AVVERA

2023 NEWSLETTER DICEMBRE

SEDE LEGALE E OPERATIVA
20146 Milano
via Sardegna, 21

SEDE OPERATIVA CERTIFICATA
21040 Origgio (VA)
Largo UmbertoBoccioni, 1

ALTRE SEDI
61211 Pesaro (PU)
via Giasone del Maino, 13
33100 Udine (UD)
via G. Tullio, 22

TELEFONO
+39 0296515401

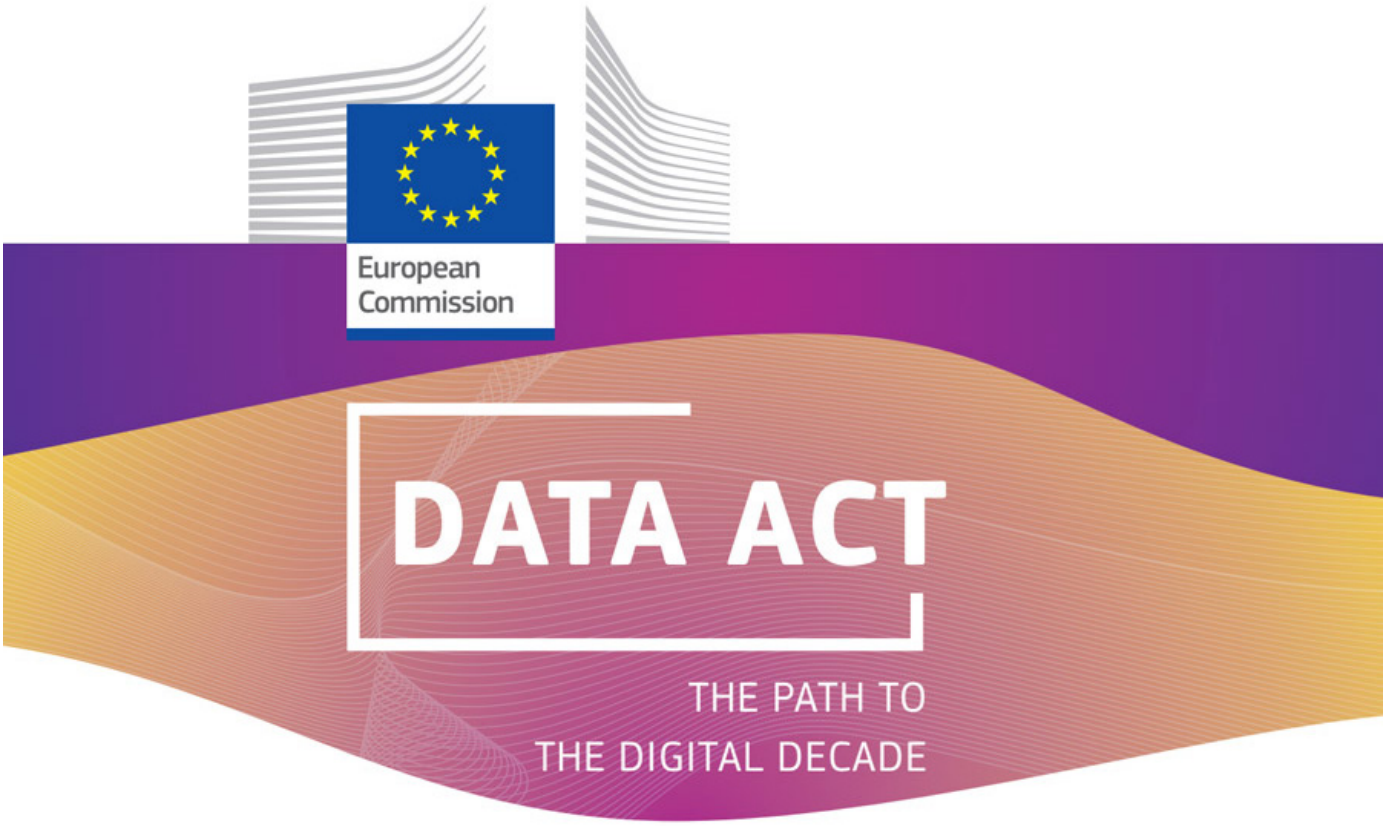
FAX
0296515499

C.F./P.IVA 06047090961
CAP. SOC. 300.000 EURO I.V.
Reg. Impo. MI
06047090961
REA 1866500
WWW.AVVERA.IT
AVVERA@LEGALMAIL.IT

