ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

Privacy:
tra semplificazioni e nuovi modelli

Cesare De Santis

Roma 15/05/2026

Agenda

- Presentazione relatore
- Privacy: tra semplificazioni e nuovi modelli
- Bibliografia & sitografia
- Q&A

Agenda

- **Presentazione relatore**
- Privacy: tra semplificazioni e nuovi modelli
- Bibliografia & sitografia
- Q&A

Presentazione relatore

Cesare De Santis

Ho lavorato a lungo per Enti della P.A. (Difesa/Aeronautica) ed aziende private (banca e alcune società di consulenza di emanazione bancaria) prima di intraprendere, nel 2008, un autonomo percorso professionale.

Attualmente sono amministratore unico di PRIMAe srl a socio unico, che opera principalmente sui temi della conformità normativa e della protezione dei dati personali. Tra i clienti di PRIMAe srl a socio unico si annoverano banche e società finanziarie nonché una società consortile di banche e un fondo sanitario di emanazione bancaria.
Assicuriamo il servizio DPO ad alcune banche e società.

Titoli/certificazioni/attestati

Laureato in Scienze statistiche ed attuariali, abilitato alla professione di attuario, CISM

Agenda

- Presentazione relatore
- **Privacy: tra semplificazioni e nuovi modelli**
- Bibliografia & sitografia
- Q&A

Evoluzione in corso della normativa: motivazioni

« …. Sebbene le parti interessate abbiano in generale ritenuto il regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati) equilibrato e valido e ancora adeguato allo scopo, alcuni soggetti, in particolare ***le piccole imprese e le associazioni con un numero limitato di operazioni di trattamento dei dati non intensive e spesso a basso rischio, hanno espresso preoccupazioni in merito all'applicazione di alcuni obblighi del regolamento generale sulla protezione dei dati.*** *Alcune di queste preoccupazioni possono essere affrontate attraverso un'interpretazione e un'applicazione più coerenti e armonizzate in tutti gli Stati membri, mentre* ***altre richiedono modifiche mirate della legislazione*** *… omissis …»*

Evoluzione in corso della normativa: sintesi proposta

« .... In questo contesto, le modifiche contenute nella presente proposta mirano ad affrontare tali preoccupazioni, in particolare chiarendo alcune definizioni chiave, ad esempio i ***concetti di dati personali****; facilitando la conformità, ad esempio sostenendo i responsabili del trattamento per quanto riguarda i criteri e i mezzi per determinare se i dati risultanti dalla pseudonimizzazione non costituiscono dati personali, in relazione agli* ***obblighi di informazione e alle notifiche di violazione dei dati*** *alle autorità di controllo; nonché chiarendo alcuni aspetti relativi al* ***trattamento dei dati per la formazione e lo sviluppo dell'IA****. Le modifiche proposte affrontano anche la mancanza di chiarezza sulle condizioni per la* ***ricerca scientifica****, ... omissis ... Si propone inoltre di estendere le* ***eccezioni all'obbligo di informazione per il trattamento*** *... omissis ... Inoltre, è ormai da tempo necessaria una soluzione normativa sul problema della "****consent fatigue****" (stanchezza da consenso) e della* ***proliferazione dei banner sui cookie*** *...omissis ... Le modifiche presentate nel presente regolamento introdurranno* ***un punto di accesso unico attraverso il quale i soggetti potranno adempiere simultaneamente ai loro obblighi di segnalazione degli incidenti previsti da più atti giuridici.*** *Promuovendo il principio "segnalare una volta, condividere più volte", il punto di accesso unico ridurrà gli oneri amministrativi per i soggetti ... omissis ...»*

Modifiche proposte: il Digital Omnibus GDPR 1/4

Modifiche al regolamento (UE) 2016/679, al regolamento (UE) 2018/1725 e alla direttiva 2002/58/CE. L'articolo 3 della proposta introdurrebbe modifiche mirate al regolamento (UE) 2016/679 ("regolamento generale sulla protezione dei dati").

