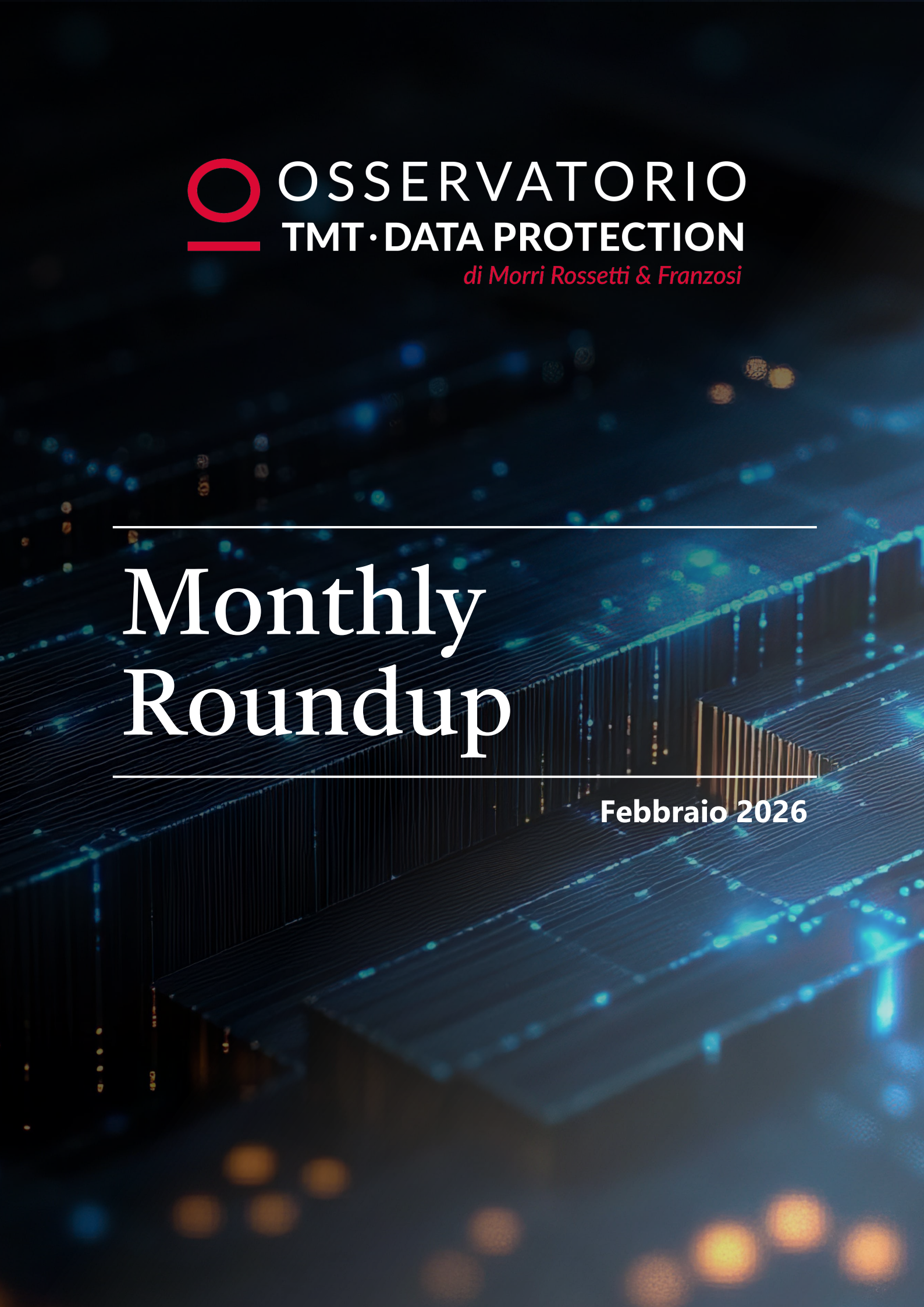

OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti & Franzosi

Monthly Roundup

Febbraio 2026

Febbraio 2026

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

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

GARANTE PRIVACY

- Il Garante privacy sanziona eCampus, stop al riconoscimento facciale; [Link]
- Garante privacy al comune di Pescara: no alle body cam della Polizia locale; [Link]
- Dal Garante ok alle Linee guida Agid su accessibilità dei servizi. [Link]

