sicurezza delle informazioni.

stessi e non correggendo, successivamente, eventuali violazioni della privacy;
2. privacy come impostazione predefinita, in modo tale che la tutela dei dati personali sia impostata *by default* in qualsiasi prodotto, servizio o pratica commerciale;
3. privacy incorporata nel progetto tramite specifiche misure tecniche e organizzative (ad es. attraverso la pseudonimizzazione o la minimizzazione dei dati sin dalla fase di progettazione);
4. massima funzionalità, in modo da rispettare tutte le esigenze;
5. sicurezza e protezione dei dati durante tutto il ciclo di vita del prodotto o servizio;
6. visibilità e trasparenza di tutto il processo di trattamento dei dati personali;
7. centralità dell'utente e, conseguentemente, rispetto dei suoi diritti, nonché tempestività e chiarezza nel rispondere alle richieste dello stesso.

Adozione della ISO 31700

L'ISO 31700 è un nuovo standard internazionale per la protezione dei dati personali costituito da linee guida che possono essere tenute in considerazione e seguite da qualsiasi tipo di organizzazione o società, a seconda delle esigenze specifiche (ad es. multinazionali, ma anche PMI e *startup*).

Tale standard offre indicazioni e raccomandazioni nel processo di gestione dei rischi per la privacy e nella progettazione della struttura di gestione degli stessi all'interno delle organizzazioni.

Lo standard ISO 31700 contiene 30 requisiti, nonché indicazioni generali su come implementare il principio di *privacy by design*, quali:

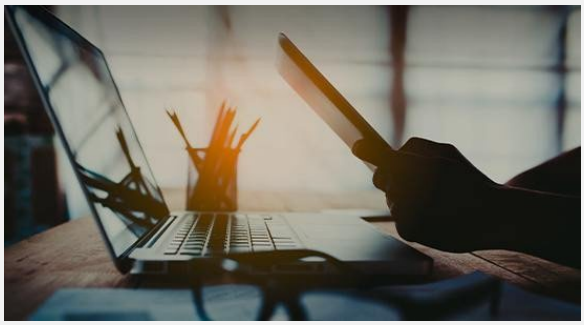
1. progettazione di funzionalità che consentano ai consumatori di far valere i propri diritti alla protezione dei dati personali;
2. sviluppo di funzionalità che consentano di determinare le preferenze dei consumatori in materia di protezione dei dati personali;
3. assegnazione di ruoli alle autorità competenti;
4. individuazione di responsabilità multifunzionali;
5. sviluppo di know-how, competenze e capacità in materia di protezione dei dati personali;
6. gestione della documentazione e delle informazioni;
7. requisiti per la comunicazione con i consumatori (i.e. fornire ai consumatori informazioni sulla privacy, individuare i soggetti responsabili nel fornire tali informazioni, rispondere alle richieste e ai reclami dei consumatori stessi, predisporre comunicazioni diverse in base alle differenti fasce di consumatori, predisporre specifiche comunicazioni in caso di data breach);
8. requisiti di gestione del rischio (i.e. condurre privacy risk assessment, valutare le funzionalità di terze parti in materia di privacy, stabilire e documentare i requisiti per i controlli sulla privacy, monitorare e aggiornare la valutazione del rischio, includere i rischi per la privacy nella progettazione della resilienza della cybersecurity);
9. sviluppo, implementazione e gestione dei controlli sulla privacy (i.e. integrare la progettazione e l'operatività dei controlli sulla privacy nel processo di sviluppo e gestione del prodotto, progettare e implementare i controlli sulla privacy, progettare le fasi di test, gestire la migrazione, gestire l'operatività, prevenire e gestire le violazioni della privacy, gestire per l'intero ciclo di vita dei dati i controlli sulla privacy per i processi e i prodotti da cui dipende il prodotto in esame);
10. requisiti per la cessazione dell'utilizzo dei dati (i.e. progettare i controlli sulla privacy in

caso di dismissione e termine di utilizzo dei dati).

Il testo della ISO 31700 è disponibile, in lingua inglese, qui.