- *il paragrafo 1 chiarirebbe la definizione di dati personali di cui all'articolo 4 del regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati) precisando che* ***le informazioni non sono da considerarsi dati personali per un determinato soggetto quando non esistono mezzi ragionevolmente utilizzabili per identificare la persona fisica*** *a cui si riferiscono. Di conseguenza, tale entità non rientrerebbe, in linea di principio, nell'ambito di applicazione di tale regolamento.*
- *Il paragrafo 2 prevedrebbe due ulteriori deroghe al trattamento di categorie particolari di dati: prevedrebbe* ***una deroga al divieto generale di trattamento dei dati biometrici, quando ciò sia necessario per confermare l'identità dell'interessato e quando i dati e i mezzi per tale verifica siano sotto il controllo esclusivo di tale interessato****.* ***Prevederebbe inoltre un'esenzione per il trattamento residuale di categorie particolari di dati personali per lo sviluppo e il funzionamento di un sistema di IA o di un modello di IA****, a determinate condizioni, tra cui l'adozione di misure organizzative e tecniche adeguate per evitare la raccolta di categorie particolari di dati personali e la cancellazione di tali dati.*
- *Il paragrafo 3 chiarirebbe la situazione di cui all'articolo 12 del regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati) in cui* ***il diritto di accesso è abusato dagli interessati per fini diversi dalla protezione dei loro dati personali.*** *Di conseguenza, il titolare del trattamento potrebbe rifiutarsi di soddisfare la richiesta o addebitare una tariffa ragionevole. Inoltre, chiarirebbe le condizioni per dimostrare che una richiesta di accesso era eccessiva.*

Modifiche proposte: il Digital Omnibus GDPR 2/4

- *Il paragrafo 4 si concentrerebbe sull'obbligo del titolare del trattamento di **informare gli interessati** in merito al trattamento dei loro dati personali ai sensi dell'articolo 13 del regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati), **eliminando tale obbligo nei casi in cui vi siano motivi ragionevoli per ritenere che l'interessato disponga già delle informazioni**, a meno che il titolare del trattamento non trasmetta i dati ad altri destinatari o categorie di destinatari, trasferisca i dati verso un paese terzo, effettui un processo decisionale automatizzato o il trattamento sia suscettibile di comportare un rischio elevato per i diritti dell'interessato.*
- *Il paragrafo 5 **chiarirebbe i requisiti per il processo decisionale individuale automatizzato** ai sensi dell'articolo 22 del regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati), nel contesto della stipula o dell'esecuzione di un contratto tra l'interessato e un titolare del trattamento, in particolare che il requisito della «necessità» è indipendente dal fatto che la decisione possa essere presa con mezzi diversi da quelli esclusivamente automatizzati.*
- *Il paragrafo 6 allineerebbe l'obbligo del titolare del trattamento di notificare le violazioni dei dati all'autorità di controllo competente ai sensi dell'articolo 33 del regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati) con il suo obbligo di notificare tali violazioni agli interessati, stabilendo che **la notifica è richiesta solo se una violazione dei dati può comportare un rischio elevato per i diritti dell'interessato**. Estenderebbe inoltre il termine per la notifica a 96 ore. Si propone inoltre che i responsabili del trattamento utilizzino il punto di accesso unico quando notificano le violazioni dei dati all'autorità di controllo. Inoltre, il comitato europeo per la protezione dei dati sarebbe tenuto a preparare e presentare alla Commissione una proposta di **modello comune per le notifiche di violazioni dei dati**, che la Commissione sarebbe autorizzata ad adottare mediante un atto di esecuzione, previa revisione, se necessario.*

Modifiche proposte: il Digital Omnibus GDPR 3/4

- *Il paragrafo 7 armonizzerebbe gli elenchi delle attività di trattamento che richiedono e non richiedono una **valutazione d'impatto sulla protezione dei dati, prevedendo che a livello dell'UE sia fornito un unico elenco delle operazioni di trattamento che richiedono e non richiedono una valutazione d'impatto sulla protezione dei dati, contribuendo in tal modo all'armonizzazione del concetto di rischio elevato**. Il comitato europeo per la protezione dei dati sarebbe tenuto a preparare proposte relative a tali elenchi. Sarebbe inoltre tenuto a preparare una proposta relativa a un modello comune e a una metodologia comune per lo svolgimento delle valutazioni d'impatto sulla protezione dei dati, che la Commissione sarebbe autorizzata ad adottare mediante un atto di esecuzione, previa revisione, se necessario.*
- *Il paragrafo 8 stabilisce che **la Commissione può sostenere**, insieme al comitato europeo per la protezione dei dati, **i responsabili del trattamento nel valutare se i dati risultanti dalla pseudonimizzazione non costituiscano dati personali**, specificando i mezzi e i criteri pertinenti per tale valutazione, compreso lo stato dell'arte delle tecniche disponibili e i criteri per valutare il rischio di reidentificazione...*
- *Il paragrafo 12 **riforma il regime giuridico relativo al trattamento dei dati personali su o da apparecchiature terminali ("dispositivi connessi"),** attualmente parte della direttiva 2002/58/CE (direttiva ePrivacy). Nel regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati) è inserito un nuovo **articolo 88 bis** che stabilisce il requisito del consenso per la conservazione o l'accesso ai dati personali sulle apparecchiature terminali delle persone fisiche e che assoggetta il trattamento dei dati personali su e da apparecchiature terminali alle norme del regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati). Un nuovo **articolo 88 ter** del regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati), per le indicazioni automatizzate e leggibili da dispositivi elettronici delle scelte individuali e il rispetto di tali indicazioni da parte dei fornitori di siti web una volta disponibili gli standard.*

