UNISTUDIO & GAMBINO
LEGAL AND TAX ADVISORS

Ottobre 2025

NOVITA' IN MATERIA DI PRIVACY, CYBERSICUREZZA E INTELLIGENZA ARTIFICIALE

Verifiche ed azioni da intraprendere nel biennio 2025-2026

Informativa n.	23/2025
Riferimenti normativI	Regolamento (UE) 679/2016 (c.d. "GDPR")
	Regolamento (UE) n. 2554/2022 (c.d. "DORA")
	Regolamento (UE) 1689/2024 (c.d. "AI Act")
	D. Lgs. n. 138/2024 (c.d. "Decreto NIS2")
	Informativa Unistudio n.16/2025

VIA DURINI 26
20121 MILANO
T. +39.02.83418800

VIA DEI TRE OROLOGI 14
00197 ROMA
T. +39.06.8088855

VIA DOMINUTTI 20
37135 VERONA
T. +39.045.8013399

info@unistudioegambino.it
www.unistudioegambino.it
C.F. e P.IVA 02901730230

UNISTUDIO & GAMBINO
LEGAL AND TAX ADVISORS

Alla luce del piano dell'attività ispettiva che il Garante per la protezione dei dati personali (c.d. "Garante Privacy") ha predisposto per il 2025 e dall'analisi dei più recenti provvedimenti sanzionatori, sono molteplici, tra gli adempimenti in ambito privacy che incombono su titolari e responsabili del trattamento, quelli a cui prestare particolare attenzione soprattutto nel biennio 2025-2026.

Per aiutare i propri clienti nell'attività di esecuzione e/o aggiornamento di un "self-assesment" sullo stato di attuazione del GDPR all'interno delle proprie organizzazioni, lo Studio ha predisposto, in calce alla presente nota, un breve elenco dei principali adempimenti che tiene anche conto della prassi del Garante Privacy di indagare, nell'ambito delle proprie attività ispettive, anche profili di non esclusiva competenza, come l'implementazione delle misure di sicurezza tecniche e organizzative definite dall'Agenzia per la Cybersicurezza Nazionale (c.d. "ACN") nell'ambito del Decreto NIS2.

Lo Studio offre, infatti, alle realtà private che, per dimensione o per attività, rientrano nell'ambito di applicazione del richiamato Decreto NIS2, supporto nell'adeguamento ai correlati obblighi in materia di adozione di specifiche misure di sicurezza informatica sviluppate nel contesto del Framework Nazionale per la Cybersecurity e la Data Protection; adeguamento che deve essere ultimato entro ottobre 2026.

Lo Studio è in grado, inoltre, di accompagnare, quanti intendono sviluppare o avvalersi di sistemi di intelligenza artificiale, nell'adeguamento all'AI Act, normativa europea che definisce specifici obblighi, anche di informazione e di verifica della tutela dei diritti inviolabili nell'utilizzo di tali sistemi.

È stata prevista un'applicazione del regolamento in diverse fasi:

a. il 2 febbraio 2025 sono entrati in vigore i divieti per le AI a rischio inaccettabile;
b. dal 2 agosto 2025 hanno trovato applicazione diretta le norme dell'AI Act sulla governance e gli obblighi per i modelli di IA per finalità generali (c.d. "GPAI");
c. a far data dal 2 agosto 2026 l'atto avrà piena applicazione per i sistemi considerati ad alto rischio;
d. dal 2 agosto 2027 si applicheranno le regole per i sistemi AI che integrano l'intelligenza artificiale in prodotti regolamentati da specifiche leggi dell'UE (es. quelli utilizzati nel comparto salute).

Vi sono evidenti profili di connessione tra i sistemi di intelligenza artificiale e la disciplina sul trattamento dei dati personali, anche in termini di sicurezza dei dati impiegati per addestrare gli strumenti di IA e per le elaborazioni degli stessi, e la necessità di essere costantemente aggiornati al quadro regolamentare che va via via definendosi, di pari passo con l'adozione dei provvedimenti attuativi dell'AI Act da parte della Commissione Europea e dell'Agenzia per l'Italia Digitale (c.d. "AgID") e dell'ACN, autorità preposte alla vigilanza sul rispetto dell'AI Act in Italia.

Il rispetto degli obblighi di cui alle richiamate normative non è da intendersi esclusivamente quale prescrizione legislativa al cui mancato adempimento possono seguire, per l'impresa, sanzioni di maggiore o minore entità, ma anche quale fattore cruciale per la crescita del livello di fiducia riconosciuto all'impresa stessa da parte di utenti e clienti; nonché quale presidio per la reputazione delle organizzazioni e, in tale ottica, deve essere affrontato con approccio olistico e coordinato, mirato alla gestione dei rischi e alla sicurezza della catena di approvvigionamento.

***

Lo Studio mette a disposizione dei propri clienti il seguente elenco dei principali adempimenti, quale strumento di "self assessment" per verificare se l'organizzazione ha svolto o deve ancora svolgere alcuni degli adempimenti indicati.
Lo Studio rimane a disposizione per qualsiasi richiesta di chiarimento da inviare all'indirizzo mail privacy@unistudioegambino.it.