C.F./P.IVA 06047090961
CAP. SOC. 300.000 EURO I.V.
Reg. Impo. MI
06047090961
REA 1866500

WWW.AVVERA.IT
AVVERA@LEGALMAIL.IT

DATA ACT E IL CONSENSO DELL'UTENTE AL TRATTAMENTO E CONDIVISIONE DEI DATI



Con l'obiettivo di rafforzare l'economia dei dati, ridurre il divario digitale e assistere le competenze europee nel settore tecnologico, il Data Act, che integra il Regolamento sulla Governance dei dati (Regolamento UE 2022/868), vuole agevolare le imprese, in particolare alle PMI e alle start-up, garantendo neutralità dell'accesso ai dati, portabilità e interoperabilità dei dati ed evitando effetti di dipendenza nei confronti di imprese molto grandi con un notevole potere economico nell'economia digitale ("Gatekeeper", come disciplinati nel Regolamento (UE) 2022/1925, c.d. Digital Market Act).

Il Data Act individua gli strumenti che possono raccogliere e generare dati (personali e non):

- i prodotti connessi, intesi come beni che ottengono, generano o raccolgono dati accessibili durante l'utilizzo, in grado di comunicare dati tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso da dispositivo e la cui funzione primaria non è la conservazione, il trattamento o la trasmissione di dati per conto terzi;
- i servizi correlati, intesi come servizi digitali, anche software (esclusi i servizi di comunicazione elettronica), strettamente interconnessi con un prodotto, in modo tale che l'assenza impedirebbe al prodotto di svolgere una o più delle proprie funzioni, e che comporta l'accesso ai dati dal prodotto connesso da parte del fornitore o del servizio.

Obiettivo del Data Act è rendere sempre disponibili gratuitamente all'utente i propri dati (personali e non) che sono stati raccolti, generati, utilizzati e conservati dai prodotti e servizi.

Con la medesima logica dei diritti di accesso e di portabilità dei dati personali, come disciplinati dal Regolamento (UE) 2016/679, i dati dell'utente dovranno essere accessibili in un formato completo e di uso comune, tramite sistemi di semplice e sicuro utilizzo e che siano fruibili, con gli adeguamenti minimi necessari, ad essere esportati per l'utilizzo di terzi soggetti, ricomprendendo i relativi metadati necessari per interpretare e utilizzare tali dati.

È da considerare con particolare attenzione, il caso di un prodotto connesso oppure di un servizio correlato, che genera dati riferibili a una persona fisica identificata o identificabile (interessato) e per cui il relativo trattamento deve essere soggetto alle norme stabilite ai sensi del GDPR, anche quando non sia possibile distinguere tra i dati personali e non. In quest'ottica, i prodotti connessi e i servizi correlati devono essere progettati, fabbricati e forniti, affinché vi sia il minor impatto possibile sulla privacy (intesa in senso generale) degli interessati, offrendo la possibilità di esercitare direttamente i diritti di cui godono gli interessati (articoli 15-22 GDPR), ove tecnicamente possibile.

DATA ACT E IL CONSENSO DELL'UTENTE AL TRATTAMENTO E CONDIVISIONE DEI DATI

In linea con questo principio di tutela degli utenti e in maniera similare a quanto disciplinato dall'articolo 12 del GDPR, il Data Act vorrebbe prevedere che siano fornite all'utente le informazioni minime necessarie, prima della conclusione di un accordo con un fornitore di servizi correlati, nel caso lo stesso possa avere accesso ai dati raccolti e generati durante la fornitura di tali servizi. Infatti, l'articolo 3 del Data Act attualmente prevede che tali informazioni siano somministrate in maniera semplice e in un formato chiaro e comprensibile, tra cui, in particolare:

- la natura, il volume, la frequenza di raccolta e il formato dei dati, nonché le modalità di accesso e recupero dei dati da parte dell'utente, compreso il periodo di conservazione;
- la natura e il volume stimato dei dati generati durante la fornitura del servizio correlato, nonché le modalità di accesso e recupero dei dati da parte dell'utente;
- le opzioni di consenso dettagliate e significative per il trattamento dei dati;
- se il fornitore di servizi che fornisce il servizio correlato, in qualità di titolare dei dati, intende utilizzare i dati consultati dal prodotto connesso stesso o consentire a uno o più terzi di utilizzare i dati per finalità concordate con l'utente;
- i dati identificativi del fornitore del servizio correlato e, ove applicabile, di altre parti incaricate del trattamento dei dati;
- i mezzi di comunicazione che consentono all'utente di contattare rapidamente il fornitore e di comunicare efficacemente con il suo personale;
- le modalità con cui l'utente può richiedere che i dati siano condivisi con un destinatario dei dati e, se del caso, revocare il consenso alla condivisione dei dati;
- le modalità con cui l'utente è in grado di gestire le autorizzazioni per consentire l'utilizzo dei dati, ove possibile con opzioni di autorizzazione dettagliate e comprendenti la possibilità di revocare tali autorizzazioni a un titolare dei dati o ai terzi nominati dal titolare dei dati, o di escludere gli indirizzi geografici;
- la durata dell'accordo tra l'utente e il fornitore del servizio correlato, nonché le modalità per risolvere l'accordo anticipatamente.

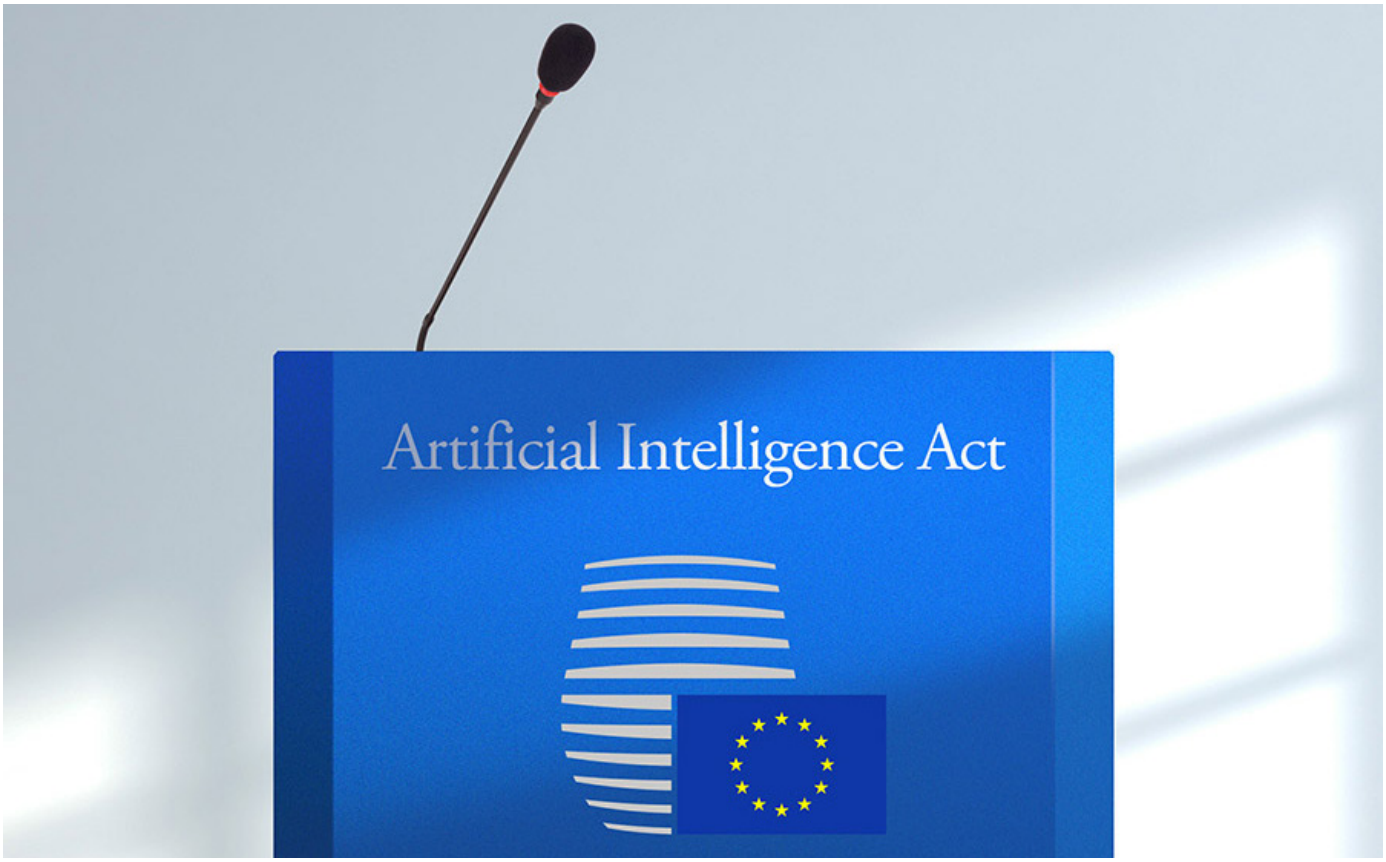
Infine, ai sensi dell'articolo 6 del Data Act, i destinatari che ricevono i dati su richiesta dell'utente devono trattare tali dati solo per le finalità e alle condizioni concordate con l'utente, rispettando i requisiti posti dalla normativa sulla protezione dei dati personali e non devono, in particolare:

- rendere indebitamente difficile l'esercizio dei diritti o delle scelte degli utenti;
- utilizzare i dati che riceve per la profilazione di persone fisiche, se non in conformità delle disposizioni del GDPR;
- comunicare a terzi i dati senza informare l'utente in modo chiaro e facilmente accessibile e senza chiedere l'esplicita autorizzazione contrattuale dell'utente;
- mettere i dati che riceve a disposizione di un'impresa che fornisce servizi di piattaforma di base per i quali uno o più di tali servizi sono stati designati come Gatekeeper;
- utilizzare i dati che riceve per sviluppare un prodotto in concorrenza con il prodotto da cui provengono i dati consultati né condividere i dati con un altro terzo a tal fine.

Fonti

https://www.europarl.europa.eu/doceo/document/TA-9-2023-0069_IT.html

ACCORDO SU AI ACT, DETTAGLI SULLA NORMATIVA EUROPEA SULL'INTELLIGENZA ARTIFICIALE



Venerdì 8 Dicembre 2023, il Parlamento e il Consiglio dell'Unione Europea hanno trovato un accordo provvisorio sull'Artificial Intelligence Act (AI Act), per regolamentare come gli strumenti di intelligenza artificiale possano essere utilizzati e stabilirne i limiti tramite dei divieti. L'obiettivo sarebbe quello di favorire lo sviluppo e l'utilizzo dei sistemi di intelligenza artificiale, tutelando al contempo i diritti e le libertà fondamentali dei cittadini europei (in particolare, la protezione dei dati personali e la privacy).

Sulla base delle informazioni ad oggi disponibili Parlamento e Consiglio dell'Unione Europea avrebbero concordato di vietare l'utilizzo dell'intelligenza artificiale per le seguenti attività:
- utilizzo di sistemi di categorizzazione biometrica che utilizzano caratteristiche particolari di carattere sensibile (ad esempio, convinzioni politiche, religiose, filosofiche, orientamento sessuale, razza);
- raccolta non mirata di immagini del volto da Internet o da filmati di telecamere a circuito chiuso per la creazione di database di riconoscimento facciale;
- rilevazione delle emozioni sul posto di lavoro e nelle istituzioni scolastiche;
- classificazione sociale basata sul comportamento sociale o sulle caratteristiche personali;
- manipolazione del comportamento umano per aggirare il loro libero arbitrio;
- approfittare delle vulnerabilità delle persone (a causa della loro età, disabilità, situazione sociale o economica).

Sarebbero state concordate anche delle garanzie ed eccezioni per un utilizzo dei sistemi di identificazione biometrica in spazi accessibili al pubblico per finalità di contrasto alla criminalità, a condizione che vi sia un'autorizzazione preventiva da parte dell'autorità giudiziaria e con riferimento ad un elenco rigorosamente definito di reati. Un utilizzo dei sistemi di identificazione biometrica "post-remoto" verrebbe utilizzato esclusivamente per la ricerca mirata di una persona condannata o sospettata di aver commesso uno dei predetti reati. Invece, un utilizzo dei sistemi di identificazione biometrica "in tempo reale" sarebbe conforme a condizioni rigorose e il suo impiego sarebbe limitato ad una delle seguenti finalità:
- ricerche mirate di vittime (per rapimento, traffico di esseri umani, sfruttamento sessuale),
- prevenzione di una minaccia terroristica specifica e attuale, localizzazione o identificazione di una persona sospettata di aver commesso uno dei reati specifici che saranno menzio-

nati nel Regolamento (ad esempio, terrorismo, traffico di esseri umani, sfruttamento sessuale, omicidio, rapimento, stupro, rapina a mano armata, partecipazione a un'organizzazione criminale, reati ambientali).