EDPB

- EDPB-EDPS Joint opinion 2/2026 on the Proposal for Regulation as regards the simplification of the digital legislative framework (Digital Omnibus); [Link]
- EDPB Work Programme 2026-2027; [Link]
- Coordinated Enforcement Action, implementation of the right to erasure by controllers. [Link]

AGCOM

- Siti e piattaforme porno: dal 1° febbraio scatta l'obbligo di verifica dell'età anche per i siti stabiliti in paesi UE diversi dall'Italia; [Link]
- Segnalazione Fieg sui servizi AI di Google: il Consiglio dispone l'audizione delle parti. [Link]

Canali whistleblowing sotto la lente del Garante: novità ANAC e check di conformità per le aziende

Con la **Deliberazione 30 dicembre 2025, n. 797**, l'Autorità Garante per la protezione dei dati personali (il "**Garante**" o l'"**Autorità**") ha definito il piano ispettivo per il semestre gennaio-luglio 2026, che, tra le varie attività, prevede – in continuità con il semestre precedente – attività ispettive aventi ad oggetto il tema *whistleblowing*.

Per chiarezza, con "*whistleblowing*" si intende, ai sensi del D.lgs. 24/2023 (il **"Decreto WB**") – che ha recepito nell'ordinamento italiano la direttiva UE 20/19/1937 riguardante "*la protezione delle persone che segnalano violazioni del diritto dell'Unione*" (c.d. Whistleblowing), qualsiasi segnalazione, proveniente da chiunque, riguardante la comunicazione di informazioni su comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità di una società e ai quali il segnalante abbia assistito in ragione dello svolgimento della propria attività lavorativa o professionale (di seguito "**Segnalazione**").

Di particolare rilievo, al riguardo, sono le violazioni rilevanti ai sensi del D.lgs. 8 giugno 2001, n. 231 ("**Decreto 231**"), e quindi le condotte penalmente rilevanti ai sensi degli artt. 24 e ss. del Decreto 231, nonché le infrazioni del Modello Organizzativo 231, del Codice Etico e, più in generale, delle diverse componenti del sistema di regole e procedure eventualmente adottate dalle società.

La normativa *whistleblowing* richiede espressamente l'implementazione di diverse tipologie di canali di segnalazione, preferendo quelli informatici. Infatti, attraverso tali *software*/applicativi, è possibile adottare stringenti misure di sicurezza e assicurare un maggiore livello di protezione dei dati personali tanto nella fase di acquisizione delle Segnalazioni quanto in quella di gestione delle stesse.

D'altra parte, le piattaforme, adeguatamente progettate e configurate, assicurano di cifrare i dati a riposo e di mantenere una interlocuzione riservata con la persona segnalante.

Il tema della protezione dei dati è infatti centrale nella gestione delle Segnalazioni, imponendo di conseguenza lo svolgimento di valutazioni e lo svolgimento di specifici adempimenti nel rispetto del Regolamento Generale (UE) 2016/679 ("**GDPR**"), del D. Lgs. n. 196/2003, come modificato dal D. Lgs. n. 101/2018 ("**Codice Privacy**").

Premesso quanto sopra, **l'attività ispettiva del Garante prevede proprio la prosecuzione delle verifiche sull'utilizzo degli applicativi maggiormente diffusi per l'acquisizione e la gestione delle segnalazioni whistleblowing.**

Ma prima di comprendere come si possono preparare le aziende per eventuali controlli, è necessario analizzare le recenti novità introdotte dall'Autorità Nazionale Anticorruzione ("**ANAC**").

I principali aggiornamenti dell'ANAC

L'ANAC ha di recente emanato due provvedimenti: la **Delibera n. 478 del 26 novembre 2025**, contenente le nuove linee guida sui canali interni di segnalazione ("**LG Canali Interni**"), e la **Delibera n. 479 del 26 novembre 2025**, con cui vengono aggiornate e integrate le precedenti Linee guida n. 311/2023 allo scopo di assicurarne una coerenza complessiva

(complessivamente intesi, "**Aggiornamenti ANAC**").

