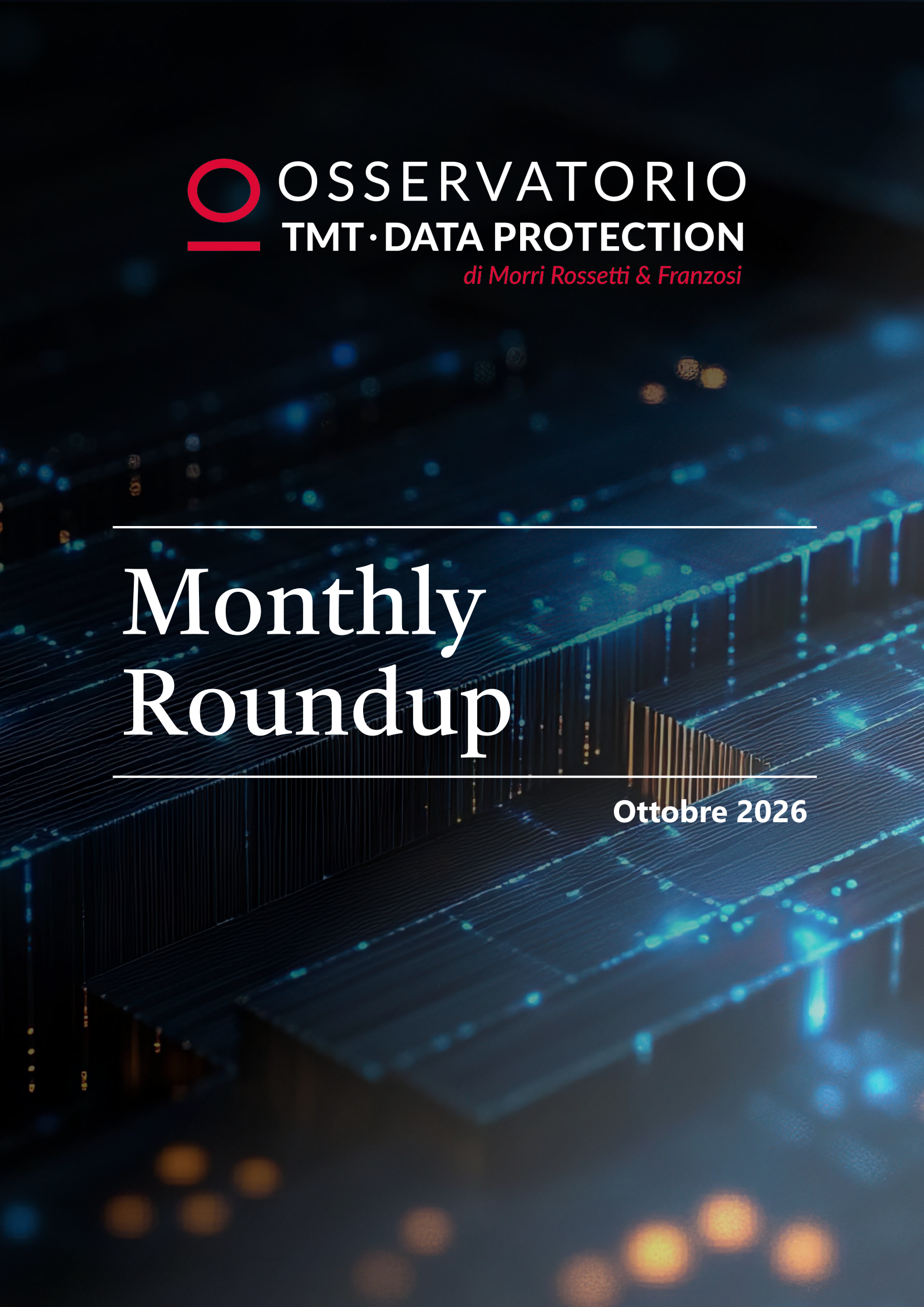


OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti & Franzosi

Monthly Roundup

Ottobre 2026

Ottobre 2026

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

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

GARANTE PRIVACY

- Email marketing, in vigore le Linee guida sui tracking pixel; [Link]
- Vita digitale e dati personali Il Garante incontra le Associazioni dei consumatori; [Link]
- Sistemi di Informazione Creditizia (SIC), importanti chiarimenti dal Garante Privacy; [Link]
- Via libera all'IT-Wallet; [Link]
- Garanti europei, la tutela della privacy per i bambini. [Link]

