IDENTITÀ DIGITALE

eIDAS 2.0: sicurezza, interoperabilità e impatti sulla compliance

Il Regolamento eIDAS 2.0 introduce un'identità digitale europea uniforme, migliorando sicurezza, interoperabilità e accesso ai servizi. Le novità includono l'European Digital Identity Wallet e potenziati servizi fiduciari. Impatti significativi riguardano la sicurezza informatica e la conformità al D. Lgs. 231/2001, richiedendo formazione, audit e aggiornamenti dei Modelli 231

Pubblicato il 11 lug 2024

Ivan Rotunno
socio AODV231

Roberto Villa
consigliere AODV231

Il 30 aprile 2024 il Consiglio Europeo ha approvato il Regolamento (UE) 1183/2024 ("**eIDAS 2.0**"), che contiene le previsioni di riforma del Regolamento (UE) 910/2014, meglio noto come "Regolamento eIDAS" (*electronic IDentification, Authentication and trust Services*) e finalizzato a integrare i principi introdotti nel 2014 per la creazione di **un'identità digitale europea uniforme**, facilitando l'accesso sicuro ai servizi pubblici e privati, nonché migliorando l'interoperabilità e la sicurezza dei servizi di identificazione elettronica e di trust service a livello europeo.

eIDAS 2.0: la nuova frontiera dei sistemi di identificazione digitale

26 Giugno 2023

di **Nicola Testa e**

Indice degli argomenti

Gli obiettivi di eIDAS 2.0

Le novità apportate da eIDAS 2.0 non sono solo una risposta alle crescenti esigenze di protezione dei dati personali ma rappresentano anche una pietra miliare per **l'innovazione nei servizi fiduciari**, estendendo le loro funzionalità e ampliando le possibilità di verifica di conformità. Queste modifiche avranno un impatto profondo sulle strategie aziendali, imponendo nuovi obblighi in termini di responsabilità amministrativa e spingendo verso l'adozione di misure implementative sempre più sofisticate.

Ai sensi del Considerando 10, il Regolamento eIDAS 2.0 si propone di creare "Un quadro armonizzato in materia di identità digitale [con] l'obiettivo di creare valore economico fornendo un accesso più agevole a beni e servizi e riducendo in modo significativo i costi operativi legati alle procedure di identificazione e autenticazione elettroniche, ad esempio durante l'onboarding (acquisizione) di nuovi clienti, riducendo il rischio di reati informatici, quali furto di identità, furto di dati e frodi online, così da favorire guadagni in termini di efficienza e

promuovere la trasformazione digitale sicura delle microimprese e delle piccole e medie imprese (PMI) dell'Unione."**[1]**

Numerosi sono dunque gli spunti che questa norma offre per un'analisi dal punto di vista della cosiddetta **compliance integrata** poiché la sua disciplina si interseca in numerosi passaggi con le previsioni esistenti dettate in materia di protezione dei dati personali, di sicurezza informatica e assume rilevanza anche ai fini della conformità alla responsabilità amministrativa delle persone giuridiche di cui al D. Lgs. 231/2001.

Principali novità di eIDAS 2.0

eIDAS 2.0 introduce dei nuovi principi rispetto a quanto previsto dal previgente Regolamento nei seguenti ambiti:

- il servizio di **archiviazione elettronica** (denominato *eArchiving*), attraverso il quale ad esempio, le aziende potranno conservare in modo sicuro i documenti sensibili o le comunicazioni interne;
- l'**ampliamento dei servizi fiduciari,** che estende i servizi di conservazione qualificati alle **firme elettroniche**, ai **sigilli elettronici** e ai **documenti archiviati elettronicamente,** autenticando non solo le firme elettroniche, ma anche i documenti archiviati digitalmente; in questo caso, ad esempio, un'azienda potrà utilizzare servizi di conservazione qualificati per garantire l'integrità dei contratti digitali;
- la **verifica della conformità, mediante la quale i** prestatori di servizi fiduciari qualificati saranno sottoposti a verifiche periodiche per garantire il rispetto dei requisiti eIDAS 2.0 e delle misure di gestione dei rischi di cybersicurezza, contribuendo pertanto alla sicurezza delle operazioni aziendali.

L'introduzione dell'European Digital Identity Wallet ("EDIW")

In questo contesto, merita particolare attenzione l'introduzione dell'**European Digital Identity Wallet ("EDIW")** che diventerà istituto obbligatorio nel prossimo

futuro e permetterà ai cittadini degli Stati Membri di utilizzare un sistema di riconoscimento valido su tutto il territorio europeo.