Per i sistemi di intelligenza artificiale classificati come ad alto rischio (a causa del loro potenziale danno significativo alla salute, alla sicurezza, ai diritti fondamentali, all'ambiente, alla democrazia e allo stato di diritto), sarebbero stati concordati degli obblighi precisi, tra cui una valutazione obbligatoria dell'impatto sui diritti fondamentali, da applicarsi ai sistemi di intelligenza artificiale nel settore assicurativo e bancario e nel caso possa condizionare il comportamento degli elettori e l'esito delle elezioni. I cittadini dovrebbero avere anche il diritto di presentare reclami sui sistemi di intelligenza artificiale e di ricevere spiegazioni sulle decisioni basate su tali sistemi ad alto rischio che hanno un impatto sui loro diritti.

Il Regolamento dovrebbe introdurre anche delle norme specifiche per i modelli di intelligenza artificiale di uso generale (GPAI), che dovranno aderire ai requisiti di trasparenza proposti inizialmente dal Parlamento, includendo la stesura di una documentazione tecnica, il rispetto della legge sul copyright dell'UE e la diffusione di sintesi dettagliate sui contenuti utilizzati per la formazione.

Per i modelli GPAI ad alto impatto che potrebbero comportare rischi sistemici, dovrebbero essere previsti degli obblighi più stringenti, relativi alla gestione dei rischi e al monitoraggio degli incidenti gravi, alla valutazione dei modelli e ai test avversari, al fine di garantire la sicurezza informatica e riferire sulla loro efficienza energetica. Su questo punto, gli eurodeputati avrebbero anche insistito sul fatto che, fino alla pubblicazione di standard UE armonizzati, i modelli GPAI con rischio sistemico possano affidarsi a codici di pratica e di condotta.

L'inosservanza delle norme potrebbe portare a multe che vanno da 35 milioni di euro o il 7% del fatturato annuo globale (a seconda di quale sia il valore più alto) per le violazioni delle applicazioni di intelligenze artificiali vietate, 15 milioni di euro o il 3% per le violazioni di altri obblighi e 7,5 milioni di euro o l'1,5% per la fornitura di informazioni errate. Sarebbero previsti tetti più proporzionati per le sanzioni amministrative per le PMI e le start-up in caso di violazioni dello AI Act.

L'accordo politico sarà soggetto ad approvazione formale del Parlamento e il Consiglio dell'Unione Europea e dovrebbe entrare in vigore 20 giorni dopo la pubblicazione nella Gazzetta Ufficiale. Il Regolamento dovrebbe essere applicabile due anni dopo la sua entrata in vigore, ad eccezione di alcune disposizioni specifiche, infatti i divieti si dovrebbero applicare dopo 6 mesi, mentre le norme sull'IA per scopi generali si applicheranno dopo 12 mesi. Per superare il periodo di transizione prima che il Regolamento diventi generalmente applicabile, la Commissione intende lanciare un "Patto per l'IA", con l'obiettivo di riunire gli sviluppatori europei e internazionali, che su base volontaria volgiano impegnarsi ad attuare gli obblighi fondamentali del nuovo Regolamento prima della sua attuazione.

Fonti:

https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai

https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473

NEWSLETTER DICEMBRE

AVVERA

SEDE LEGALE E OPERATIVA
20146 Milano
via Sardegna, 21

SEDE OPERATIVA CERTIFICATA
21040 Origgio (VA)
Largo Umberto Boccioni, 1

ALTRE SEDI
61211 Pesaro (PU)
via Giasone del Maino, 13

33100 Udine (UD)
via G. Tullio, 22

TELEFONO
+39 0296515401

FAX
0296515499

C.F./P.IVA 06047090961
CAP. SOC. 300.000 EURO I.V.
Reg. Impo. MI
06047090961
REA 1866500

WWW.AVVERA.IT
AVVERA@LEGALMAIL.IT

CSQ ISO 9001 CSQ ISO 45001 CSQ ISO/IEC 27001