EDPB

- L'EDPB pubblica una dichiarazione sulle sfide in materia di protezione dei dati degli occhiali intelligenti; [Link]

ACN

- NIS: ACN incontra la Commissione europea; [Link]
- ACN semplifica la registrazione NIS 2027; [Link]
- Online l'Operational summary di ACN con I dati e gli indicatori della minaccia cyber in Italia. [Link]

NIS2: dalla registrazione alle verifiche, cosa cambia per i soggetti NIS con la Determinazione 314287/2026



Con la Determinazione n. 314287 del 20 ottobre 2026, applicabile a partire dal 25 ottobre, l'Agenzia per la Cybersicurezza Nazionale ("**ACN**") ha aggiornato e sostituito la precedente Determinazione n. 127437/2026, riguardante le modalità di utilizzo e accesso alla piattaforma digitale ACN (la "**Piattaforma**").

La nuova Determinazione semplifica la registrazione annuale per i soggetti già presenti nell'elenco, disciplina gli effetti di alcune operazioni societarie e rafforza i meccanismi di verifica delle informazioni comunicate all'ACN.
L'obiettivo è quello di rendere più agevole il percorso di accreditamento alla Piattaforma. **Ma quali sono le principali novità per le imprese?**

Registrazione annuale e continuità dello "*status* NIS"

Una delle principali semplificazioni riguarda le organizzazioni già registrate e presenti nell'elenco dei soggetti NIS. Se le informazioni precedentemente comunicate non sono cambiate, non sarà necessario effettuare nuovamente la registrazione annuale nella finestra dal 1° gennaio al 28 febbraio.

La semplificazione opera, in particolare, quando non siano intervenute modifiche rispetto alle informazioni contenute nella dichiarazione presentata nell'annualità precedente o nelle successive dichiarazioni integrative trasmesse nel corso della medesima annualità. In questi casi, l'ACN comunicherà comunque al soggetto, a fini ricognitivi, la sua permanenza nell'elenco dei soggetti NIS.

Cosa significa in pratica? Un soggetto registrato nel 2026 che non abbia modificato le informazioni già comunicate non dovrà ripetere la registrazione nel 2027.

Se, invece, tali informazioni sono cambiate, dovrà procedere alla nuova registrazione, descrivendo le modifiche intervenute. Qualora la variazione riguardi la rimozione di una o più tipologie di soggetto, dovranno essere indicate anche le relative motivazioni.

La continuità riguarda anche la qualificazione del soggetto. In assenza di variazioni, i soggetti già iscritti mantengono infatti lo "**status NIS**", come soggetto essenziale o importante, attribuito nell'annualità precedente.

La Determinazione introduce inoltre una **valutazione preliminare dello status NIS**: al termine della compilazione della dichiarazione, il soggetto potrà confermare la valutazione proposta oppure contestarla, fornendo le relative motivazioni.

La semplificazione, quindi, non elimina la necessità per le imprese di tenere sotto controllo le informazioni precedentemente trasmesse. Al contrario, rende ancora più importante disporre di un processo interno che consenta di individuare tempestivamente eventuali variazioni rilevanti ai fini NIS2.

Registrazione e operazioni societarie

L'ACN disciplina espressamente anche gli effetti di alcune operazioni societarie sulla registrazione NIS. In caso di **fusione**, anche per incorporazione, se almeno uno dei soggetti partecipanti rientra

nell'ambito di applicazione del Decreto NIS2, il soggetto risultante dall'operazione è tenuto a registrarsi. I soggetti NIS partecipanti alla fusione devono, inoltre, comunicare i dati identificativi del soggetto risultante dall'operazione.

Un obbligo informativo è previsto anche in caso di **cessione di uno o più rami d'azienda** relativi alle attività che hanno determinato l'inclusione del soggetto nell'ambito di applicazione del Decreto NIS2. In questa ipotesi, il soggetto NIS deve comunicare i dati identificativi del cessionario.

Accesso alla Piattaforma: nuove modalità di autenticazione

Cambiano anche le modalità di accesso alla Piattaforma. A SPID e CIE si aggiungono la Carta Nazionale dei Servizi (**CNS**) e l'autenticazione tramite **eIDAS** [1], ampliando così le modalità attraverso le quali gli utenti possono identificarsi e accedere ai servizi della Piattaforma.