* * *

Diritto all'oblio: cosa prevede la Riforma Cartabia



Il D.lgs. n. 150 del 2022 (attuazione della l. n. 134 del 2021, recante delega al Governo per l'efficienza del processo penale, nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari), entrato in vigore a partire dal 30 dicembre 2022, prevede l'introduzione dell'art. 64-ter alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale.

In particolare, l'art. 64-ter, rubricato *"Diritto all'oblio degli imputati e delle persone sottoposte ad indagini"*[4], prevede che la persona nei cui confronti sia stata pronunciata una sentenza di proscioglimento, di non luogo a procedere o un provvedimento di archiviazione possa richiedere e ottenere che nel provvedimento sia apposta e sottoscritta – dalla cancelleria del giudice che ha emesso la sentenza o il provvedimento – una **specifica annotazione che precluda l'indicizzazione o disponga la deindicizzazione**[5] **sulla rete Internet dei dati personali riportati nella sentenza o nel provvedimento**, ai sensi e nei limiti con quanto previsto dall'art. 17 del Regolamento (UE) 679/2016 ("**GDPR**"), nonché dall'art. 42 del D.lgs. 196/2003 ("**Codice Privacy**").

Il diritto all'oblio

Il diritto all'oblio, regolato dall'art. 17 del GDPR, è una figura di creazione giurisprudenziale e indica il diritto a non rimanere esposti senza limiti di tempo a una rappresentazione non più attuale della propria persona con pregiudizio alla reputazione e alla riservatezza, a causa della ripubblicazione, a distanza di importanti intervalli temporali, di notizie relative a vicende personali del passato che, seppur legittimamente pubblicate in un determinato momento storico, non risultano più di interesse pubblico o non più

[4] "La persona nei cui confronti sono stati pronunciati una sentenza di proscioglimento o di non luogo a procedere ovvero un provvedimento di archiviazione può richiedere che sia preclusa l'indicizzazione o che sia disposta la deindicizzazione, sulla rete internet, dei dati personali riportati nella sentenza o nel provvedimento, ai sensi e nei limiti dell'articolo 17 del regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016. Resta fermo quanto previsto dall'articolo 52 del decreto legislativo 30 giugno 2003, n. 196.
Nel caso di richiesta volta a precludere l'indicizzazione, la cancelleria del giudice che ha emesso il provvedimento appone e sottoscrive la seguente annotazione, recante sempre l'indicazione degli estremi del presente articolo: «Ai sensi e nei limiti dell'articolo 17 del Regolamento del Parlamento europeo del 27 aprile 2016, n. 679, è preclusa l'indicizzazione del presente provvedimento rispetto a ricerche condotte sulla rete internet a partire dal nominativo dell'istante».
Nel caso di richiesta volta ad ottenere la deindicizzazione, la cancelleria del giudice che ha emesso il provvedimento appone e sottoscrive la seguente annotazione, recante sempre l'indicazione degli estremi del presente articolo: «Il presente provvedimento costituisce titolo per ottenere, ai sensi e nei limiti dell'articolo 17 del regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, un provvedimento di sottrazione dell'indicizzazione, da parte dei motori di ricerca generalisti, di contenuti relativi al procedimento penale, rispetto a ricerche condotte a partire dal nominativo dell'istante".

[5] L'attività di deindicizzazione consiste nell'escludere che il nome di un soggetto compaia tra i risultati di un motore di ricerca in esito a una interrogazione del medesimo; con la deindicizzazione si elimina una particolare modalità di ricerca del dato, il quale rimane presente in rete e continua ad essere raggiungibile, ma con una ricerca più complessa e più lunga.

rappresentative dell'identità personale del soggetto interessato.

La tutela del diritto all'oblio va bilanciata con il diritto della collettività alla conoscenza del fatto, la quale esprime il diritto di manifestazione del pensiero e quindi di cronaca e di conservazione della notizia per finalità storico-sociale e documentaristica (sul punto, cfr. Cass. civ. n. 9147/2020).

