

Aggiornamento Data protection, AI, IT e IP

n. 6 / 2024

DATA PROTECTION

17 Luglio 2024 – Comitato europeo per la protezione dei dati personali - EDPB: nuove FAQ di chiarimento sul trasferimento dei dati personali verso gli USA ai sensi del *Data Privacy Framework*.

17 Luglio 2024 – Il Comitato europeo per la protezione dei dati personali – EDPB ha approvato il sigillo europeo per la certificazione della *compliance* dei trattamenti al GDPR.

INTELLIGENZA ARTIFICIALE.

12 Luglio 2024 – Pubblicato in Gazzetta Ufficiale UE il Regolamento 2024/1689 sull'Intelligenza Artificiale (AI Act).

17 Luglio 2024 – Il Comitato Europeo per la protezione dei dati personali – EDPB ha adottato una dichiarazione sul ruolo delle Autorità europee per la protezione dei dati personali nell'ambito del nuovo quadro normativo sull'Intelligenza Artificiale.

MERCATI DIGITALI.

17 Luglio 2024 – Tribunale UE: respinto il ricorso della Bytedance (TikTok) avverso la decisione della Commissione UE che la designa come *gatekeeper* ai sensi del DMA.

12 Luglio 2024 – La Commissione UE trasmette i risultati preliminari a X (ex Twitter) per violazione del Digital Services Act (Regolamento UE 2022/2065).

INFORMATION TECHNOLOGY

12 Luglio 2024 - Corte di Cassazione: in caso di bonifico errato la banca è responsabile se non verifica la corrispondenza tra IBAN e beneficiario e non può appellarsi alla privacy per rifiutare di fornire i dati personali del percettore per errore.

9 Luglio 2024 – Corte di Cassazione: è valida l'impugnazione del licenziamento trasmessa mediante l'invio di una PEC con allegato un file word.

8 Luglio 2024 – Consiglio di Stato: illegittima l'esclusione di un concorrente da una gara per aver inviato l'offerta tecnica attraverso il servizio We Transfer.



DATA PROTECTION

17 Luglio 2024 – Comitato europeo per la protezione dei dati personali- EDPB: nuove FAQ di chiarimento sul trasferimento dei dati personali verso gli USA ai sensi del *Data Privacy Framework*.

L'EDPB ha adottato due documenti di domande frequenti (FAQ) riguardanti il quadro normativo UE-USA in materia di privacy dei dati (DPF), volti a fornire maggiori chiarimenti sul funzionamento del DPF.

Le [FAQ per le persone fisiche](#) forniscono informazioni sul funzionamento del DPF: come beneficiarne, come presentare un reclamo e come verrà gestito questo reclamo.

Allo stesso modo, le [FAQ per le aziende](#) spiegano quali aziende statunitensi sono idonee ad aderire al DPF: cosa fare prima di trasferire i dati personali a un'azienda negli Stati Uniti certificata DPF e dove trovare ulteriori indicazioni.

17 Luglio 2024 – Il Comitato europeo per la protezione dei dati personali – EDPB ha approvato il sigillo europeo per la certificazione della *compliance* dei trattamenti al GDPR.

L'EDPB ha adottato un parere che approva il catalogo dei criteri EuroPriSe per la certificazione delle attività di trattamento da parte dei Titolari del trattamento, introducendo un sigillo europeo per la protezione dei dati. I sigilli europei per la protezione dei dati fungono da strumenti importanti che contribuiscono alla conformità al GDPR.

Nel settembre 2022 l'EDPB aveva adottato un [parere sui criteri di certificazione EuroPriSe](#), consentendone il riconoscimento in Germania come criteri di certificazione per le operazioni di trattamento da parte dei titolari. A seguito di un aggiornamento del sistema, il nuovo parere ha approvato i criteri come applicabili in tutta l'UE/SEE e come sigillo europeo di protezione dei dati.

La certificazione GDPR contribuisce a documentare la conformità e ad aumentare la trasparenza e la fiducia. Consente di valutare meglio il grado di protezione offerto da prodotti, servizi, processi o sistemi utilizzati dalle organizzazioni che trattano dati personali.

Il sigillo europeo per la protezione dei dati EuroPriSe sarà aggiunto al [registro dei meccanismi di certificazione e dei sigilli di protezione dei dati](#) in conformità con l'articolo 42, paragrafo 8, del GDPR dopo i necessari controlli giuridici, linguistici e di formattazione e sarà reso disponibile sul sito web del Comitato europeo per la protezione dei dati.