Per gli utenti che non possano disporre di credenziali SPID, CIE, CNS o eIDAS, è inoltre prevista la possibilità di richiedere credenziali personali. La relativa procedura può essere avviata direttamente dalla Piattaforma attraverso la funzione "*Richiedi credenziali*" (*cfr*. FAQ ACC.1).

Registrazioni tardive: cambia la gestione delle dichiarazioni

La Determinazione interviene anche sulla gestione delle registrazioni tardive.
Dal **31 ottobre 2026** non sarà più possibile trasmettere tali dichiarazioni attraverso la Piattaforma per l'anno 2026, in modo da consentire l'introduzione delle modifiche previste dalla nuova Determinazione.

Per le annualità successive viene invece precisato che le dichiarazioni tardive presentate entro il 1° settembre saranno trattate ai fini della registrazione nell'annualità di riferimento.

Controlli sulle informazioni comunicate in sede di registrazione: le verifiche di coerenza

Accanto alle semplificazioni, la nuova disciplina rafforza i meccanismi attraverso i quali l'ACN può verificare le informazioni comunicate dai soggetti NIS in sede di registrazione.

L'ACN può effettuare verifiche di coerenza, d'ufficio e a campione, anche con strumenti automatizzati, e, se lo ritiene necessario, può richiedere attraverso la Piattaforma informazioni aggiuntive, modifiche o integrazioni della dichiarazione.

Il soggetto NIS deve rispondere **entro 10 giorni** dalla richiesta. In caso di risposta tardiva, l'ACN procede alla valutazione sulla base delle informazioni disponibili, con la possibilità che ne derivi una valutazione dello status NIS differente rispetto a quello corrente o rispetto alla valutazione preliminare generata dalla Piattaforma.

Sono inoltre previste ulteriori verifiche di coerenza entro 60 giorni[2] dalla comunicazione di inserimento, permanenza (con variazioni o meno), espunzione o mancato inserimento per carenza dei presupposti nell'elenco dei soggetti NIS. In questi casi, i soggetti NIS possono

[1] Il Regolamento eIDAS (Reg. UE 910/2014) rappresenta la base normativa per le interazioni elettroniche tra imprese, cittadini e autorità pubbliche, migliorando la sicurezza e l'efficienza dei servizi online e delle transazioni commerciali elettroniche nell'UE. La sua implementazione consente l'uso delle identità digitali italiani negli altri Stati membri dell'UE.

[2] Il termine può essere prorogato dall'ACN per una sola volta e fino a un massimo di ulteriori 30 giorni se necessario svolgere approfondimenti.

presentare istanza di revisione entro 60 giorni dalla ricezione della comunicazione.

Per i soggetti NIS il punto non è soltanto assicurarsi che la dichiarazione sia completa al momento della trasmissione. Diventa altrettanto importante conservare gli elementi sulla base dei quali sono state effettuate le valutazioni e organizzarsi internamente per poter rispondere tempestivamente a eventuali richieste dell'ACN.

Aggiornamento annuale delle informazioni

La Determinazione introduce l'obbligo di verificare la correttezza e l'aggiornamento delle **informazioni trasmesse in sede di registrazione** nell'ambito dell'aggiornamento annuale delle informazioni, da effettuarsi tra il 15 aprile e il 31 maggio.

Fermo restando il controllo delle ulteriori informazioni già oggetto dell'aggiornamento annuale (quali, ad esempio, l'elenco dei componenti degli organi amministrativi e direttivi, gli indirizzi IP e i nomi di dominio e i fornitori rilevanti), la verifica interesserà quindi anche:

- il codice fiscale della capogruppo (ove applicabile);
- (ove applicabile) l'indicazione delle imprese collegate nei confronti delle quali il soggetto NIS soddisfa almeno uno dei criteri di cui all'art. 3, co. 10, del Decreto NIS2 (influenza dominante sulle decisioni relative alle misure di gestione del rischio; detenzione/gestione dei sistemi informativi e di rete da cui dipende la fornitura dei servizi; svolgimento di operazioni di cybersicurezza; fornitura di servizi ICT o di sicurezza, anche gestiti);
- (ove applicabile) l'indicazione delle imprese collegate che soddisfano nei confronti del soggetto NIS almeno uno dei criteri di cui all'art. 3, co. 10, del Decreto NIS2;
- i codici ATECO;
- le normative settoriali applicabili e citate all'interno del Decreto NIS2;
- la riconducibilità del soggetto NIS alla categoria di micro, piccola, media o grande impresa[3];
- le tipologie di soggetto a cui il soggetto NIS è riconducibile (es., fornitore di energia elettrica, *data center*, *managed service provider*, fornitore di mercati *online*, etc.).