Modifiche proposte: il Digital Omnibus GDPR 4/4

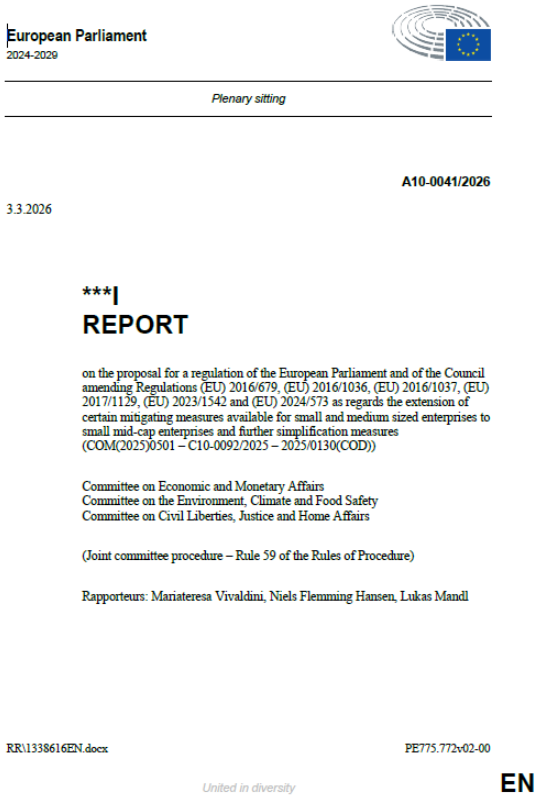
- *Nell'articolo 4: l'articolo 4 della proposta introdurrebbe modifiche mirate al regolamento (UE) 2018/1725[(1)] , al fine di allinearne il testo alle modifiche al regolamento (UE) 2016/679 introdotte nell'articolo 3.*
- *Articolo 5: l'articolo 5 prevede modifiche alla direttiva 2002/58/CE, la direttiva sulla privacy e le comunicazioni elettroniche ("direttiva ePrivacy"). L'articolo 4 di tale direttiva è abrogato. L'aggiunta all'articolo 5, paragrafo 3, di tale direttiva consente di trasferire al regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati) le norme relative alla conservazione e all'accesso ai dati personali dalle apparecchiature terminali di una persona fisica, mediante l'inserimento di un nuovo articolo 88 bis del regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati), come descritto sopra.*

(1) *Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (Testo rilevante ai fini del SEE.)*

Digital Omnibus per GDPR: un aggiornamento

Continua intanto in Europa il percorso di evoluzione normativa, in ottica di semplificazione, del GDPR, e di altre normative, iniziato alla fine dell'anno scorso, con la presentazione del "Digital Omnibus".

Il Parlamento UE, all'inizio di marzo 2026, ha approvato in seduta plenaria il c.d. Omnibus IV il cui testo costituirà la base per le negoziazioni successive (c.d. Trilogo).