L'obbiettivo degli Aggiornamenti ANAC è quello di garantire una maggiore omogeneità ed efficienza nell'intero sistema di gestione delle Segnalazioni, assicurando e mantenendo la piena tutela della riservatezza dell'identità del segnalante, del contenuto della Segnalazione e dei dati personali di tutti i soggetti coinvolti.

Le principali novità sono contenute principalmente nel documento LG Canali interni, ove l'ANAC affronta espressamente per la prima volta il tema della **condivisione dei canali interni all'interno di gruppi di imprese**.

Nello specifico, l'ANAC individua **due diverse soluzioni** praticabili a seconda del numero di lavoratori impiegati.

Nel caso di società di gruppi che impiegano "**fino a 249 lavoratori**", le stesse possono, in via alternativa:

- condividere il canale interno; o
- affidare la gestione del canale di segnalazione a terzi (c.d. esternalizzazione), che, in riferimento ai gruppi di imprese, può coincidere anche con la capogruppo.

Diversamente, qualora i **dipendenti siano più di 249**, l'unica soluzione praticabile sarà l'affidamento della gestione del canale di segnalazione a terzi (c.d. esternalizzazione).

Ora, quali sono i principali adempimenti per una corretta implementazione delle novità ANAC?

Se si fa riferimento a un gruppo, dove la singola impresa ha meno di 249 lavoratori e la Società intende condividere il canale, la stessa dovrà:

a. nominare un gestore della segnalazione in riferimento a ciascuna società del gruppo;
b. adottate misure tecniche e organizzative per garantire che ciascun gestore abbia accesso solo alle segnalazioni relative alla propria società. Nei gruppi societari, ciò si traduce, ad esempio, nell'istituzione di una piattaforma unica ma ramificata a livello di gruppo, con tanti sotto-canali quante sono le società del gruppo (la società acquisisce la segnalazione attraverso il sotto-canale e tratta e istruisce le segnalazioni attraverso il proprio gestore). La singola società, ricevuta la segnalazione, ove opportuno, potrà avvalersi della capacità investigativa della capogruppo, previa informativa al segnalante;
c. stipulare un contratto che definisca compiti e responsabilità nell'ambito di tale rapporto;
d. ciascuna società dovrà dare conto della scelta della condivisione del canale interno e della relativa gestione nell'atto organizzativo/MOG.

In riferimento ai ruoli privacy delle parti, le LG Canali Interni prevedono espressamente: ove sia previsto questo tipo di condivisione del canale interno, pur venendo in rilievo l'ipotesi della condivisione, non potrà configurarsi una contitolarità del trattamento ex art. 26 del GDPR, dovendosi – al contrario – far riferimento a un rapporto titolare/responsabile di cui all'art. 28 del GDPR, con conseguente qualifica della capogruppo come responsabile del trattamento.

Al contrario, tutti i gruppi di imprese, a prescindere dalla soglia dimensionale, possono ricorrere alla cd. Esternalizzazione.

Ove sia applichi questo scenario, le imprese dovranno:

a. stipulare un contratto di affidamento con il soggetto terzo che disciplini:

- le modalità di ricezione delle segnalazioni;

- il ruolo e i compiti dei soggetti che gestiscono le segnalazioni;
- le modalità e i termini di conservazione dei dati;
- le ipotesi di conflitto di interessi;
- le fasi della procedura di gestione delle segnalazioni e relative tempistiche.

In questi casi, il soggetto terzo dovrà essere nominato responsabile del trattamento *ex* art. 28 del GDPR.

b. Nominare un referente interno per assicurare il coordinamento con il gestore. Ogni società del gruppo deve infatti avere contezza solo delle segnalazioni di propria spettanza affinché il relativo organo di indirizzo possa adottare gli eventuali provvedimenti conseguenti agli esiti dell'istruttoria svolta dal gestore.

Il parere del Garante privacy sulle Linee guida ANAC in materia di *whistleblowing*

Per completezza, occorre menzionare altresì che il Garante ha espresso il proprio parere positivo sugli Aggiornamenti ANAC, limitandosi ad apportare alcune precisazioni al fine di garantirne la piena conformità al GDPR e al Decreto WB.