Per i soggetti già inseriti nell'elenco NIS, tali informazioni saranno **precompilate** sulla base dei dati trasmessi fino al 14 aprile dell'anno in corso. La presenza di dati precompilati non dovrebbe tuttavia tradursi in una loro conferma automatica. L'aggiornamento annuale diventa un momento di controllo sostanziale della situazione dell'impresa, soprattutto quando nel corso dell'anno siano intervenuti cambiamenti.

Categorizzazione e verifiche di conformità

La Determinazione interviene, infine, anche sul processo di categorizzazione delle attività e dei servizi NIS, sul quale l'ACN può effettuare verifiche di conformità a campione.

Fino al **31 dicembre 2026**, l'ACN potrà fornire riscontro al soggetto NIS entro 150 giorni dalla trasmissione dell'elenco categorizzato. Successivamente, in linea con l'art. 30, co. 3, del

[3] Questo punto rappresenta una novità rispetto alla determinazione precedente dove veniva chiesto ai soggetti NIS di indicare il numero di dipendenti e i valori di fatturato e bilancio "aggregati" in caso di imprese appartenenti al medesimo perimetro di controllo (Raccomandazione 2003/361/CE). Con la nuova Determinazione, invece, viene richiesto al soggetto NIS di indicare la riconducibilità alle categorie di micro, piccole, medie o grandi imprese e, solo qualora in fase di compilazione siano automaticamente rilevante incongruenze, il soggetto NIS dovrà indicare anche i valori di fatturato, bilancio e numero di dipendenti.

Decreto NIS2, il termine sarà di 90 giorni (salvo proroga).

Secondo quanto comunicato dall'ACN, nelle prossime settimane **circa il 10% dei soggetti NIS sarà contattato** nell'ambito delle attività volte ad affinare le relative analisi di impatto riguardanti la categorizzazione.

Cosa dovrebbero fare i soggetti NIS

Nel complesso, la nuova Determinazione semplifica alcuni adempimenti, soprattutto per i soggetti la cui situazione è rimasta invariata, ma attribuisce maggiore rilievo alla qualità e all'aggiornamento delle informazioni presenti sulla Piattaforma.

Per le imprese già incluse nell'elenco NIS, diventa quindi utile verificare sin d'ora se, rispetto all'ultima dichiarazione trasmessa, siano intervenute modifiche che rendano necessaria procedere alla registrazione; controllare che eventuali operazioni societarie siano correttamente intercettate dai processi NIS2; individuare le funzioni interne responsabili dell'aggiornamento delle informazioni; e conservare evidenza delle valutazioni effettuate, soprattutto rispetto alla categorizzazione delle attività e dei servizi.

L'obiettivo dovrebbe essere quello di evitare che la gestione della Piattaforma resti confinata ai diversi adempimenti annuali. Le informazioni comunicate all'ACN dovrebbero essere mantenute allineate con l'evoluzione effettiva dell'organizzazione, così da rendere più semplice sia l'aggiornamento periodico sia la gestione di eventuali verifiche.

L'esercizio del potere sanzionatorio nel GDPR alla luce delle Linee Guida EDPB 04/2026



L'esercizio del potere sanzionatorio nel GDPR alla luce delle Linee Guida EDPB 04/2026

Il Comitato europeo per la protezione dei dati ("**European Data Protection Board**" o "**EDPB**") ha adottato, in data 17 settembre 2026, le nuove Linee Guida 04/2026 (le "**LG 04/2026**") sull'esercizio del **potere di irrogare sanzioni amministrative pecuniarie** in relazione agli altri poteri correttivi previsti dal Regolamento (UE) 2016/679 ("**GDPR**").

Le LG 04/2026 non modificano il sistema sanzionatorio delineato dal GDPR, né, tantomeno, introducono nuovi limiti o importi delle sanzioni. Il loro obiettivo è diverso: fornire alle autorità di controllo un quadro uniforme per **stabilire, a fronte di una violazione, se ricorrano i presupposti per l'irrogazione di una sanzione pecuniaria** o se sia più appropriato ricorrere a uno degli altri poteri correttivi previsti dal GDPR.

La precisazione assume particolare rilievo se si considera il rapporto con le precedenti indicazioni dell'EDPB in materia di sanzioni[4]. Le LG 04/2026 non si concentrano, infatti, sulla **quantificazione** dell'ammenda, ma sulla fase antecedente, ossia sulla **decisione circa l'opportunità stessa di applicarla**.