European Parliament
2024-2029

Plenary sitting

A10-0041/2026

3.3.2026

***I
REPORT

on the proposal for a regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures
(COM(2025)0501 – C10-0092/2025 – 2025/0130(COD))

Committee on Economic and Monetary Affairs
Committee on the Environment, Climate and Food Safety
Committee on Civil Liberties, Justice and Home Affairs

(Joint committee procedure – Rule 59 of the Rules of Procedure)

Rapporteurs: Mariateresa Vivaldini, Niels Flemming Hansen, Lukas Mandl

RR\1338616EN.docx PE775.772v02-00

EN United in diversity EN

Aggiornamento delle definizioni di categorie di imprese

- ✓ Per «micro, piccole e medie imprese» si intendono le imprese *che occupano meno di 250 persone e che hanno un fatturato annuo non superiore a 50 milioni di EUR o un totale di bilancio annuo non superiore a 43 milioni di EUR*;

- ✓ Per «**piccole imprese a media capitalizzazione**(1)» si intendono le imprese *che non appartengono alla categorie delle micro, piccole o medie imprese e che:*
  - *(i) impiegano meno di 1000 dipendenti;*
  - *(ii) e hanno un fatturato annuo non superiore a 200 milioni di EUR*

  oppure;
  - *(iii) hanno un totale di bilancio annuo non superiore a 172 milioni di EUR;*

(1) *Small Mid-Cap enterprises (SMC)*

Semplificazione per aziende di minore dimensione

« … Il presente report introduce una definizione armonizzata e operativa delle piccole imprese a capitalizzazione intermedia (SMC) in una serie di atti dell'Unione, al fine di migliorare la chiarezza giuridica, rafforzare la coerenza normativa e garantire una ***semplificazione proporzionata per le imprese che hanno superato la categoria delle PMI ma continuano a dover affrontare ostacoli strutturali simili a quelli che colpiscono le imprese più piccole*** *…»*

Allargamento esenzioni relative al ROPA(1)

La revisione dell'art. 30 del GDPR, con l'aggiunta di nuovi paragrafi, è finalizzata ad allargare le esenzioni attualmente previste all'obbligo di tenere ed aggiornare il Registro delle Attività di Trattamento.

5. Gli obblighi di cui ai paragrafi 1 e 2 **non si applicano alle *microimprese, alle piccole e medie imprese, alle piccole imprese a capitalizzazione intermedia o alle organizzazioni* che impiegano meno di *1.000* persone**, a meno che *e nella misura in cui una specifica attività* di trattamento *da esse svolta:*

(i) sia suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, ai sensi dell'articolo 35*, in particolare per quanto riguarda i casi di cui al paragrafo 3 di tale articolo*;

oppure

(ii) costituisca un'attività principale ai sensi dell'articolo 37, paragrafo 1, lettera b) o c). In tal caso, gli obblighi di cui ai paragrafi 1 e 2 del presente articolo si applicano esclusivamente a tale specifica attività di trattamento.

5 bis. In deroga al paragrafo 5, **gli obblighi di cui ai paragrafi 1 e 2 si applicano alle autorità e agli organismi pubblici**.».

(1) *Record of Processing Activities*

Revisione ROPA: trattamento dati sensibili (1/2)

Modifica al Considerando 10 GDPR

10. … In tale contesto, il trattamento di categorie particolari di dati personali *da parte di micro, piccole e medie imprese (PMI), SMC o organizzazioni* con un numero di *dipendenti non superiore a 1.000*, necessario ai fini dell'adempimento degli obblighi e dell'esercizio di diritti specifici del titolare del trattamento o dell'interessato nel settore del diritto del lavoro, della sicurezza sociale e della protezione sociale, come di cui all'articolo 9, paragrafo 2, lettera b), del regolamento (UE) 2016/679, ***non comporterebbe sempre un rischio elevato per gli interessati*** *e* non dovrebbe, di per sé, richiedere la conservazione dei registri *delle attività* di trattamento*,* ***a meno che non si valuti che il trattamento possa comportare un rischio elevato***.

Revisione ROPA: trattamento dati sensibili (2/2)

Aggiunta del Considerando 10 bis

(10 bis) Allo stesso tempo, l'obbligo di conservare i registri delle attività di trattamento **dovrebbe sempre applicarsi alle attività per le quali il titolare del trattamento o il responsabile del trattamento *è tenuto a designare un responsabile della protezione dei dati*** ai sensi dell'articolo 37, paragrafo 1, lettere b) e c), del regolamento (UE) 2016/679.

Tali attività principali consistono in operazioni di trattamento che, in virtù della loro natura, della loro portata e/o della loro finalità, richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, oppure quando le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento su larga scala di categorie particolari di dati ai sensi dell'articolo 9 e di dati personali relativi a condanne penali e reati di cui all'articolo 10 del regolamento (UE) 2016/679.