A livello europeo, il diritto all'oblio (denominato "*diritto alla cancellazione*") è sancito dall'art. 17 del GDPR ed è il diritto, in capo all'interessato, di ottenere dal titolare del trattamento la cancellazione dei propri dati personali, solo in presenza di determinate condizioni, specificatamente indicate.

Una delle più note sentenze in materia di diritto all'oblio è la sentenza della Corte di Giustizia dell'Unione europea del 13 maggio 2014, causa C-131/12 (c.d. "**caso Google Spain**"), a seguito della quale il Gruppo di lavoro articolo 29 ha adottato le Linee guida WP 225 2014, contenenti un elenco di criteri comuni che le Autorità di controllo devono utilizzare nella gestione dei reclami relativi alle richieste di cancellazione da parte di persone fisiche e ove vengono illustrate le conseguenze di tale diritto alla cancellazione, fornendo un orientamento per la ponderazione dei diritti.

Suddette Linee guida ribadiscono, così come la giurisprudenza nazionale, che le valutazioni devono essere effettuate caso per caso e che l'accoglimento o meno della richiesta può variare a seconda del caso in questione, dal momento che il diritto all'oblio non è assoluto.

In particolare, il caso Google Spain – considerato da molti una pietra miliare nell'affermazione del diritto all'oblio – ha inquadrato il diritto all'oblio come il diritto alla deindicizzazione del dato personale dal motore di ricerca. In tale sede, infatti, la Corte di Giustizia dell'Unione europea ha sancito una serie di importanti principi, tra cui l'obbligo del gestore di un motore di ricerca non a cancellare l'informazione presente sul sito della fonte originaria, bensì a sopprimere, in presenza di determinate condizioni e su richiesta, dall'elenco di risultati che appare a seguito di una ricerca effettuata "per parole", i *link* verso pagine *web* pubblicate da terzi e contenenti informazioni relative all'interessato.

La Corte ha altresì precisato che l'obbligo di cancellazione alla quale è tenuto il gestore del motore di ricerca sorge a seguito di un equo bilanciamento tra il legittimo interesse degli utenti ad avere accesso alle informazioni di cui l'interessato chiede la deindicizzazione e il diritto all'oblio dell'interessato stesso. Tale obbligo può sorgere anche qualora il trattamento dei dati risulti inizialmente lecito poiché, con il trascorrere del tempo, può divenire incompatibile con la normativa applicabile.

La giurisprudenza della Corte di Giustizia dell'Unione europea e la Corte di Cassazione hanno stabilito che, di regola, non è possibile imporre alle testate giornalistiche la rimozione degli articoli collegati ad un nome. La soluzione percorribile è, invece, la deindicizzazione della notizia dai motori di ricerca: in altri termini, si tratta di un "ordine" dato ai motori di ricerca di non "mostrare" più i risultati di cui l'interessato ha chiesto l'oscuramento.

Alla luce di quanto sopra, seppur tale diritto alla cancellazione non risulti una novità, in Italia potrebbe costituire un punto di svolta posto che a livello nazionale a decidere sul punto era sempre chiamata l'autorità competente (i.e. autorità giudiziaria o l'Autorità Garante per la protezione dei dati personali, c.d. "**Garante Privacy**").

Infatti, fino al 1° gennaio 2023, gli interessati, per poter avvalersi del proprio diritto all'oblio, erano tenuti ad avviare contenziosi e/o a rivolgersi al

Garante Privacy, i quali analizzavano le richieste caso per caso.

Con la Riforma Cartabia, invece, l'interessato può richiedere, **direttamente** alla cancelleria del giudice che ha emesso il provvedimento, l'apposizione e sottoscrizione di specifica annotazione che precluda l'indicizzazione o disponga la deindicizzazione, sulla rete Internet, dei propri dati personali.

Inoltre, sulla base della lettera della norma, non sembrano previsti mezzi di impugnazione specifici, facendo ritenere che il provvedimento della cancelleria risulti inoppugnabile. Di contro, in caso di inottemperanza da parte della cancelleria, risulta ipotizzabile un ricorso per ottemperanza avanti al Tribunale Amministrativo Regionale.