[4] Le Linee Guida 04/2022 dell'EDPB, adottate il 12 maggio 2022, forniscono i criteri generali di calcolo di una sanzione amministrativa pecuniaria inflitta, da parte di una Autorità di Controllo, ai sensi dell'art. 83 del Regolamento (UE) n. 679/2016.

In altri termini, le nuove indicazioni dell'EDPB mirano a rafforzare l'uniformità delle prassi adottate dalle autorità di controllo europee nella valutazione dei presupposti per l'irrogazione di una sanzione amministrativa pecuniaria, sia che venga applicata autonomamente sia in combinazione con altre misure correttive.

L'intervento si inserisce nel più ampio quadro delineato dal GDPR, che ha significativamente ampliato gli strumenti a disposizione delle autorità di controllo per assicurare il rispetto della normativa in materia di protezione dei dati personali, attribuendo alle sanzioni pecuniarie un ruolo centrale nell'attività di *enforcement*.

In tale contesto, le LG 04/2026 individuano una metodologia articolata in **cinque fasi, finalizzata a orientare il processo decisionale** delle autorità e a favorire un'applicazione maggiormente coerente e prevedibile del GDPR nei diversi Stati membri.

Le cinque fasi del procedimento

1. Base giuridica della sanzione. Il primo passaggio consiste nel **verificare se la violazione accertata sia astrattamente sanzionabile mediante un'ammenda**. L'autorità deve, pertanto, individuare la specifica base giuridica che consente l'applicazione della sanzione, rinvenibile direttamente nel GDPR oppure, nei casi in cui il Regolamento rinvia al diritto degli Stati membri, nella normativa nazionale.
2. Imputazione soggettiva. L'autorità deve **individuare il soggetto cui la violazione può essere concretamente imputata**, verificando quale soggetto fosse giuridicamente vincolato dalla disposizione violata e se la responsabilità possa quindi essere attribuita al titolare o al responsabile del trattamento, alla luce della concreta ripartizione degli obblighi e delle responsabilità nel caso esaminato.
3. Elemento soggettivo. Occorre **accertare se la violazione sia stata commessa intenzionalmente o per negligenza**, trattandosi di una condizione necessaria ai fini dell'irrogazione di un'ammenda. Infatti, la mera constatazione dell'inosservanza di una disposizione del GDPR non è, di per sé, sufficiente: è necessario esaminare anche la condotta del soggetto cui la violazione è imputata e il relativo grado di colpevolezza.
4. Circostanze del caso concreto. La quarta fase è dedicata all'esame **dei possibili fattori aggravanti e attenuanti**. Assume particolare rilievo la gravità della violazione: secondo l'approccio dell'EDPB, quando l'infrazione ha carattere minore, l'autorità può ritenere non necessaria l'ammenda e ricorrere, ad esempio, a un ammonimento ai sensi dell'art. 58(2)(b) GDPR. Al contrario, se l'infrazione non è qualificabile come minore, sussiste una forte presunzione a favore dell'applicazione di una sanzione pecuniaria, ferma restando la valutazione di tutte le circostanze rilevanti.
5. Efficacia, proporzionalità e dissuasività. Il quinto passaggio richiede di **verificare se l'irrogazione dell'ammenda sia, nel caso concreto, efficace, proporzionata e dissuasiva**, in coerenza con quanto previsto dall'art. 83(1) GDPR. L'autorità deve valutare se l'applicazione della sanzione pecuniaria costituisca lo strumento più adeguato rispetto alle caratteristiche della violazione e alle circostanze del caso, con la possibilità di discostarsi dall'approccio ordinario, qualora le peculiarità della fattispecie lo giustifichino.

La metodologia delineata dall'EDPB evidenzia, dunque, come la decisione di applicare un'ammenda **non sia il risultato automatico**

dell'accertamento di una violazione, ma il punto di arrivo di una valutazione progressiva, nella quale vengono esaminati dapprima i presupposti giuridici e soggettivi della responsabilità e, successivamente, la gravità della condotta e l'adeguatezza della sanzione rispetto al caso concreto.

La qualificazione della violazione come *"minore"*

Particolare rilievo, anche in prospettiva applicativa, assume il **quarto passaggio** della metodologia delineata dall'EDPB, nell'ambito del quale l'autorità è chiamata a esaminare le circostanze della fattispecie e, in particolare, i fattori aggravanti e attenuanti individuati dall'art. 83(2) GDPR, al fine di stabilire anche se la violazione possa essere qualificata come "minore".