Tali casi rivestono particolare importanza quando il trattamento dei dati personali presenta rischi strutturali o ricorrenti e dovrebbero pertanto richiedere che siano sempre conservati i registri delle relative attività di trattamento.

Tuttavia, nel settore privato, le attività principali di un titolare del trattamento o di un responsabile del trattamento riguardano le loro attività primarie e non riguardano il trattamento dei dati personali come attività accessorie. **Ad esempio, qualora il trattamento di categorie particolari di dati personali ai sensi dell'articolo 9, paragrafo 2, lettera b), del regolamento (UE) 2016/679 costituisse un'attività accessoria, non sarebbe necessario conservare registrazioni relative a tale specifica attività di trattament**o.

Codici/certificazione: strumenti semplificati per PMI/SMC

Aggiornamento artt. 40 e 42 GDPR:

- – L'articolo 40, che prevede che gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggino le associazioni e altri organismi che rappresentano categorie di titolari del trattamento o di responsabili del trattamento a elaborare codici di condotta, e che in tal modo **si tenga conto delle esigenze specifiche delle micro, piccole e medie imprese. Tale requisito dovrebbe essere esteso per includere le esigenze specifiche delle SMC.**
- – L'articolo 42, che prevede che, quando gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello dell'Unione, l'istituzione di meccanismi di certificazione in materia di protezione dei dati e di sigilli e marchi di protezione dei dati da parte degli organismi di certificazione di cui all'articolo 43 del presente regolamento o delle autorità di controllo competenti, **si tenga conto delle esigenze specifiche delle micro, piccole e medie imprese. Tale requisito dovrebbe essere esteso anche alle esigenze specifiche delle SMC**.

Il nuovo modello DPIA di EDPB

La valutazione d'impatto del trattamento sulla protezione dei dati personali (DPIA(1)) per quei trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati è stata introdotta dall'art. 35 del GDPR.

I criteri per una DPIA «sufficientemente completa» sono stati pubblicati da Gruppo ex art. 29, ora EDPB, già in una linea guida del 2017 (WP248).

Da parte di Autorità di controllo nazionali (CNIL) sono stati pubblicati modelli (Privacy Impact Assessment) per l'esecuzione di questo adempimento.

Il 14 aprile 2026 l'European Data Protection Board (EDPB) ha pubblicato un nuovo modello di DPIA, ora in consultazione pubblica.

"Il modello di valutazione d'impatto sulla protezione dei dati (DPIA) dell'EDPB è oggetto di una consultazione pubblica (fino al 9 giugno NdR)*. Al termine della consultazione pubblica, il modello sarà messo a punto (previa eventuali modifiche del caso),* ***dopodiché tutte le autorità garanti della protezione dei dati avvieranno le procedure necessarie per adottare tale modello come modello unico o come «meta-modello» con cui saranno compatibili i modelli specifici nazionali.*** *Nel frattempo, le organizzazioni sono invitate a utilizzare questo modello e a fornire un riscontro nell'ambito della consultazione pubblica.»* (*dal sito EDPB con traduzione automatica DeepL)*

(1) Data Protection Impact Assessment

Descrizione del modello DPIA di EDPB

Il modello si sviluppa su 7 sezioni che vanno dall'identificazione degli attori e del contesto del trattamento alla decisione finale, passando per la descrizione sistematica del trattamento, la sua analisi, la verifica di conformità e la valutazione della necessità e proporzionalità di esso nonché la valutazione e gestione del rischio.

0. Panoramica del trattamento

Questa sezione contiene i seguenti elementi: l'identificazione del titolare del trattamento (o dei contitolari, con tabella separata per ciascuno e specificazione delle rispettive responsabilità), l'elenco dei responsabili e sub-responsabili del trattamento con definizione dei rispettivi obblighi e compiti, la denominazione del trattamento (compreso il nome nel registro dei trattamenti), e la pianificazione con le date di avvio e termine nonché condizioni previste per il trattamento.

Fa parte di questa sezione anche la scheda tecnica della DPIA con le motivazioni che hanno portato alla necessità di compilarla e le informazioni relative alle modalità di predisposizione ed al suo completamento e convalida.