INTELLIGENZA ARTIFICIALE.

12 Luglio 2024 – Pubblicato in Gazzetta Ufficiale UE il Regolamento 2024/1689 sull'Intelligenza Artificiale (AI Act).

Il [Regolamento \(UE\) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti \(CE\) n. 300/2008, \(UE\) n. 167/2013, \(UE\) n. 168/2013, \(UE\) 2018/858, \(UE\) 2018/1139 e \(UE\) 2019/2144 e le direttive 2014/90/UE, \(UE\) 2016/797 e \(UE\) 2020/1828 \(regolamento sull'intelligenza artificiale\)](#) è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea del 12 Luglio 2024.

Rappresenta la prima legge organica e completa al mondo per la disciplina dell'Intelligenza Artificiale e mira ad affrontare i rischi per la salute, la sicurezza e i diritti fondamentali. Inoltre, il Regolamento 2024/1689 tutela la democrazia, lo Stato di diritto e l'ambiente.

Il Regolamento 2024/1689 **entra in vigore il 1° agosto 2024** ma sarà applicabile solo dal **2 agosto 2026**. Alcune norme **si applicheranno tuttavia dopo 6 o 12 mesi**.

Saranno applicabili **dal 2 febbraio 2025**:

- (a) gli articoli da 1 a 4, relativi a oggetto, ambito di applicazione, definizioni (i contratti di fornitura potranno dunque impiegare definizioni tecniche e giuridiche dell'AI Act) e obblighi di alfabetizzazione IA (obbligo per i fornitori e gli sviluppatori di avere personale addestrato e competente, che potrà trovare specifico ingresso nella contrattualistica con i fornitori).
- (b) l'art. 5 sulle pratiche di IA vietate (particolare attenzione dovrà essere prestata – ad esempio - alle profilazioni avanzate che utilizzano la biometria, soprattutto sui luoghi di lavoro, per verificare l'applicabilità del divieto).

Dopo 12 mesi (**dal 2 agosto 2025**) si applicheranno:

- (a) le norme sull'impianto sanzionatorio (con sanzioni fino a 35 milioni di euro o al 7% del fatturato globale annuo; la sanzione per i fornitori di modelli IA a scopi generali – fino a 15 milioni di euro o fino al 3% del fatturato – si applicherà dopo 24 mesi);
- (b) le norme sui modelli di IA per finalità generali – GPAI (tematica di compliance e contrattuale, alla luce di svariati modelli – come Chat-GPT e l'IA generativa – già oggi integrati in soluzioni di ampio utilizzo quotidiano);
- (c) le norme sulle Autorità di notifica, sulle relative procedure di notifica e sugli organismi notificati;
- (d) l'art. 78 (“Riservatezza dei dati trattati in conformità al Regolamento”);
- (e) le norme che istituiscono la banca dati UE sui sistemi di IA ad alto rischio.

Infine, è rinviata **al 2 agosto 2027** l'applicabilità delle norme sui sistemi di IA “ad alto rischio”, così come dei connessi obblighi.

Il Regolamento 2024/1689 si applicherà ai soggetti pubblici e privati, all'interno e all'esterno dell'UE, a condizione che il sistema di IA sia immesso sul mercato dell'Unione o che il suo utilizzo abbia effetti su persone situate nell'UE.

Le norme vincoleranno sia i fornitori/sviluppatori di sistemi IA (ad esempio uno sviluppatore di uno strumento di screening dei CV) quanto gli utilizzatori professionali finali (detti “deployer”) di sistemi di IA ad alto rischio (ad esempio, un'azienda che acquista il suddetto strumento di screening).

Il Regolamento 2024/1689 si applicherà inoltre a tutta la filiera commerciale (importatori, distributori, fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il loro nome o marchio, etc): gli importatori di sistemi di IA nella UE dovranno ad esempio garantire che il fornitore extra-UE abbia già eseguito l'appropriata procedura di valutazione della conformità e che il sistema IA rechi una marcatura di conformità europea (CE) e sia corredato della documentazione e delle istruzioni per l'uso richieste.

Sono inoltre previsti specifici obblighi per i fornitori di modelli di IA per finalità generali (detti GPAI) compresi i modelli di IA generativa di grandi dimensioni (i sistemi LLM – Large Language Models, come Chat-GPT, Copilot, Gemini, etc).