La qualificazione incide sulla scelta dello strumento da adottare. Qualora la violazione presenti carattere minore, l'approccio delineato dall'EDPB è nel senso che, in linea generale, **non debba essere irrogata un'ammenda**, potendo l'autorità ricorrere, ad esempio, a un ammonimento.

Diversamente, quando l'infrazione non riveste carattere minore, le Linee Guida individuano una **forte presunzione a favore dell'irrogazione di una sanzione amministrativa pecuniaria**.

L'impostazione sopra delineata non equivale, tuttavia, a introdurre una soglia automatica basata sull'assenza di un danno o di conseguenze economiche per gli interessati: la qualificazione della violazione richiede, infatti, una **valutazione complessiva delle circostanze del caso concreto**, alla luce dei diversi elementi rilevanti ai sensi dell'art. 83 GDPR.

In questa prospettiva, assume rilievo anche la distinzione tra una **condotta occasionale e una carenza di natura strutturale**: la reiterazione di una medesima violazione nel tempo può, infatti, incidere sulla valutazione dell'infrazione e rendere meno plausibile la riconduzione della condotta a un episodio isolato e circoscritto.
Per le organizzazioni, ciò evidenzia l'importanza non soltanto dell'adozione formale di procedure e misure di conformità, ma anche della capacità di **dimostrarne l'effettiva applicazione e il costante monitoraggio**, nonché di intervenire tempestivamente per correggere eventuali anomalie riscontrate.

Il quadro nazionale: la Cassazione delimita i termini per l'esercizio dei poteri del Garante per la protezione dei dati personali

A completare il quadro intervengono tre recenti pronunce della Corte di Cassazione (nn. 22791, 24861 e 24862 del 2026), che precisano i limiti temporali entro cui il Garante per la protezione dei dati personali (il "**Garante**") può esercitare i propri poteri correttivi e sanzionatori. Le decisioni non introducono nuove regole, ma **chiariscono la portata della disciplina vigente**, individuando con maggiore precisione il momento di decorrenza dei relativi termini.

Con riferimento ai **reclami**, la Corte ha ribadito l'autonomia del procedimento di reclamo rispetto all'eventuale successivo procedimento correttivo e sanzionatorio. Pertanto, il superamento del termine previsto per decidere sulla fondatezza del reclamo – nove mesi, prorogabili fino a dodici – **non determina la decadenza dal potere sanzionatorio del Garante**.

Quanto al **termine di 120 giorni**, la Cassazione ha precisato che esso riguarda **la notifica della contestazione e non l'adozione del provvedimento sanzionatorio finale**. Il termine decorre dal momento in cui la violazione può ritenersi **definitivamente accertata**, e non dalla prima acquisizione di una sua possibile notizia.

Prima di tale momento, il Garante può svolgere le necessarie attività istruttorie, senza essere soggetto a un termine decadenziale predeterminato, purché proceda secondo criteri di ragionevolezza e senza ritardi ingiustificati.

Una volta notificata tempestivamente la contestazione, **non è previsto un ulteriore termine decadenziale** per l'adozione della sanzione, fermo restando il termine di prescrizione quinquennale dell'illecito.

Continuità con le Linee Guida 04/2022

Come già anticipato, sotto il profilo sistematico, le LG 04/2026 si pongono in continuità con la metodologia già elaborata dall'EDPB. Le Linee Guida 04/2022 sono infatti dedicate alla fase successiva, ossia alla *quantificazione* dell'ammenda una volta stabilito che debba essere applicata, mentre le nuove Linee Guida si concentrano sul **momento decisionale che la precede**, fornendo criteri per stabilire se la sanzione pecuniaria costituisca la misura appropriata e come vada valutata rispetto agli ulteriori strumenti correttivi previsti dal GDPR.

Cosa possono fare concretamente le imprese?

Le indicazioni dell'EDPB presentano rilevanti ricadute anche sul piano organizzativo. La *compliance* in materia di protezione dei dati va considerata come un **processo concreto e dimostrabile**, non limitato alla predisposizione di documenti e procedure.