In particolare, viene ribadito l'obbligo per gli enti pubblici e privati di adottare canali interni caratterizzati da elevati standard di sicurezza, mediante misure tecniche e organizzative idonee a tutelare l'identità del segnalante, del segnalato e dei terzi coinvolti.

Particolare rilievo è attribuito, inoltre, all'obbligo di effettuare una valutazione di impatto sulla protezione dei dati (DPIA), nonché alla possibilità di esternalizzare la gestione del canale, con qualificazione del fornitore quale responsabile del trattamento ai sensi dell'art. 28 GDPR, e alla condivisione del canale tra più enti, purché sia garantito un accesso selettivo e conforme ai principi di sicurezza e riservatezza.

Elementi da attenzionare in caso di attività ispettive del Garante

Le imprese destinatarie degli obblighi di cui alla normativa *Whistleblowing* sono tenute, in un'ottica di adeguamento preventivo e secondo un criterio meramente esemplificativo, ad adottare i seguenti presidi organizzativi e tecnici:

- **segregazione degli accessi e tracciabilità dei log:** devono essere definiti profili autorizzativi coerenti con il principio del privilegio minimo, assicurando che si possa accedere esclusivamente ai dati e alle funzionalità strettamente necessari allo svolgimento delle proprie mansioni. In particolare, deve essere garantita una chiara separazione funzionale tra i soggetti preposti della ricezione e istruttoria delle Segnalazioni e coloro che esercitano attività di amministrazione dei sistemi informativi;
- **tutela dell'identità del segnalante attraverso misure di sicurezza tecniche** (es., cifratura, pseudonimizzazione, etc.);
- **limitazione della conservazione e cancellazione dei dati:** devono essere predeterminati termini di conservazione coerenti con le finalità del trattamento, implementando ove possibili meccanismi di cancellazione automatica o di blocco dei dati, con eventuali deroghe adeguatamente motivate e documentate.
- **gestione dei fornitori e dei rischi connessi agli applicativi informatici:** i rapporti con i fornitori devono essere disciplinati mediante accordi sul trattamento dei dati (DPA) e clausole contrattuali idonee a regolamentare subfornitori, localizzazione dei dati e trasferimenti verso Paesi terzi. Infine, le misure di sicurezza dichiarate devono essere verificabili e documentate attraverso apposita **DPIA** che deve essere effettiva, aggiornata e coerente con l'evoluzione del sistema.

Data breach: le novità del DL PNRR e del Digital Omnibus

Solo nel mese di gennaio 2026 in Italia sono stati registrati complessivamente 225 eventi *cyber*, con un aumento del 42% rispetto ai 158 rilevati nel mese precedente[1].

Questi dati descrivono una dinamica ormai nota: il numero di eventi di sicurezza cresce in modo costante, mentre sempre più organizzazioni – spesso di dimensioni ridotte – si trovano a dover affrontare decisioni complesse in tempi molto rapidi. Una di queste decisioni riguarda la gestione delle violazioni di dati personali e, in particolare, la scelta se notificare o meno l'incidente all'autorità di controllo.

È in questo contesto che si inserisce **il D.L. 19/2026**, recante ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza e in materia di politiche di coesione (il "**DL PNRR**" o il "**Decreto**").

Il Decreto, approvato dal Consiglio dei ministri lo scorso 29 gennaio, introduce una revisione organica di oltre 400 adempimenti amministrativi. Tra le novità più interessanti figura una misura destinata a incidere direttamente sulla gestione dei *data breach*: l'introduzione di una **procedura semplificata per le imprese con meno di 5 dipendenti**.

La modifica interviene direttamente sul Codice Privacy (D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018) attraverso l'inserimento del nuovo articolo 2-*quaterdecies*.1, rubricato "*Procedura di notifica delle violazione di dati personali da parte di microimprese*".

Ma cosa cambia nella pratica per le imprese interessate?