1. Descrizione sistematica del trattamento

Questa sezione comprende:

- ✓ la descrizione di alto livello del trattamento in termini di:
  - dati personali trattati, con indicazione di appartenenza a particolari categorie, e categorie di interessati cui si riferiscono,
  - finalità,
  - usi secondari o compatibili dei dati,
  - natura, ambito e contesto del trattamento;
- ✓ la descrizione funzionale del trattamento in termini di:
  - operazioni di trattamento usate,
  - mezzi utilizzati,
  - rispetto codici di condotta.

2. Analisi del trattamento

Questa sezione comprende tre sottosezioni nelle quali vengono trattate:

- ✓ la liceità del trattamento (basa giuridica e motivo per revocare il divieto di trattamento di categorie particolari di dati)
- ✓ la minimizzazione dei dati con pertinenza, destinatari, tempi di conservazione e metriche di qualità dei dati
- ✓ le misure di sostegno alla conformità:
  - ai principi GDPR
  - all'esercizio dei diritti degli interessati
  - ad altri requisiti GDPR (rilascio/revoca consenso, rapporto con responsabili, garanzie per trasferimenti all'estero)
  - alla privacy by design e by default
  - alla sicurezza del trattamento

3. Necessità e proporzionalità del trattamento

In questa sezione sono riportate le considerazioni sulla necessità e proporzionalità del trattamento:

- ✓ Minacce poste dal trattamento, così come è stato progettato e pianificato per essere attuato (comprese misure tecniche, legali/contrattuali e organizzative per mitigare i rischi)
- ✓ Valutazione necessità del trattamento (sia efficace e il meno invasivo possibile per i diritti e le libertà dell'interessato)
- ✓ Valutazione proporzionalità del trattamento (importanza del trattamento e i suoi potenziali benefici per l'interessato e per la collettività)

4. Valutazione e gestione del rischio

Questa sezione riguarda la valutazione e gestione dei rischi ed è suddivisa in

- Impatti sui diritti e sulle libertà degli interessati causati da eventi non predefiniti, accidentali, illeciti o anomali [Minacce derivanti da malfunzionamenti e deviazioni rispetto alla progettazione e alle impostazioni predefinite, minacce alla riservatezza, all'integrità e alla disponibilità dati (relative alla sicurezza informatica), ecc.]
- Metodo utilizzato [livelli gravità/probabilità (scala) nonché metriche, priorità e livello accettazione del rischio]
- Valutazione del rischio intrinseco [probabilità, gravità, fattori modulanti (aggravanti/attenuanti), livello di rischio, accettabilità]
- Piano d'azione (misure mitigazione aggiuntive e rischi mitigati, valutazione del rischio residuo, pianificazione attività per realizzare misure aggiuntive)

5. Coinvolgimento delle parti interessate

Questa sezione comprende il parere del DPO (conclusioni e raccomandazioni) e come è stato dato seguito al suo parere nonché il parere degli interessati o dei loro rappresentanti (spiegare la loro partecipazione al processo di DPIA, incluse le spiegazioni del perché non sia stato ritenuto opportuno che partecipassero o perché non sia stato loro possibile farlo).

6. Conclusione e decisione

Concludere con la decisione sulla fattibilità del trattamento dei dati, che può essere:

- ✓ abbandonare il trattamento dei dati (i rischi sono inaccettabili, non è possibile superare uno dei test richiesti, su consiglio del responsabile della protezione dei dati, degli interessati o dell'Autorità di controllo) o
- ✓ consultare l'Autorità di controllo o;
- ✓ procedere con il trattamento dei dati come previsto o
- ✓ procedere con il trattamento dei dati a determinate condizioni (ovvero modificando la progettazione del trattamento per affrontare meglio i rischi individuati).

In quest'ultimo caso, spiegare le condizioni specifiche che devono essere soddisfatte prima di procedere con il trattamento.

Digital Omnibus AI in approvazione

Brussels, 13 May 2026
(OR. en)

9247/26

Interinstitutional File:
2025/0359 (COD)

SIMPL 99
ANTICI 102
DATAPROTECT 157
CYBER 224
TELECOM 230
CODEC 907

INFORMATION NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence - Letter sent to the European Parliament

At its meeting on 13 May 2026, the Permanent Representatives Committee:

a) confirmed the agreement on the compromise text of the above-mentioned draft Regulation, as it was reached between the negotiating parties on 6 May 2026 and as it is contained in document 9034/26; and

b) authorised the Presidency to address the habitual offer letter to the European Parliament.

The letter together with its annex, as it was sent to the European Parliament, is set out in the Annex.