In caso di controllo, assumono particolare rilievo:

- la possibilità di ricostruire le valutazioni effettuate e le misure adottate (*accountability* documentale);
- l'evidenza del recepimento delle indicazioni formulate dal DPO;
- la previsione di meccanismi idonei a individuare e correggere tempestivamente eventuali non conformità;
- la tracciabilità delle violazioni già verificatesi, soprattutto quando la loro reiterazione possa evidenziare una criticità organizzativa non occasionale.

In questa prospettiva, le LG 04/2026 non si limitano ad orientare l'operato delle autorità: offrono, infatti, anche alle imprese una **griglia di autovalutazione** utile a comprendere, ex ante, quali profili saranno concretamente apprezzati in sede di controllo.

* * *

IA, governance, formazione e lavoro: le principali novità del D.Lgs. 179/2026



Il prossimo 23 ottobre entrerà in vigore il D.Lgs. 179/2026 (il "**Decreto**"), secondo decreto attuativo della Legge italiana sull'intelligenza artificiale (L. 132/2025).

Il Decreto si inserisce nel quadro normativo nazionale in materia di IA insieme al D.Lgs. 160/2026, dedicato all'utilizzo dell'IA da parte delle forze di polizia e contenente disposizioni in tema di responsabilità penale e civile (per maggiori approfondimenti, si rinvia al nostro precedente contributo "*IA e responsabilità d'impresa: cosa cambia con il D.Lgs. 160/2026*").

A una prima lettura, il Decreto potrebbe apparire principalmente incentrato sulla definizione delle competenze delle Autorità nazionali e sulla promozione della formazione in materia di IA nei settori dell'istruzione, delle professioni, della PA e della giustizia. In realtà, il Decreto contiene diverse disposizioni di immediato interesse anche per le imprese.

Oltre a completare il quadro nazionale di coordinamento con l'AI Act, il Decreto introduce specifiche disposizioni sull'utilizzo dell'IA nei rapporti di lavoro, collega l'impiego dei sistemi di IA agli obblighi in materia di salute e sicurezza sul lavoro e istituisce lo Spazio di sperimentazione italiano per l'IA (c.d. *sandbox* AI), all'interno del quale i sistemi di IA possono essere testati in un ambiente controllato secondo condizioni e criteri predeterminati e sotto la vigilanza di AgID e ACN. Ma quali sono, in concreto, i principali profili di interesse del Decreto per le imprese?

Governance

Il Decreto definisce il sistema nazionale di governance dell'IA. In tale contesto, l'Agenzia per l'Italia digitale ("**AgID**") viene designata quale autorità di notifica. Essa è pertanto responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione, la notifica e il monitoraggio degli organismi di valutazione della conformità – ossia quegli enti indipendenti accreditati, previsti dall'AI Act, per verificare che i sistemi di IA ad alto rischio rispettivo i requisiti di sicurezza e trasparenza previsti dalla legge.

All'Agenzia per la cybersicurezza nazionale ("**ACN**") viene invece attribuito il ruolo di autorità nazionale di vigilanza del mercato sui sistemi di IA e di punto di contatto unico nazionale.

Accanto ad AgID e ACN, il Decreto attribuisce specifiche competenze a **Banca d'Italia**, **CONSOB** e **IVASS** con riferimento ai sistemi di IA ad alto rischio impiegati nei rispettivi settori vigilati, nonché al **Garante Privacy** per i profili di propria competenza.

La scelta del legislatore riflette un modello di vigilanza fondato sulla specializzazione settoriale delle Autorità coinvolte. Proprio per questo motivo, il Decreto prevede accordi, protocolli d'intesa e altre forme di cooperazione finalizzate ad assicurare il coordinamento tra le diverse Autorità competenti.

Il Decreto rafforza inoltre i poteri ispettivi delle autorità: AgID può svolgere attività di *audit* e verifica, sia periodiche sia straordinarie, nonché avviare procedimenti relativi alla limitazione, sospensione o revoca della designazione degli organismi notificati. ACN potrà invece effettuare controlli anche sulle prove svolte in condizioni reali e condurre ispezioni senza preavviso.

Sono infine previste sanzioni amministrative in linea con quanto stabilito dall'art. 99 dell'AI Act, fino a 35 milioni di euro o al 7% del fatturato mondiale annuo (per la violazione del divieto delle pratiche di IA vietate), oltre a misure correttive non pecuniarie per le violazioni caratterizzate da scarsa offensività o pericolosità.