UNISTUDIO & GAMBINO
LEGAL AND TAX ADVISORS

GDPR

Adempimenti generali

- ☐ I dati personali sono trattati solo da personale autorizzato e istruito al trattamento?
- ☐ È stato definito e attuato un percorso di formazione dedicato ai dipendenti e collaboratori?
- ☐ Sono state definite *policy* aziendali per il corretto trattamento dei dati personali?
- ☐ Sono stati definiti piani di verifica dei dati trattati, in relazione all'obbligo di trattare i dati solo in forza di presupposto di legge (es. esecuzione di contratto, adempimento di obbligo di legge, legittimo interesse) o di espresso consenso e, in ogni caso, previo rilascio di idonea informativa sul trattamento (estesa ex art. 13 o 14 GDPR ed aggiornata periodicamente)?
- ☐ Sono state adottate misure di sicurezza, tecniche e organizzative, idonee al trattamento svolto (avendo riguardo anche alle misure di sicurezza indicate dall'Agenzia per la Cybersicurezza Nazionale (c.d. "ACN"), che costituiscono un valido strumento per valutare l'adeguatezza delle misure adottate)?
- ☐ È stato predisposto un registro delle attività di trattamento in qualità di titolare e di responsabile del trattamento?
- ☐ È stato definito un piano di verifiche periodiche di impatto del trattamento dei dati (c.d. "DPIA").

Adempimenti alla luce del piano di ispezioni del Garante per il 2025

- ☐ L'organizzazione è in grado di rispondere proattivamente alle istanze degli interessati?
- ☐ L'organizzazione è in grado di gestire le interlocuzioni con il Garante Privacy nell'ambito di istruttorie relative a reclami e segnalazioni formali?
- ☐ L'organizzazione ha nominato il *data protection officer* (c.d. DPO)
    - in caso di risposta positiva, ha verificato il possesso, da parte del soggetto nominato, dei requisiti di legge (es. sanzione del Garante pari a 700.000 euro a società che aveva nominato DPO il proprio rappresentante legale)?
    - in caso di risposta negativa, si ricorda al riguardo che ogni valutazione anche precedentemente svolta che abbia condotto a ritenere non sussistente l'obbligo di nomina deve essere ripetuta con cadenza almeno annuale, tenendo conto anche dei trattamenti svolti per conto di terzi in qualità di responsabili del trattamento?
- ☐ Se l'organizzazione utilizza banche dati pubbliche o private, sono stati verificati i sistemi di sicurezza e i profili di accessibilità delle banche dati stesse, nonché la capacità di rilevare tempestivamente e/o prevenire le violazioni di dati personali (c.d. *data breach*) mediante *assesment* o *audit* mirati?
- ☐ Se l'organizzazione offre o si avvale di servizi di *call center* e servizi di *marketing*, è stata verificata l'adeguatezza dei trattamenti svolti anche con riferimento all'eventuale attivazione di contratti non richiesti?
- ☐ È stato definito un piano di *audit* sui responsabili del trattamento?
- ☐ Si è proceduto alla verifica dei sistemi di acquisizione dei consensi per l'impiego di *cookies* di profilazione?
- ☐ Le DPIA sono svolte prima che inizino i trattamenti e ripetute periodicamente?
- ☐ È stato definito un piano per l'aggiornamento periodico del registro delle attività di trattamento?

Decreto NIS2

- ☐ Si è verificato se l'organizzazione rientra nel perimetro di applicazione del Decreto NIS2 (cfr. checklist di cui all'informativa Unistudio n. 16/2025 - Imprese (con più di 50 dipendenti) che operano nel settore energetico, dei trasporti (aereo, ferroviario, marino e di terra), quelle che offrono infrastrutture digitali (*cloud*, nomi di dominio, *data center* e *content delivery network*) e servizi digitali (*marketplace*, motori di ricerca e *social network*), i prestatori di servizi fiduciari qualificati e non qualificati, i fornitori di reti pubbliche di comunicazione elettronica, di servizi bancari e finanziari, nonché le imprese che operano nel settore sanitario e nella fabbricazione di dispositivi medici e medico-diagnostici; rientrano nell'ambito di applicazione altresì i fornitori di servizi postali e di corriere, i produttori e i distributori di sostanze

chimiche, le imprese alimentari, i produttori di computer e prodotti di elettronica e ottica, di autoveicoli (compresi rimorchi e semirimorchi), nonché gli enti e gli istituti di ricerca)?

- ☐ In caso di risposta positiva si è provveduto alla registrazione al portale dell'ACN entro il 28 febbraio 2025?
- ☐ È stata programmata l'implementazione di un sistema di notifica degli incidenti ad ACN, da realizzarsi entro gennaio 2026?
- ☐ È stato definito un programma di implementazione delle misure di sicurezza di cui al Framework Nazionale per la Cybersecurity e la Data Protection da realizzarsi entro ottobre 2026?
- ☐ Si è verificato se l'organizzazione è soggetta anche agli obblighi di cui al DORA, che è diventato obbligatorio da gennaio 2025?

AI Act

- ☐ L'organizzazione ha definito, in linea con le indicazioni dell'AgID e dell'ACN, autorità preposte alla vigilanza del rispetto dell'AI Act, una strategia aziendale per l'uso dell'intelligenza artificiale?
- ☐ L'organizzazione ha definito una *policy* per i dipendenti al fine di evitare che vengano usati sistemi di AI destinati all'uso personale in ambito lavorativo?
- ☐ L'organizzazione ha definito una *policy* volta ad assicurare il corretto sviluppo e l'adeguata acquisizione di sistemi di AI?
- ☐ Se sistemi di AI sono già in uso, l'organizzazione ha mappato e verificato il livello di rischio?
- ☐ Se sistemi di AI sono già in uso, l'organizzazione ha provveduto ad informare i dipendenti e i destinatari dei relativi servizi secondo quanto previsto dall'AI Act.