L'EDIW rappresenta una vera e propria identità digitale e costituirà **il portafoglio europeo dei singoli cittadini** all'interno del quale verranno inseriti dati e documenti identificativi personali (come per es. il passaporto, la carta d'identità, le certificazioni rilasciate dalle autorità nazionali ed europee, la patente), divenendo il primo vero circuito unico digitale interconnesso, interoperabile e sicuro.

Per queste ragioni, la normativa eIDAS 2.0 impone **un livello più elevato di trasparenza, di tutela della vita privata e di controllo sui dati personali da parte degli utenti**, sin dalla progettazione del sistema di raccolta delle informazioni, mediante la predisposizione di un'interfaccia comune per l'accesso e la gestione dei portafogli europei di identità digitale**[2]**.

Tale meccanismo permetterà agli utenti di **tracciare tutte le transazioni effettuate** mediante l'uso del portafoglio europeo di identità digitale, individuando le tipologie di dati personali condivisi, i soggetti coinvolti nelle operazioni di trattamento e i metadati inerenti alle attività svolte (es. ora e data della transazione). In base alle indicazioni fornite dalla normativa, le informazioni raccolte nell'ambito di queste transazioni dovrebbero essere conservate anche nell'eventualità in cui l'operazione non venga conclusa**[3]**.

Pur individuando nell'interoperabilità e nell'interconnessione dei sistemi gli obiettivi principali della disciplina, il Regolamento eIDAS 2.0 mantiene la visione antropocentrica fissata dal programma strategico per il decennio digitale 2030**[4]** e sottolinea la necessità di rispettare i diritti per la protezione dei dati personali, con particolare riferimento allo sviluppo di un sistema che consenta agli utenti di controllare le proprie informazioni e di chiedere la cancellazione dei dati personali dai portafogli.

Impatti di eIDAS 2.0 sulla sicurezza informatica

Tra gli ambiti indicati dal sopra citato Considerando 10, particolare enfasi è posta alla esigenza che i sistemi di identificazione e autenticazione forniscano **un elevato livello di garanzia in termini di sicurezza informatica**, onde contenere i tipici rischi legati agli ambienti digitali e on-line.

Questa esigenza trova la sua ratio nel fatto che un impianto normativo che mira a creare una interoperabilità dei sistemi pubblici e privati basati sulla certezza dell'identità digitale associata a un utente online, non può prescindere dal garantire la sicurezza che, da un lato, vi sia corrispondenza tra utente e sua identità digitale e, dall'altro, la tecnologia utilizzata sia tale da ridurre il più possibile gli incidenti informatici basati sulla cd. sicurezza delle identità e, conseguentemente, alle connesse frodi legate al furto di tale identità.

La circostanza da ultimo evidenziata emerge anche dall'ultimo Rapporto Clusit 2024 nel quale si dà atto che la "**identificazione del sottoscrittore con SPID o CIE e con firma digitale con OTP sono misure robuste che riducono le possibilità di azione dei truffatori e tutelano gli utenti e le aziende.** Tuttavia, permangono situazioni in cui i truffatori riescono ad aggirare, in modo artificioso, i controlli e i sistemi informativi, cagionando danni a cittadini ignari, che devono tutelarsi tramite denuncia per furto di identità."**[5]**.

Tenendo presente questo scenario, si deve quindi leggere la decisione del legislatore europeo di inserire nel Considerando 50 le tipologie di presidi che i prestatori di servizi fiduciari sono tenuti ad adottare al fine di far fronte a "*guasti del sistema, errori umani, azioni malevole o fenomeni naturali, per gestire i rischi posti alla sicurezza dei sistemi informativi e di rete che tali prestatori utilizzano nella prestazione dei loro servizi, nonché per notificare minacce informatiche e incidenti significativi conformemente alla medesima direttiva. Per quanto riguarda la segnalazione di incidenti, i prestatori di servizi fiduciari dovrebbero notificare eventuali incidenti che abbiano un impatto significativo sulla prestazione dei loro servizi, compresi quelli causati dal furto o dalla perdita di*

dispositivi o da danni ai cavi di rete, o quelli verificatisi nel contesto dell'identificazione di persone" **[6]**.

Questi presidi devono considerarsi integrativi rispetto a quelli fissati dalla Direttiva (UE) 2022/2555 (cd. "**Direttiva Nis 2**") che, all'art. 3, include i prestatori di servizi fiduciari tra i soggetti essenziali di cui all'Allegato 1.