Lavoro, HR, salute e sicurezza

Una delle disposizioni di maggiore impatto pratico riguarda l'utilizzo dell'IA nei rapporti di lavoro. Il Decreto conferma infatti un principio destinato a incidere direttamente sui processi HR: l'IA può supportare le decisioni, ma non può sostituire la responsabilità umana nelle scelte che producono effetti sui lavoratori.

In particolare, il Decreto prevede che le decisioni finali relative a costituzione, modificazione o risoluzione del rapporto di lavoro, comprese le valutazioni delle prestazioni e l'adozione di provvedimenti disciplinari, non possano essere

assunte unicamente sulla base di trattamenti automatizzati.

La decisione finale deve essere rimessa a una persona fisica e il consenso del lavoratore non può costituire un'eccezione a tale divieto. Sono invece escluse da tale previsione le attività di ricerca e selezione delle candidature, anche quando comportino la mancata ammissione alle successive fasi del processo di selezione.

Il datore di lavoro è inoltre tenuto a informare i lavoratori dell'utilizzo di tali sistemi di IA. Le decisioni adottate in violazione di tali disposizioni, così come gli eventuali licenziamenti conseguenti, sono espressamente qualificati dal Decreto come nulli.

Il Decreto interviene anche sul versante della salute e sicurezza sul lavoro, collegando l'impiego dell'IA agli obblighi previsti dal Testo Unico in materia di salute e sicurezza (D.Lgs. 81/2008).

I sistemi di IA che possono incidere sull'organizzazione del lavoro, sui ritmi produttivi, sulle modalità di esecuzione della prestazione o su processi decisionali rilevanti ai fini della sicurezza devono infatti essere presi in considerazione nell'ambito della valutazione dei rischi aziendali. I datori di lavoro sono inoltre tenuti a garantire adeguate attività di informazione e formazione dei lavoratori.

Le disposizioni assumono particolare rilevanza per le organizzazioni che stanno introducendo strumenti di IA nei processi di selezione, valutazione delle *performance*, organizzazione del lavoro o gestione del personale. Non si tratta infatti soltanto di verificare la conformità all'AI Act, ma anche di valutare l'impatto di tali sistemi sugli obblighi lavoristici e prevenzionistici già previsti dall'ordinamento italiano.

Tutela delle informazioni aziendali

Anche i dati, gli algoritmi e i metodi matematici utilizzati per l'addestramento dei sistemi di IA possono assumere particolare rilevanza sotto il profilo della tutela delle informazioni aziendali.

Il Decreto conferma infatti che, al ricorrere dei relativi presupposti, dati, algoritmi e metodi matematici utilizzati per l'addestramento possono beneficiare delle tutele previste per le informazioni aziendali riservate e per il *know-how*.

La previsione assume rilievo in un contesto in cui il valore competitivo è sempre più legato a dati, metodologie e conoscenze tecniche utilizzate nello sviluppo delle soluzioni di IA. Per le imprese, ciò evidenzia l'importanza di individuare correttamente gli *asset* informativi strategici e di adottare misure idonee a garantirne la riservatezza e la protezione.

Conclusioni e spunti operativi

Il Decreto contiene diversi elementi che le imprese dovrebbero iniziare a considerare già oggi. Da un lato, la designazione delle Autorità competenti e il rafforzamento dei relativi poteri ispettivi contribuiscono a rendere più concreto il quadro di *enforcement* dell'AI Act in Italia.

Dall'altro, le nuove regole sull'utilizzo dell'IA nei rapporti di lavoro e il collegamento con gli obblighi in materia di salute e sicurezza confermano come l'adozione di sistemi di IA non possa essere considerata una questione esclusivamente tecnologica.

Per molte imprese, il Decreto rappresenta quindi un ulteriore segnale della necessità di affrontare la *governance* dell'IA in modo trasversale, coinvolgendo non soltanto le funzioni IT, ma anche HR, *compliance*, *privacy*, *cybersecurity* e sicurezza sul lavoro.

In termini pratici, vista anche la prossima entrata in vigore del Decreto, potrebbe essere opportuno verificare:

- quali sistemi di IA siano già utilizzati nei processi aziendali;
- se tali sistemi incidano su processi HR o sull'organizzazione del lavoro;
- se il relativo impiego debba essere considerato nell'ambito della valutazione dei rischi aziendali;
- se vi sono *policy* o procedure interne che disciplinino l'utilizzo dell'IA e la supervisione umana delle decisioni supportate da tali sistemi e, in caso contrario, adottarle;
- se l'organizzazione disponga di adeguati presidi di *governance* in vista della piena applicazione dell'AI Act.

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