In conclusione, risulta da vedere adesso come verrà applicata la norma e come si evolverà la situazione sia a livello di modalità di effettuazione delle notifiche che delle azioni esperibili in caso di mancato rispetto dell'annotazione sul provvedimento (ad es. in caso di mancata deindicizzazione).

Nel nostro Osservatorio abbiamo già trattato il tema del diritto all'oblio e del diritto alla cancellazione in diverse occasioni, quali, a titolo esemplificativo:

- Diritto all'oblio: il Garante Privacy conferma la possibilità di ottenere la deindicizzazione per coloro che sono estranei a vicende giudiziarie;
- Autorità di controllo svedese sanziona Google per violazione del diritto alla cancellazione.

* * *

Decreto Trasparenza: il Garante Privacy si esprime in merito agli obblighi introdotti in materia di protezione dei dati personali

Come noto, lo scorso 13 agosto 2022 è entrato in vigore il D.Lgs. 104/2022 (c.d. "**Decreto Trasparenza**"), in attuazione della Direttiva UE 1152/2019, relativa al miglioramento delle condizioni di lavoro nell'UE, che ha introdotto ulteriori obblighi informativi qualora il datore di lavoro utilizzi "***sistemi decisionali o di monitoraggio automatizzati*** *deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori*".

L'impiego di tali sistemi decisionali e di monitoraggio automatizzati dà luogo a trattamenti di dati personali e presenta, quindi, profili rilevanti in materia. In ragione di ciò, le nuove disposizioni necessitano di essere coordinate con la normativa applicabile in materia di protezione dei dati personali, in particolare con il Regolamento UE 2016/679 ("**GDPR**") e il D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018 ("**Codice Privacy**").

A seguito delle Circolari interpretative dell'Ispettorato Nazionale del Lavoro e del Ministero del Lavoro (Circolare n. 19 del 20/9/2022 e Circolare n. 4 del 10/8/2022), il Garante per la protezione dei dati personali, in data 24/1/2023, ha rilasciato un documento

relativo alle questioni interpretative e applicative in materia di protezione dei dati personali connesse ai nuovi obblighi introdotti con il Decreto Trasparenza.

Il presente contributo è volto a sintetizzare le osservazioni del Garante e a riassumere gli adempimenti che i datori di lavoro sono tenuti a porre in essere – relativamente ai profili in materia di protezione dei dati personali – anche alla luce dell'interpretazione sistematica del Garante.

Per maggiori approfondimenti, anche relativi agli aspetti di natura prettamente giuslavoristica, si rimanda agli ulteriori contributi (rispettivamente del 8/8/2022 e del 4/10/22), predisposti a cura dello Studio Morri Rossetti.

Utilizzo di sistemi decisionali o di monitoraggio automatizzati

L'elemento del Decreto Trasparenza che ha destato maggiori perplessità è la previsione in virtù della quale il datore di lavoro è chiamato a informare il dipendente ove questi utilizzi sistemi decisionali o di monitoraggio automatizzati. Le difficoltà interpretative di tale previsione sono principalmente dovute all'individuazione di tali sistemi, essendo tale definizione particolarmente generica.

La Circolare n. 4 del 10/8/2022 aveva fornito una propria interpretazione al riguardo, identificando come tali gli strumenti che – anche ove vi sia un intervento umano meramente accessorio – generino decisioni automatizzate sulla base dei dati da essi stessi raccolti ed elaborati, alle quali sia interamente rimessa la disciplina della vita lavorativa del dipendente (con la conseguenza di un rilevante impatto su quest'ultima).