Gli obblighi in materia di cyber sicurezza definiti nella NIS 2 "*dovrebbero essere considerati complementari ai requisiti imposti ai prestatori di servizi fiduciari*". Per questo, il legislatore europeo ritiene opportuno che i prestatori di servizi fiduciari "*adottino tutte le misure adeguate e proporzionate per gestire i rischi posti ai loro servizi, anche in relazione ai clienti e ai terzi che vi fanno affidamento",* nonché segnalino gli incidenti in base alle disposizioni della Direttiva NIS 2. Tali obblighi in materia di cyber sicurezza e segnalazione dovrebbero riguardare anche la protezione fisica dei servizi forniti**[7]**.

Riguardo la segnalazione di eventi accidentali o malevoli, i prestatori di servizi fiduciari dovranno preoccuparsi di definire un processo di analisi e di eventuale notifica degli incidenti atti a provocare un impatto significativo sulla prestazione dei servizi, "*compresi quelli causati dal furto o dalla perdita di dispositivi o da danni ai cavi di rete, o quelli verificatisi nel contesto dell'identificazione di persone*"**[8]**.

eIDAS 2.0 e la protezione dei dati personali

Rispetto all'attuale contesto normativo europeo, **il Regolamento eIDAS 2.0 risponde agli obiettivi fissati dal programma strategico per il decennio digitale 2030**, che mira a garantire l'accesso ai servizi digitali pubblici, privati e transfrontalieri tra gli Stati membri, definendo un quadro europeo comune per la creazione di un'identità digitale affidabile.

Il piano decennale promosso dall'Europa si basa su **un meccanismo di cooperazione annuale[9]** che coinvolge la Commissione e gli Stati membri ed è

finalizzato a sostenere un mercato unico digitale interconnesso e interoperabile, che assicuri a ciascun individuo il completo controllo e la sicurezza delle proprie informazioni nei rapporti e nelle operazioni di scambio**[10]**.

La normativa eIDAS 2.0, inoltre, tiene in considerazione quanto esposto all'interno della "dichiarazione europea sui diritti e i principi digitali per il decennio digitale" ("**Dichiarazione**"), proclamata dal Parlamento europeo, dal Consiglio e dalla Commissione il 23 gennaio 2023, nella quale le istituzioni richiamano gli obiettivi principali del modello dell'Unione per la trasformazione digitale della società e dell'economia europea.

Tra questi, la Dichiarazione comprende, in particolare, **il rispetto dei diritti fondamentali, l'accessibilità, la resilienza, la sicurezza dei dati e la disponibilità di servizi[11]**. Al fine di promuovere un ambiente digitale equo, la Dichiarazione evidenzia la necessità di regolamentare le interazioni con gli algoritmi e i sistemi di intelligenza artificiale, assicurando la protezione dei dati e garantendo, nel contempo, il rispetto della vita privata del singolo individuo.

In quest'ottica, **il Considerando 12 dell'eIDAS** chiarisce che la nuova normativa mira a definire delle garanzie specifiche per impedire l'associazione dei dati personali raccolti nell'ambito della prestazione dei servizi con altre informazioni personali derivanti da trattamenti differenti da parte dei fornitori di mezzi di identificazione elettronica e di attestati elettronici.

I nuovi servizi introdotti da eiDAS 2.0

Rispetto alla disciplina precedente, il Regolamento eiDAS 2.0 ha una portata applicativa più ampia e introduce nuovi servizi, specificando ulteriormente l'applicazione dei principi di limitazione delle finalità, di minimizzazione e di protezione dei dati fin dalla progettazione e per impostazione predefinita di cui al Regolamento (UE) 2016/679 ("**GDPR**"), con riferimento alla gestione dei flussi delle informazioni raccolte nel corso delle operazioni d'identificazione elettronica e delle attività di trust service**[12]**.

Portafogli europei di identità digitale: i paletti dell'Edps

Sulla nuova disciplina eIDAS 2.0 e, nello specifico, sulla diffusione dei **portafogli europei di identità digitale**, è intervenuto l'European Data Protection Supervisor ("**EDPS**"), individuando una serie di potenziali criticità che la normativa potrebbe presentare circa il trattamento dei dati personali in un ambiente unico digitale**[13]**.

La creazione di un modello comune e interconnesso del sistema EDIW comporta indubbiamente un rischio di **ammassamento e dispersione dei dati personali** che, secondo l'Autorità di Supervisione europea, potrebbe condurre allo sfruttamento dei dati, fino ad una potenziale illegittima profilazione dell'interessato, dovuta a una raccolta eccedente ed eccessiva rispetto allo scopo originario del trattamento.