This information is provided in accordance with point 1 h) of note 9493/20 on 'Strengthening legislative transparency'.

FRIA: che cosa è

La valutazione dell'impatto sui diritti fondamentali [Fundamental Rights Impact Assessment (FRIA)] ai sensi dell'art. 27 "Valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio" comma 1 di AI Act comprende:

a) una descrizione dei processi del deployer in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista;

b) una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza;

c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico;

d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13;

e) una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso;

f) le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo.

DPIA vs FRIA

(9 ter) *all'articolo 27* (dell'AI Act n.d.r.), *il paragrafo 4 è sostituito dal seguente:*

«4. *Se uno qualsiasi degli obblighi previsti dal presente articolo è già soddisfatto attraverso la valutazione d'impatto sulla protezione dei dati condotta ai sensi dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, il responsabile della diffusione* (deployer n.d.r.) *può, nel condurre la valutazione d'impatto sui diritti fondamentali di cui al paragrafo 1 del presente articolo, includere riferimenti incrociati alle sezioni pertinenti di tale valutazione d'impatto sulla protezione dei dati o includere parti rilevanti di tale valutazione d'impatto sulla protezione dei dati nella valutazione d'impatto sui diritti fondamentali.»;*

(9 quater)All'articolo 27, il paragrafo 5 è sostituito dal seguente:

«5. *L'Ufficio AI elabora un modello di questionario, anche mediante uno strumento automatizzato, per agevolare i responsabili della diffusione* (deployers n.d.r.) *nell'adempimento dei loro obblighi ai sensi del presente articolo in modo semplificato. Tale modello, se del caso, offre ai responsabili della diffusione* (deployers n.d.r.) *la possibilità di includere riferimenti incrociati alle sezioni pertinenti della valutazione d'impatto sulla protezione dei dati o di* | *includere parti rilevanti di tale valutazione d'impatto sulla protezione dei dati nella valutazione d'impatto sui diritti fondamentali ai sensi del paragrafo 4 del presente articolo.»;*

Fine della presentazione

Grazie per l’attenzione !

(Nota bene: le slide che seguono sono state richiamate in maniera ipertestuale dall’interno delle slide che precedono)

Allegato 2 - Criteri per una valutazione d'impatto sulla protezione dei dati accettabile

Il WP29 propone i seguenti criteri che i titolari del trattamento possono utilizzare per stabilire se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno oppure se una metodologia per lo svolgimento di una tale valutazione sia sufficientemente completa per garantire il rispetto del regolamento generale sulla protezione dei dati:

- ☐ una descrizione sistematica del trattamento è fornita (articolo 35, paragrafo 7, lettera a)):
  - ☐ la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);
  - ☐ vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
  - ☐ viene fornita una descrizione funzionale del trattamento;
  - ☐ sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);
  - ☐ si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);
- ☐ la necessità e la proporzionalità sono valutate (articolo 35, paragrafo 7, lettera b)):
  - ☐ sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):
    - ☐ misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
      - ☐ finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));
      - ☐ liceità del trattamento (articolo 6);
      - ☐ dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));
      - ☐ limitazione della conservazione (articolo 5, paragrafo 1, lettera e));
    - ☐ misure che contribuiscono ai diritti degli interessati:
      - ☐ informazioni fornite all'interessato (articoli 12, 13 e 14);
      - ☐ diritto di accesso e portabilità dei dati (articoli 15 e 20);
      - ☐ diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);
      - ☐ diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);
      - ☐ rapporti con i responsabili del trattamento (articolo 28);
      - ☐ garanzie riguardanti trattamenti internazionali (capo V);
      - ☐ consultazione preventiva (articolo 36).
- ☐ i rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c)):
  - ☐ l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:
    - ☐ si considerano le fonti di rischio (considerando 90);
    - ☐ sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
    - ☐ sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;
    - ☐ sono stimate la probabilità e la gravità (considerando 90);
  - ☐ sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);
- ☐ le parti interessate sono coinvolte:
  - ☐ si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);
  - ☐ si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9).