La Circolare forniva anche degli esempi pratici in cui sussiste l'obbligo di informativa:

1. assunzione o conferimento dell'incarico tramite l'utilizzo di chatbots durante il colloquio, la profilazione automatizzata dei candidati, lo screening dei curricula, l'utilizzo di software per il riconoscimento emotivo e test psicoattitudinali, etc.;
2. gestione o cessazione del rapporto di lavoro con assegnazione o revoca automatizzata di compiti, mansioni o turni, definizione dell'orario di lavoro, analisi di produttività, determinazione della retribuzione, promozioni, etc., attraverso analisi statistiche, strumenti di *data analytics* o *machine learning*, rete neurali, *deep-learning*, etc.

In alternativa, non è necessario procedere all'informativa nel caso, ad esempio, di utilizzo di sistemi automatizzati deputati alla rilevazione delle presenze in ingresso e in uscita, cui non consegua un'attività interamente automatizzata finalizzata a una decisione datoriale.

Con riferimento, poi, ai sistemi incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori, il datore di lavoro ha l'obbligo di informare il lavoratore dell'utilizzo di tali sistemi automatizzati, quali – a puro titolo di esempio: tablet, dispositivi digitali e *wearables*, gps e geolocalizzatori, sistemi per il riconoscimento facciale, sistemi di *rating* e *ranking*, etc., purché tali sistemi incidano "*sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori*".

La Circolare precisava, in aggiunta, che si deve ritenere sussistente l'obbligo informativo anche in relazione all'utilizzo di sistemi decisionali o di monitoraggio automatizzati integrati negli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, allorquando presentino le caratteristiche tecniche e le funzioni descritte in precedenza.

Le prime indicazioni del Garante Privacy

Secondo quanto riportato dalle prime indicazioni del Garante, la disciplina del Decreto Trasparenza, che trova applicazione sia nel caso in cui il trattamento da parte del datore di lavoro venga effettuato in fase di pre-assunzione, che nel caso in cui venga posto in essere in costanza di rapporto di lavoro, è considerabile una disciplina maggiormente specifica e tutelante per gli interessati nel contesto lavorativo, conformemente a quanto previsto dall'art. 88 del GDPR.

Tale disciplina trova giustificazione anche in considerazione del fatto che l'impiego di tali sistemi di monitoraggio particolarmente invasivi – come sottolineato dal Garante – pone, anzitutto, **un tema di liceità dei trattamenti di dati personali effettuati mediante gli stessi**, tenuto conto della disciplina di settore in materia di impiego di strumenti tecnologici nel contesto lavorativo (cfr. art. 114 del Codice Privacy, che rimanda all'art. 4 dello Statuto dei Lavoratori).

Inoltre, le specificità delle tecnologie di questi sistemi, nonché la natura dei dati trattati (ad esempio, i dati biometrici e quelli relativi alle emozioni del lavoratore) e le funzionalità che spesso ad essi sono associate, sollevano, altresì, dubbi in ordine alla stessa **proporzionalità del loro impiego**, nonché di **compatibilità con i principi generali in materia di protezione dei dati e con il quadro di garanzie in materia di libertà e dignità del lavoratore**, potendosi, peraltro, porsi in contrasto con le disposizioni nazionali che vietano al datore di lavoro di trattare informazioni attinenti alla sfera privata del lavoratore (cfr. art. 113 del Codice Privacy, che rimanda all'art. 8 dello Statuto dei Lavoratori).

- **I nuovi obblighi informativi**

L'articolo 4 del Decreto Trasparenza ha pertanto introdotto, *inter alia*, **nuovi obblighi** informativi in capo al datore di lavoro, tra cui quello di informare adeguatamente i lavoratori nel caso utilizzi sistemi decisionali o di monitoraggio automatizzati ai fini della assunzione o del conferimento dell'incarico, o per altre attività collegate al rapporto di lavoro e alla sua gestione. Alcune delle specifiche informazioni che devono essere fornite ai dipendenti integrano quanto previsto dagli artt.13 e 14 del GDPR, mentre altre ne costituiscono una specificazione.