Raccolta e gestione dei dati: la necessità di standard pertinenti

È necessario definire degli standard di riferimento pertinenti circa le finalità di raccolta e gestione dei dati, le condizioni e le modalità di trattamento, nonché i soggetti destinatari di tali informazioni all'interno del circuito di scambio.

Una protezione effettiva dei dati sin dalla progettazione

Inoltre, per il presidente dell'EDPS è essenziale che vengano previsti presidi efficaci, atti ad assicurare una protezione effettiva dei dati sin dalla progettazione dell'interfaccia EDIW, poiché l'impiego di misure non adeguate potrebbe contribuire al verificarsi di gravi incidenti di sicurezza, *data breach*, furti di identità e attività illecite di rilevanza penale**[14]**.

Comunicazioni di dati tra le relying parties

Particolare attenzione dovrà essere dedicata alle comunicazioni di dati tra i titolari di portafogli e i fornitori di servizi digitali, le cosiddette *Relying Parties.* È fondamentale che prima del trattamento e delle attività di scambio vengano definiti i compiti, gli obblighi e le responsabilità delle parti operanti nel circuito.

Per l'Autorità, l'analisi preliminare dei rischi e la definizione di standard di sicurezza elevati per la gestione dei portafogli digitali sarà essenziale anche dal punto di vista della cyber sicurezza.

Il processo di adeguamento degli operatori di settore

In questo contesto, il processo di adeguamento che gli operatori di settore saranno chiamati ad affrontare dal punto di vista della protezione dei dati partirà dalla definizione di un modello conforme ai principi di trasparenza, liceità e correttezza, sin dalla progettazione degli scambi e dei flussi informativi.

Individuazione di rischi specifici

Preliminare all'adozione di specifiche misure di sicurezza, sarà l'individuazione di specifici rischi derivanti dalla raccolta e dallo scambio di numerose informazioni personali contenute all'interno dei portafogli europei di identità digitale. La minimizzazione come impostazione predefinita dovrà costituire un elemento centrale dell'interfaccia operativa EDIW.

Definizione dei ruoli e dei soggetti autorizzati ad accedere alle informazioni

Infine, sarà essenziale definire i ruoli e i soggetti autorizzati ad accedere alle informazioni contenute nei portafogli europei d'identità digitale, sensibilizzando tutti gli operatori che entrano in gioco nel processo di raccolta, gestione, condivisione e archiviazione dei dati. Le tecnologie utilizzate per conseguire gli obiettivi fissati dalla normativa dovranno essere sviluppate garantendo sempre

la più ampia accessibilità, utilizzabilità e interoperabilità dei dati all'utente, senza soluzione di continuità**[15]**.

eIDAS e sistema "231"

Ulteriore aspetto di rilevanza ai fini della presente analisi è anche quello degli **impatti dell'eIDAS 2.0 sui prestatori dei servizi fiduciari** in termini di regole di governance e security.

Innovazioni nel campo dei servizi fiduciari e verifiche di conformità

In particolare, stante la presenza tra i reati presupposto della responsabilità amministrativa di cui al D. Lgs. 231/2001 dell'art. 640-*quinquies* del codice penale rubricato "Frode informatica del soggetto che presta servizi di certificazione di firma elettronica" con l'adozione del Regolamento eIDAS 2.0, **le aziende che prestano servizi fiduciari dovranno pertanto adeguarsi ai nuovi standard di sicurezza e interoperabilità** previsti dal regolamento, con i seguenti principali impatti:

- **miglioramento delle misure di sicurezza**: le aziende saranno obbligate a rafforzare le loro misure di sicurezza informatica per proteggere i dati personali e i sistemi di identificazione digitale. L'adozione di tali misure potrà ridurre il rischio di incorrere in reati informatici e, di conseguenza, la responsabilità amministrativa ai sensi del D. Lgs. 231/2001;
- **compliance e formazione**: le imprese dovranno assicurare che il personale sia adeguatamente formato sui nuovi protocolli di sicurezza e sui rischi connessi all'uso dell'identità digitale. Una formazione efficace può prevenire incidenti di sicurezza causati da errori umani o superficialità;
- **internal audit e monitoraggio**: sarà cruciale implementare sistemi di audit ICT e monitoraggio continui per garantire la conformità con eIDAS 2.0 e per individuare tempestivamente eventuali violazioni.