I fornitori di modelli gratuiti e open source sono esentati dalla maggior parte di questi obblighi. Tale esenzione non riguarda tuttavia gli obblighi applicabili ai fornitori di modelli di IA per finalità generali GPAI che comportano rischi sistemici.

Il Regolamento 2024/1689 non si applicherà alle attività di ricerca, sviluppo e prototipazione che precedono l'immissione sul mercato e ai sistemi di IA sviluppati per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività.



17 Luglio 2024 – Il Comitato Europeo per la protezione dei dati personali – EDPB ha adottato una dichiarazione sul ruolo delle Autorità europee per la protezione dei dati personali nell’ambito del nuovo quadro normativo sull’Intelligenza Artificiale.

Il Comitato europeo per la protezione dei dati (EDPB) ha adottato una [dichiarazione sul ruolo delle autorità di protezione dei dati \(DPA\) nel quadro della legge sull'intelligenza artificiale \(AI Act\)](#).

Secondo l'EDPB, le autorità di protezione dei dati hanno già esperienza e competenza nell'affrontare l'impatto dell'IA sui diritti fondamentali, in particolare il diritto alla protezione dei dati personali, e dovrebbero pertanto essere designate come autorità di vigilanza del mercato in una serie di casi.

Ciò garantirebbe un migliore coordinamento tra le diverse autorità di regolamentazione, rafforzerebbe la certezza del diritto per tutte le parti interessate e rafforzerebbe la vigilanza e l'applicazione sia della legge sull'IA che della normativa dell'UE in materia di protezione dei dati.

Ai sensi della legge sull'IA, gli Stati membri nominano le autorità di vigilanza del mercato a livello nazionale entro il 2 agosto 2025 al fine di vigilare sull'applicazione e l'attuazione della legge sull'IA.

Nella sua dichiarazione, l'EDPB raccomanda che:

- Come già indicato nella legge sull'IA, le autorità di protezione dei dati dovrebbero essere designate come autorità di vigilanza del mercato per i sistemi di IA ad alto rischio utilizzati per l'attività di contrasto, la gestione delle frontiere, l'amministrazione della giustizia e i processi democratici;
- Gli Stati membri dovrebbero prendere in considerazione la possibilità di nominare le autorità di protezione dei dati come autorità di vigilanza del mercato anche per altri sistemi di IA ad alto rischio, tenendo conto dei pareri dell'autorità nazionale di protezione dei dati, in particolare quando tali sistemi di IA ad alto rischio si trovano in settori che possono incidere sui diritti e sulle libertà delle persone fisiche con riguardo al trattamento dei dati personali;
- Le autorità di protezione dei dati, se designate come autorità di vigilanza del mercato, dovrebbero essere designate come punti di contatto unici per il pubblico e le controparti a livello degli Stati membri e dell'UE;
- È opportuno stabilire procedure chiare per la cooperazione tra le autorità di vigilanza del mercato e le altre autorità di regolamentazione incaricate della supervisione dei sistemi di IA, comprese le autorità di protezione dei dati. Inoltre, dovrebbe essere istituita un'adeguata cooperazione tra l'Ufficio dell'UE per l'IA e le autorità di protezione dei dati/il Comitato europeo per la protezione dei dati.

MERCATI DIGITALI.

17 Luglio 2024 – Tribunale UE: respinto il ricorso della Bytedance (TikTok) avverso la decisione della Commissione UE che la designa come gatekeeper ai sensi del DMA.

La Bytedance Ltd è una società che, tramite le sue società figlie, fornisce la piattaforma di social network online TikTok. Con decisione del 5 settembre 2023, la Commissione ha designato la Bytedance come gatekeeper ai sensi del Regolamento 2022/1925 sui mercati digitali (il cosiddetto *Digital Markets Act* – DMA o Legge sui Mercati Digitali). Nel novembre 2023 la Bytedance ha proposto ricorso al Tribunale UE richiedendo l'annullamento di tale decisione.

Con la sentenza nella causa T-1077/23 (Bytedance / Commissione UE), pronunciata otto mesi dopo la proposizione del ricorso, il Tribunale ha respinto il ricorso della Bytedance.