Il punto di partenza: l'obbligo di notifica dei *data breach*

Per comprendere la portata della riforma occorre partire dalla disciplina generale contenuta nel GDPR (Reg. UE 679/2019). L'articolo 33 del GDPR stabilisce che, in caso di violazione di dati personali – il c.d. *data breach* – il titolare del trattamento deve notificare l'incidente all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.

L'obbligo non sussiste soltanto quando sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche.

In termini concreti, ciò significa che ogni qualvolta venga compromessa la riservatezza, l'integrità o la disponibilità di dati personali, il titolare, salvo l'eccezione prevista dal GDPR, deve notificare l'incidente al Garante Privacy, utilizzando la piattaforma telematica disponibile sul sito dell'Autorità.

Il punto più delicato non è tuttavia l'adempimento formale della notifica, bensì la valutazione che lo precede. L'architettura dell'articolo 33 GDPR si fonda infatti su una valutazione preventiva del rischio. Il titolare deve stabilire se la violazione sia idonea a produrre un rischio per i diritti e le libertà degli interessati e,

[1] Agenzia per la Cybersicurezza Nazionale, Operational Summary, Dati e indicatori della minaccia cyber in Italia, gennaio 2026.

soprattutto, se tale rischio sia sufficientemente significativo da giustificare la notifica.

Si tratta di un passaggio che richiede competenze tecniche, giuridiche e organizzative. Nella pratica, la decisione di notificare un *data breach* nasce quasi sempre da un confronto tra responsabili IT, DPO (ove nominato), consulenti privacy e legali, spesso in tempi estremamente ristretti.

Per le grandi organizzazioni questo processo è spesso parte delle procedure interne di gestione degli incidenti. Per le microimprese, invece, il quadro è molto diverso: la stessa valutazione del rischio potrebbe diventare un esercizio complesso, quando non addirittura paralizzante. Ed è proprio su questo punto che interviene la novità introdotta dal DL PNRR.

La procedura semplificata per le microimprese

Il DL PNRR inserisce nel Codice Privacy una disciplina specifica destinata alle imprese con meno di 5 dipendenti, prevedendo l'introduzione di una procedura semplificata per la notifica dei *data breach* ai sensi dell'articolo 33 del GDPR. La norma non definisce direttamente i dettagli tecnici della procedura, ma demanda al Garante Privacy il compito di definirli attraverso un proprio provvedimento.

Tuttavia, il Decreto indica due elementi che dovranno necessariamente caratterizzare il nuovo sistema. Da un lato, l'introduzione di strumenti di **autovalutazione guidata**, destinati presumibilmente ad aiutare le microimprese a orientarsi nella valutazione del rischio e a comprendere se una violazione richieda o meno la notifica.

Dall'altro, la previsione di un **canale di assistenza semplificata**, pensato per supportare le imprese tenute alla notifica.

***Data breach* e Digital Omnibus**

Parallelamente alle novità introdotte dal legislatore italiano, il tema delle notifiche di *data breach* è oggetto di una riflessione anche a livello europeo. Il 19 novembre 2025, la Commissione europea ha presentato la proposta COM(2025) 837, il c.d. *Digital Omnibus* (il "**Digital Omnibus**" o la "**Proposta**").

Tra i diversi interventi prospettati, vi è anche una revisione della disciplina delle notifiche di *data breach* prevista dall'articolo 33 del GDPR.

La Proposta introduce innanzitutto un cambiamento concettuale significativo. L'obbligo di notifica all'autorità di controllo verrebbe allineato all'obbligo di comunicazione agli interessati, prevedendo che la notifica sia richiesta soltanto quando la violazione comporti un rischio elevato per i diritti degli interessati.

In altre parole, verrebbe superato l'attuale modello a due soglie – "rischio" per la notifica all'autorità, "rischio elevato" per la comunicazione agli interessati – a favore di un criterio unico più selettivo. La Proposta introduce inoltre un'estensione del termine per la notifica, che passerebbe dalle attuali 72 ore a **96 ore**.