Tra le informazioni ulteriori che il datore di lavoro, in qualità di titolare del trattamento, deve fornire all'interessato rientrano:

a) gli aspetti del rapporto di lavoro sui quali incide l'utilizzo di sistemi decisionali o di monitoraggio automatizzati;
b) il funzionamento dei sistemi;
c) i parametri principali utilizzati per programmare o addestrare i sistemi decisionali o di monitoraggio automatizzati, inclusi i meccanismi di valutazione delle prestazioni;
d) le misure di controllo adottate per le decisioni automatizzate, gli eventuali processi di correzione e il responsabile del sistema di gestione della qualità;
e) il livello di accuratezza, robustezza e cybersicurezza dei sistemi decisionali o di monitoraggio automatizzati e le metriche utilizzate per misurare tali parametri, nonché gli impatti potenzialmente discriminatori delle metriche stesse.

Tra gli elementi che, invece, specificano gli obblighi informativi di cui agli artt. 13 e 14 del GDPR, rientrano:

a) la logica dei sistemi decisionali o di monitoraggio automatizzati (la cui indicazione è espressamente richiesta dai menzionati articoli nel caso di ricorso ai processi decisionali automatizzati, compresa la profilazione, di cui all'art. 22 del GDPR; e
b) l'indicazione delle categorie di dati trattati (informazione richiesta ai sensi dell'art. 14(1)(d)), qualora i dati oggetto di

trattamento non siano ottenuti presso l'interessato.

Quanto al momento entro il quale devono essere assolti gli adempimenti informativa, fatto salvo quanto previsto dagli articoli 13 e 14 del GDPR, il Garante conferma che:

a) per i rapporti di lavoro instaurati anteriormente all'1° agosto 2022, è previsto che i dipendenti possano ottenere i predetti elementi informativi **a seguito di specifica richiesta scritta rivolta al datore di lavoro**;
b) per i rapporti di lavoro instaurati successivamente a tale data, gli obblighi informativi aggiuntivi devono essere adempiuti, per espressa disposizione normativa (art. 1(2), del D.Lgs. 152/1997), prima dell'inizio dell'attività lavorativa.

In un'ottica di evitare la frammentazione delle informazioni destinate agli interessati e nella prospettiva di una semplificazione degli adempimenti richiesti al datore di lavoro, il Garante consiglia *che tutte le informazioni siano complessivamente fornite al lavoratore prima dell'inizio del trattamento, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, e congiuntamente (quindi nello stesso documento) alle informazioni di cui agli artt. 13 e 14 del GDPR*.

- **Gli ulteriori adempimenti in materia di protezione dei dati personali**

In aggiunta a quanto sopra, considerato che l'impiego di sistemi di monitoraggio nel contesto lavorativo può comportare il trattamento di informazioni associate – direttamente o indirettamente – ai dipendenti, il datore di lavoro, titolare del trattamento, prima di effettuare trattamenti di dati personali dei lavoratori attraverso tali sistemi, dovrà altresì:

a) verificare la sussistenza di un idoneo presupposto di liceità, ai sensi degli artt. 5(1)(a) e 6 del GDPR,
b) verificare le condizioni per il lecito impiego di strumenti tecnologici nel contesto lavorativo, in particolare nel rispetto delle disposizioni dello Statuto dei lavoratori (ad es. verifica della sussistenza dei presupposti stabiliti dall'art. 4; rispetto delle disposizioni che vietano al datore di lavoro di acquisire e comunque trattare informazioni e fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore o comunque afferenti alla sua sfera privata); e
c) rispettare i principi generali della normativa in materia di privacy, nonché porre in essere tutti gli adempimenti previsti dalla normativa applicabile.

In ogni caso, il Garante ha ribadito che l'introduzione delle nuove garanzie non modifica le tutele già previste dal GDPR e dallo Statuto dei lavoratori.

Il trattamento, inoltre, dovrà essere oggetto, da parte del datore di lavoro, di una **valutazione dei rischi per verificarne l'impatto sui diritti e sulle libertà degli interessati** e, laddove sia necessario – in ragione delle tecnologie impiegate e considerata la natura, l'oggetto, il contesto e le finalità perseguite – di una **preventiva valutazione di impatto sulla protezione dei dati personali**, ai sensi dell'art. 35 del GDPR ("**DPIA**"), obbligatoria qualora "si faccia ricorso a "*una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche*".