Il Tribunale ha anzitutto ricordato la genesi e il contenuto normativo del DMA. In particolare, esso ha sottolineato che il legislatore dell'Unione ha deciso di adottare il DMA al fine, segnatamente, di contribuire al corretto funzionamento del mercato interno stabilendo norme volte a garantire la contendibilità e l'equità per i mercati nel settore digitale in generale e per gli utenti commerciali e gli utenti finali dei servizi di piattaforma di base forniti dai gatekeeper in particolare.

Il Tribunale ha poi constatato che la Commissione poteva giustamente ritenere che la Bytedance fosse un gatekeeper. A tale riguardo, esso ha rilevato che è pacifico che la Bytedance raggiunga le soglie quantitative previste nel DMA, per quanto riguarda in particolare il suo valore di mercato globale, il numero di utenti di TikTok nell'Unione e il numero di anni in cui quest'ultima soglia relativa al numero di utenti è stata raggiunta, il che consente di presumere che essa sia un gatekeeper.

Il Tribunale ha poi ritenuto che gli argomenti dedotti dalla Bytedance non fossero sufficientemente fondati per mettere manifestamente in discussione la presunzione secondo cui la Bytedance ha un impatto significativo sul mercato interno, TikTok è un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali e la Bytedance detiene una posizione consolidata e duratura.

12 Luglio 2024 – La Commissione UE trasmette i risultati preliminari a X (ex Twitter) per violazione del Digital Services Act (Regolamento UE 2022/2065).

La Commissione UE ha notificato a X (ex Twitter) il parere preliminare secondo cui il *social media* viola la [legge sui servizi digitali](#) (DSA) in settori legati ai dark pattern, alla trasparenza della pubblicità e all'accesso ai dati per i ricercatori.

La trasparenza e la responsabilità in relazione alla moderazione dei contenuti e alla pubblicità sono al centro del DSA. Sulla base di un'indagine approfondita che comprendeva, tra l'altro, l'analisi dei documenti interni della società, colloqui con esperti e la cooperazione con i [coordinatori nazionali dei servizi digitali](#), la Commissione ha formulato constatazioni preliminari di non conformità su tre rimostranze:

- In primo luogo, X progetta e gestisce la propria interfaccia per gli "account verificati" con il "marchio di controllo blu" in modo da non corrispondere alla prassi del settore e **ingannare gli utenti. Poiché chiunque può abbonarsi per ottenere tale status "verificato"**, ciò incide negativamente sulla capacità degli utenti di prendere decisioni libere e informate in merito all'autenticità degli account e ai contenuti con cui interagiscono. Vi sono prove di "account verificati" per ingannare gli utenti.
- In secondo luogo, X non rispetta la **necessaria trasparenza in materia di pubblicità**, in quanto non fornisce un archivio pubblicitario consultabile e affidabile, ma pone invece in essere caratteristiche di progettazione e barriere di accesso che rendono l'archivio inadatto a fini di trasparenza nei confronti degli utenti. In particolare, il modello pubblicitario adottato non consente la vigilanza e la ricerca necessarie sui rischi emergenti derivanti dalla distribuzione di pubblicità online.
- In terzo luogo, X non **fornisce ai ricercatori l'accesso ai suoi dati pubblici** in linea con le condizioni stabilite dalla legge sui servizi digitali. In particolare, X vieta ai ricercatori idonei di **accedere in modo indipendente ai** suoi dati pubblici come – al contrario - indicato nelle sue condizioni di servizio. Inoltre, il processo di X volto a **concedere ai ricercatori idonei l'accesso alla sua interfaccia per programmi applicativi (API)** sembra dissuadere i ricercatori dallo svolgere i loro progetti di ricerca.

A seguito del parere preliminare della Commissione UE X ha ora la possibilità di controdedurre e rispondere per iscritto alle conclusioni preliminari. Parallelamente sarà consultato il Comitato europeo per i servizi digitali.

Se il parere preliminare della Commissione dovesse essere infine confermato, la Commissione adotterebbe una decisione di non conformità che accerta che X viola gli articoli 25, 39 e 40 (12) della legge sui servizi digitali. Tale decisione potrebbe comportare sanzioni pecuniarie fino al 6 % del fatturato mondiale totale annuo del prestatore e ordinare a quest'ultimo di adottare misure per porre rimedio alla violazione. Una decisione di non conformità può anche far scattare un periodo di vigilanza rafforzato per garantire il rispetto delle misure che il fornitore intende adottare per porre rimedio alla violazione. La Commissione può inoltre imporre penalità di mora per costringere una piattaforma a conformarsi.