Aggiornamento del Modello 231 e altre attività

Dal punto di vista degli Organismi di Vigilanza, oltre a valutare di richiedere **l'aggiornamento del Modello 231** per gli aspetti in argomento, essi dovranno porre in essere la propria attività mediante:

- incontri con il management interessato;
- effettuando analisi o approfondimenti, direttamente o eventualmente con il supporto di specialisti esterni attivati mediante la disponibilità di spesa riconosciuta agli OdV;
- avvalendosi del supporto delle funzioni di controllo interno (Internal Audit o Compliance, ove presenti);
- ricevendo opportuni flussi informativi dalla funzione ICT (o, nel caso, dall'outsourcer se il servizio viene esternalizzato).

eIDAS 2.0: governance e di gestione della sicurezza informatica

L'implementazione del Regolamento eIDAS 2.0 ha un impatto significativo non solo sui fornitori dei servizi fiduciari ma può costituire un termine di riferimento per tutte le aziende in termini di governance e di gestione della sicurezza informatica poiché l'introduzione di nuovi sistemi di verifica dell'identità digitale costituiscono, di fatto, una tutela potenziata contro le frodi informatiche ai danni di quelle aziende che offrono beni e servizi online.

Infine, in considerazione del fatto che "il modello Organizzativo non può prescindere da un sistema di gestione della sicurezza delle informazioni"**[16]**, il miglioramento del sistema di sicurezza costituisce un obiettivo per tutti gli enti che sono potenzialmente esposti al rischio di cui al D.Lgs. 231/01 e costituisce una buona prassi utilizzare standard di riferimento in materia di gestione dei controlli informatici per costruire un Modello 231 efficace dal punto di vista organizzativo, operativo e tecnologico**[17]**.

Conclusioni

In conclusione, gli OdV dovranno ancora una volta svolgere un ruolo chiave attraverso la vigilanza sui Modelli “231” delle imprese impattate da questa nuova regolamentazione. Sarà quindi sempre più essenziale adottare un approccio multidisciplinare, che combini, in questo caso, competenze legali, aziendalistiche e tecnologiche.

Note

[1] Considerando 10 del Regolamento (UE) 1183/2024.

[2] Si rinvia al Considerando 13 del Regolamento (UE) 1183/2024.

[3] Si rinvia al Considerando 13 del Regolamento (UE) 1183/2024.

[4] Si rinvia alla Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che istituisce il programma strategico per il decennio digitale 2030 (GU L 323 del 19.12.2022, pag. 4).

[5] Si rinvia al paragrafo “Analisi dei principali cyber attacchi noti del 2023 a livello globale”, contenuto nel Rapporto sulla sicurezza ICT in Italia, Clusit, 2024, pag. 78.

[6] Considerando 50 del Regolamento (UE) 1183/2024.

[7] Si rinvia al Considerando 94 della direttiva (UE) 2022/2555.

[8] Considerando 50 **del Regolamento (UE) 1183/2024.**

[9] Si rinvia al comunicato online sul “Programma strategico per il decennio digitale”, pubblicato sul sito della Commissione europea.

[10] Si richiamano i primi 5 Considerando del Regolamento (UE) 2024/1183 del Parlamento Europeo e del Consiglio dell’11 aprile 2024 che modifica il

Regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

[11] Si veda il Preambolo della "*Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*", proclamata dal Parlamento europeo, dal Consiglio e dalla Commissione in data 23 gennaio 2023.

[12] Si rinvia al Considerando 12 del Regolamento (UE) 1183/2024.

[13] Si rinvia al documento "Where are we heading with digital identities?" Cybersecurity Standardisation Conference 2023, European Standardisation in support of the EU cybersecurity legislation, intervento di Wojciech Wiewiórowski European Data Protection Supervisor, 7 febbraio 2023.

[14] Si rinvia al documento "*Where are we heading with digital identities?*" *Cybersecurity Standardisation Conference 2023, European Standardisation in support of the EU cybersecurity legislation*, intervento di Wojciech Wiewiórowski European Data protection Supervisor, 7 febbraio 2023.

[15] Si richiamano i principi fissati al Considerando 15 del Regolamento (UE) 1183/2024 ("eIDAS 2.0").

[16] F. Di Maio, Prevenzione e dissuasione dei reati nel modello organizzativo, p. 153 in A. Monti, Cybercrime e responsabilità da reato degli enti, 2022.

[17] AODV231, La prevenzione dei reati informatici: rischi 231, data protection e misure di compliance, giugno 2023.