Nel verificare la necessità di procedere con una DPIA – come indicato nelle Linee Guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati – il titolare del trattamento deve considerare altresì la

vulnerabilità degli interessati nel contesto lavorativo, nonché la circostanza che l'impiego nell'ambito lavorativo di sistemi che comportano il monitoraggio sistematico, può presentare rischi, in termini di possibile monitoraggio dell'attività dei dipendenti.

Sul punto, il Garante Privacy ricorda che nella maggior parte dei casi, un titolare del trattamento può considerare che un trattamento che soddisfi almeno due criteri debba formare oggetto di una DPIA e che maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che configuri un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati.

In tale quadro, rimane ferma la necessità di **rispettare il principio di *privacy by design* e *privacy by default***: da un lato, mediante l'adozione di misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati e integrando nel trattamento le necessarie garanzie per soddisfare i requisiti del GDPR e tutelare i diritti e le libertà degli interessati; dall'altro, ponendo in essere scelte tali da garantire che venga effettuato, per impostazione predefinita, solo il trattamento strettamente necessario per conseguire una specifica e lecita finalità.

In attuazione di tali principi, il titolare del trattamento, anche quando utilizza sistemi tecnologici realizzati da terzi, dovrà eseguire, avvalendosi del supporto del DPO, ove nominato, un'analisi dei rischi e accertarsi che siano disattivate le funzioni che non hanno una base giuridica, non sono compatibili con le finalità del trattamento, ovvero si pongono in contrasto con specifiche norme di settore previste dall'ordinamento, in particolare le norme nazionali che disciplinano le condizioni per l'impiego degli strumenti tecnologici sul posto di lavoro.

Tra gli obblighi generali connessi alle attività di trattamento dei dati personali, vi è altresì l'obbligo della tenuta e dell'aggiornamento del Registro delle attività di trattamento (obbligo che sussiste nelle ipotesi individuate dall'articolo 30 ma che rappresenta una delle misure organizzative più idonee a dimostrare l'accountability del titolare).

Tale registro consente di fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione ed è **indispensabile per consentire al titolare di censire i trattamenti effettuati** e documentarne la conformità alla disciplina in materia di protezione dei dati personali.

Conclusioni

Anche alla luce delle osservazioni del Garante, al fine di adempiere agli obblighi introdotti dal Decreto Trasparenza, si consiglia di:

- analizzare le condizioni contrattuali standard che il datore sottopone ai propri dipendenti al momento dell'instaurazione del rapporto di lavoro, assicurandosi che tutti gli elementi della norma di riferimento siano già ivi ricompresi e, in caso negativo, procedere quanto prima alla loro integrazione;
- mappare i sistemi decisionali o di monitoraggio automatizzati utilizzati e che rientrino nell'ambito di applicazione individuato dalla norma e dalle relative circolari interpretative – anche attraverso la tenuta e l'aggiornamento del registro;
- effettuare una valutazione dei rischi per verificare l'impatto dei trattamenti sui diritti e sulle libertà degli interessati e, laddove sia necessario – in ragione delle tecnologie impiegate e considerata la natura, l'oggetto, il contesto e le finalità perseguite – una preventiva valutazione di impatto sulla protezione dei dati personali, ai sensi dell'art. 35 del GDPR;

- verificare la sussistenza di idonei presupposti di liceità che giustifichi i trattamenti e prevedere che l'utilizzo di tali sistemi rispetti i principi in materia di protezione dei dati personali;
- assicurarsi che l'informativa sul trattamento dei dati personali dei dipendenti contenga le ulteriori informazioni richieste dalle disposizioni introdotte dal Decreto Trasparenza.

Naturalmente, ove tali sistemi automatizzati dovessero comportare forme, anche solo potenziali, di controllo dell'attività dei lavoratori, sarebbe necessario seguire le procedure di confronto sindacale o amministrative previste dallo Statuto dei Lavoratori.

* * *

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