INFORMATION TECHNOLOGY

12 Luglio 2024 - Corte di Cassazione: in caso di bonifico errato la banca è responsabile se non verifica la corrispondenza tra IBAN e beneficiario e non può appellarsi alla privacy per rifiutare di fornire i dati personali del percettore per errore.

Una banca, nel dare esecuzione all'ordine di bonifico di un proprio cliente, non si era avveduta della mancata corrispondenza tra il codice IBAN riportato nell'ordine medesimo e il nominativo del beneficiario indicato. Richiesta dal cliente di fornire i dati del percettore per errore delle somme, la banca si era rifiutata sostenendo di non poter accogliere la richiesta del cliente a causa della normativa a tutela della riservatezza dei dati personali.

La Prima Sezione Civile della Corte Suprema, al contrario, con ordinanza n. 17415/2024, ha pronunciato il seguente principio di diritto: *«in tema di responsabilità di una banca per operazioni effettuate a mezzo di strumenti elettronici, allorquando il beneficiario, nominativamente indicato, di un pagamento da eseguirsi tramite bonifico sia sprovvisto di conto di accredito presso la banca intermediaria, sicché nemmeno è utilizzabile la specifica disciplina ex art. 24 del d.lgs. n. 11 del 2010, si applicano le regole di diritto comune, per cui grava sull'intermediaria stessa, responsabile, secondo la teoria del "contatto sociale qualificato", nei confronti del beneficiario rimasto insoddisfatto a causa dell'indicazione, rivelatasi inesatta, del proprio IBAN, l'onere di dimostrare di aver compiuto l'operazione di pagamento, richiestagli dal solvens, adottando tutte le cautele necessarie al fine di scongiurare il rischio di un'erronea individuazione di detto beneficiario, o quanto meno, di essersi adoperata per consentirgli la individuazione del soggetto concretamente gratificato del pagamento destinato, invece, al primo, anche comunicandogli, ove necessario, i relativi dati anagrafici».*

9 Luglio 2024 – Corte di Cassazione: è valida l'impugnazione del licenziamento trasmessa mediante l'invio di una PEC con allegato un file word.

La Cassazione precisa che il requisito della impugnazione per iscritto del licenziamento, in assenza della previsione di modalità specifiche, deve ritenersi assolto anche mediante l'invio di una PEC con allegato un file formato word.

Con ordinanza n. 18529 dell'8 luglio 2024, la sezione Lavoro enuncia il seguente principio di diritto:

«Ai sensi dell'art. 6 della legge n. 604/66 il requisito della impugnazione per iscritto del licenziamento deve ritenersi assolto, in assenza della previsione di modalità specifiche, con qualunque modalità che comporti la trasmissione al destinatario di un qualsiasi atto scritto avente contenuto idoneo a comunicare l'intenzione del lavoratore di impugnare il licenziamento e allo stesso con certezza riferibile, pertanto anche mediante invio di una PEC con allegato un file formato word, non essendo necessario l'invio di una copia informatica di un documento analogico ai sensi dell'art.22 del decreto legislativo n. 82 del 2005».

8 Luglio 2024 – Consiglio di Stato: illegittima l'esclusione di un concorrente da una gara per aver inviato l'offerta tecnica attraverso il servizio We Transfer.

Il Consiglio di Stato, con la sentenza 5789/2024, si è pronunciato sull'appello proposto da una società relativo all'esclusione da una gara per l'affidamento di lavori di costruzione di aule universitarie.

Il TAR Calabria aveva respinto il ricorso, sostenendo che il ricorrente non aveva rispettato le istruzioni per la presentazione delle offerte, ed in effetti – a causa della impossibilità di caricare l'intera offerta tecnica sulla piattaforma di gara per limiti di capienza – la società aveva trasmesso l'offerta tecnica via *We Transfer*.

Il Consiglio di Stato ha però accolto l'appello chiarendo che l'invio dell'offerta tecnica attraverso *WeTransfer* non legittima l'esclusione del concorrente per violazione del principio di segretezza delle offerte. Ciò



soprattutto quando vengono scelte piattaforme eccessivamente rigide e che rendono difficoltosa la presentazione delle offerte, come nel caso esaminato da Palazzo Spada.