Struttura del modello DPIA di EDPB

0 PANORAMICA DEL TRATTAMENTO
0.1 Titolare/i del trattamento
0.2 Responsabile/i del trattamento e sub-responsabile/i
0.3 Denominazione del trattamento
0.4 Pianificazione del trattamento
0.5 Scheda tecnica della Valutazione d'impatto sulla protezione dei dati (DPIA)
1 DESCRIZIONE SISTEMATICA DEL TRATTAMENTO
1.1 Descrizione di alto livello del trattamento
1.1.a Dati personali trattati
1.1.b Finalità del trattamento
1.1.c Usi secondari o compatibili
1.1.d Natura, ambito e contesto del trattamento
1.2 Descrizione funzionale
1.3 Mezzi di trattamento, risorse di supporto e architettura sottostante
1.4 Conformità ai codici di condotta approvati
2 ANALISI DEL TRATTAMENTO
2.1 Liceità del trattamento
2.1.a Base giuridica
2.1.b Motivi per derogare al divieto di trattamento
2.2 Minimizzazione dei dati, periodi di conservazione e qualità dei dati
2.2.a Minimizzazione dei dati e periodi di conservazione
2.2.b Qualità dei dati
2.3 Misure a sostegno della conformità
2.3.a Misure a sostegno della conformità ai principi di cui all'art. 5, comma 1, lettere a)-f) del GDPR
2.3.b Misure a sostegno dell'esercizio dei diritti degli interessati
2.3.c Misure a sostegno della conformità ad altri requisiti del GDPR
2.3.d Misure a sostegno della protezione dei dati fin dalla progettazione e per impostazione predefinita
2.3.e Misure a sostegno della sicurezza del trattamento
3 CONSIDERAZIONI SULLA NECESSITÀ E LA PROPORZIONALITÀ
3.1 Impatto del trattamento sui diritti e sulle libertà degli interessati
3.2 Valutare la necessità del trattamento
3.3 Valutare la proporzionalità del trattamento
4 VALUTAZIONE E GESTIONE DEL RISCHIO
4.1 Valutazione e gestione del rischio
4.1.a Impatto sui diritti e sulle libertà degli interessati causato da eventi non predefiniti, accidentali, illeciti o anomali
4.1.b Metodo
4.1.c Valutazione del rischio intrinseco
4.2 Piano d'azione
4.2.a Misure di mitigazione aggiuntive
4.2.b Valutazione del rischio residuo
4.2.c Piano
5 COINVOLGIMENTO DELLE PARTI INTERESSATE
5.1 Consulenza del DPO
5.2 Opinioni degli interessati o dei loro rappresentanti
6 CONCLUSIONE E DECISIONE

Metriche di qualità dei dati

Accuratezza (Accuracy)
Misura quanto i dati rappresentano correttamente la realtà.
Esempio: percentuale di record con email valide o indirizzi corretti.
Formula tipica:
→ (record corretti / record totali)

Completezza (Completeness)
Valuta se tutti i campi necessari sono popolati.
Esempio: % di profili utente con tutti i campi obbligatori compilati.
Può essere per campo o per record.

Consistenza (Consistency)
Verifica che i dati non siano in conflitto tra sistemi o campi.
Esempio: stessa data di nascita in CRM e sistema billing.

Tempestività / Attualità (Timeliness)
Indica quanto i dati sono aggiornati rispetto al loro uso.
Esempio: età calcolata da una data di nascita aggiornata vs. statica.

Univocità (Uniqueness)
Misura la presenza di duplicati.
Esempio: numero di utenti duplicati rispetto al totale.

Validità (Validity)
Controlla che i dati rispettino formato e regole definite.
Esempio: email che rispettano regex standard, CAP coerenti con il paese.

Integrità (Integrity)
Riguarda la correttezza delle relazioni tra dati (chiavi primarie/esterne).
Esempio: ogni ordine deve essere collegato a un utente esistente.

Pertinenza (Relevance)
Valuta se i dati raccolti sono effettivamente necessari rispetto allo scopo (concetto cruciale anche nel GDPR: minimizzazione dei dati).

Agenda

- Presentazione relatore
- Privacy: tra semplificazioni e nuovi modelli
- **Bibliografia & sitografia**
- Q&A

Bibliografia & Sitografia

Per il report del Parlamento europeo:
https://www.europarl.europa.eu/doceo/document/A-10-2026-0041_IT.html#_section1

Per il modello DPIA di EDPB:
https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/edpb-dpia-template_en

Agenda

- Presentazione relatore
- Privacy: tra semplificazioni e nuovi modelli
- Bibliografia & sitografia
- **Q&A**

Q&A

Contatti

- cesare.desantis@primaedintorni.it

Grazie...