Un altro elemento di rilievo è la previsione di un **punto di accesso unico** per la segnalazione degli incidenti. L'obiettivo è consentire ai soggetti obbligati di adempiere, attraverso un'unica interfaccia, agli obblighi di notifica previsti da diverse normative europee[2], tra cui quelli relativi

[2] [2] Il punto di accesso unico per la segnalazione degli incidenti dovrebbe consentire ai soggetti di adempiere agli obblighi di segnalazione a norma delle direttive (UE) 2022/2555 (Direttiva NIS2) e (UE) 2022/2557 (Direttiva CER), del GDPR e dei regolamenti (UE) 2022/2554 (DORA) e (UE) n. 910/2014 (eIDAS), inviando le notifiche tramite un'unica interfaccia. Il punto di accesso unico dovrebbe iniziare a essere utilizzato ai fini della segnalazione a norma di tali atti entro 18 mesi dall'entrata in vigore del Digital Omnibus.

agli incidenti di sicurezza disciplinati dalla normativa NIS2.

Infine, il Digital Omnibus attribuisce all'EDPB (*European Data Protection Board*) il compito di elaborare un modello comune per la notifica delle violazioni dei dati personali e un elenco condiviso di circostanze nelle quali una violazione può essere considerata idonea a generare un rischio elevato per i diritti e le libertà delle persone fisiche.

Conclusioni: perché è necessario leggere insieme queste due riforme

Le due iniziative normative – da un lato il DL PNRR e dall'altro il Digital Omnibus – operano su piani diversi, ma intervengono sullo stesso tema: come rendere più chiara e gestibile la decisione di notificare un *data breach*.

La procedura semplificata prevista per le microimprese rappresenta un primo tentativo di tradurre in strumenti operativi un obbligo che, nella sua formulazione attuale, richiede valutazioni spesso complesse.

Tuttavia, il quadro normativo europeo resta ancora in evoluzione. Per questo motivo le due riforme dovranno essere monitorate in parallelo. La procedura guidata che il Garante Privacy sarà chiamato a sviluppare dovrà inevitabilmente confrontarsi con l'evoluzione dell'articolo 33 GDPR e con gli eventuali modelli comuni che potranno emergere a livello europeo.

* * *

The EU-U.S. Data Privacy Framework and international data transfers: insights from the updated EDPB FAQs for European businesses

For many European organizations, transferring personal data to the United States has long been one of the most legally sensitive aspects of GDPR compliance. The invalidation of previous legal framework created uncertainty and forced companies to rely heavily on Standard Contractual Clauses ("**SCC**") and complex transfer assessments.

The EU-U.S. Data Privacy Framework ("**DPF**") reshapes this landscape, but it does not eliminate the need for careful legal and operational checks under the GDPR. This article analyses the updated DPF FAQs, originally adopted in 2024 and most recently revised on 15 January 2026, which clarify how EU and EEA organizations can lawfully rely on the DPF in a way that is both operationally practical and fully aligned with GDPR requirements.

The legal nature of the DPF and criteria to have in order to be eligible to the DPF

The DPF is a **self-certification mechanism** for U.S.-based organizations. Companies that have self-certified under the DPF commit to comply with a detailed set of privacy principles, rules and obligations governing the processing of personal data received from the EEA.

On 10 July 2023, the European Commission adopted an adequacy decision under Article 45 of

the GDPR, recognizing that transfers to U.S. organizations actively certified under the DPF do not require additional safeguards, such as SCCs, for those specific data flows.

To be eligible to self-certify to the DPF, a company in the U.S. must be subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission ("**FTC**") or of the U.S. Department of Transportation ("**DoT**"). However, other U.S. statutory bodies may be included in the future.

As a result, certain entities such as, for example, non-profit organizations, banks, insurance companies and telecommunication service providers (with regard to common carrier activities) which do not fall under the jurisdiction of the FTC or DoT, cannot self-certify under the DPF.

Responsibilities of the EEA exporter

Before transferring personal data to a U.S. company under the DPF, an EEA data exporter must ensure that the U.S. company has an active self-certification (which must be renewed annually) and that this certification applies to the data being transferred.

The DPF List on the U.S. Department of Commerce website allows EEA exporters to check whether a company's self-certification is active and applicable. Since self-certifications must be renewed annually, it also lists companies removed from the program ("inactive participants") and the reasons for removal.

It follows that EEA exporters cannot rely on the DPF for transfers of personal data to companies that do not hold an active self-certification, while companies that have been removed from the DPF List must continue to apply the DPF Principles to any personal data received while they were participants, for as long as they retain such data.

For transfers to U.S. companies that are not (or no longer) DPF-certified, other transfer mechanisms under Articles 46-49 GDPR, such as Binding Corporate Rules or SCCs, remain available.

Particular attention shall be given to group of undertakings: in case of transfers to companies in the U.S. that are subsidiaries of a DPF-certified parent company, EEA data exporters must check if the certification of the parent company also covers the subsidiary company concerned.

HR Data: additional compliance considerations

It is important to note that the DPF applies to all types of personal data transferred from the EEA to the U.S., including data processed for commercial or health purposes, as well as human resources data collected in the context of an employment relationship ("**HR Data**"), provided that the U.S. recipient company is self-certified under the DPF to process those categories of data.
However, transfer of HR Data (such as employee records, payroll information, etc.) require additional care.

The DPF allows such transfer only where the U.S. organization's certification explicitly covers HR Data or where the organization has committed, in its privacy policy, to cooperate with and comply with the advice of EU supervisory authorities in relation to that data

Transfers to a company in the U.S. acting as a controller

Before transferring personal data to a U.S. controller, an EEA data exporter must ensure that the transfer aligns with all applicable GDPR provisions. It is important indeed, that personal data are shared with a U.S. entity if a lawful basis for processing exists under Article 6 of the GDPR.

Depending on the context, this may be contractual obligation, legal obligation, or legitimate interests, but it must be properly documented and assessed. Beyond this, compliance with the full spectrum of GDPR obligations – including purpose limitation, proportionality, data accuracy, and transparency toward data subjects – is required.

Transparency obligations remain central. Under Articles 13 and 14 GDPR, data subjects must be informed about the identity of the U.S. recipient and the fact that their personal data is transferred on the basis of an adequacy decision under the DPF. This transparency requirement underscores the GDPR's emphasis on accountability and the protection of fundamental data subject rights in cross-border transfers.

Transfers to a company in the U.S. acting as a processor

Where the U.S. organization processes personal data on behalf of the EEA exporter, whether or not the fact that the processor is self-certified under the DPF, the parties are obliged to conclude a data processing agreement ("**DPA**") under Article 28 GDPR.

The DPA must define the subject matter and duration of the processing, its nature and purpose, as well as the type of personal data processed and the categories of data subjects to whom personal data refers. It must also impose specific obligations on the processor, including processing only on documented instructions, ensuring confidentiality of personnel, implementing appropriate technical and organizational measures under Article 32 GDPR, and assisting the controller with data subject rights and security obligations.

The processor must also commit to deleting or returning personal data at the end of the service and to making available all information necessary to demonstrate compliance, including through audits.

Where the processor engages a sub-processor, it must flow down the same data protection obligations and remain fully liable to the controller for the sub-processor's performance. These contractual safeguards operate alongside the DPF commitments and are a core element of GDPR accountability.

A Practical Compliance Perspective

Operationally, the DPF addresses a specific legal obstacle, without modifying the broader framework established by the GDPR. In other words, it streamlines the analysis of international data transfers but does not diminish an organization's obligations with respect to the lawfulness of processing, fairness and transparency towards data subjects, data security, and overall accountability.

Organizations that integrate DPF verification into corporate processes – including procurement, vendor management, human resources, and privacy governance – will be best positioned to leverage the framework while remaining fully GDPR-compliant.

In nutshell, the DPF facilitates more efficient transatlantic data flows, but only if exporters continue to apply the GDPR with the same degree of diligence and rigor as before. Absent such a comprehensive approach, reliance on the DPF alone does not guarantee full compliance, nor does it eliminate the need for thorough operational and legal assessments.

Per maggiori informazioni e approfondimenti

Carlo Impalà

Partner e Responsabile Osservatorio TMT&DP

Carlo.Impala@MorriRossetti.it

Morri Rossetti & Franzosi **Osservatorio TMT&DP**

OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti & Franzosi

Piazza Eleonora Duse, 2
20122 Milano
MorriRossetti.it

Osservatorio-dataprotection.it