FIVERS

Aggiornamento
Data protection, AI, IT and IP

n. 16 / 2024

DATA PROTECTION.

10 Dicembre 2024 – Garante privacy: via libera al Codice di condotta per i produttori di software gestionali.

---

4 Dicembre 2024 – Consiglio UE: raggiunta la posizione comune sulla proposta di Regolamento FiDA (*Financial Data Access*) per standardizzare la condivisione dei dati finanziari, proteggere i segreti commerciali e regolamentare il consenso.

---

4 Dicembre 2024 – Il Comitato europeo per la protezione dei dati personali (EDPB) adotta una dichiarazione sulla necessità di coerenza della legislazione digitale con il GDPR.

INTELLIGENZA ARTIFICIALE.

10 Dicembre 2024 – EuroHPC ha selezionato sette consorzi per istituire e gestire le prime fabbriche di intelligenza artificiale in tutta Europa.

---

10 Dicembre 2024 – Seconda riunione plenaria dell'Ufficio per l'Intelligenza Artificiale della Commissione UE.

---

8 Dicembre 2024 – In vigore la Direttiva UE 2853/2024 sulla responsabilità per danno da prodotti difettosi. Novità in materia di prova e nesso di causalità del danno da sistemi di Intelligenza Artificiale.

MERCATI DIGITALI

10 Dicembre 2024 – In vigore il Cyber Resilience Act (CRA) dell'Unione Europea.

---

4 Dicembre 2024 - Commissione europea: in dirittura d'arrivo il pacchetto legislativo ViDA (*VAT in the Digital Age)* relativo all'IVA digitale.

---

2 Dicembre 2024 – Pubblicato nella Gazzetta Ufficiale dell'Unione Europea il Regolamento di esecuzione (UE) 2024/2956 che stabilisce norme tecniche di attuazione per l'applicazione del Regolamento (UE) 2022/2554 (DORA) per quanto riguarda i modelli standard in relazione al registro delle informazioni degli accordi contrattuali con i fornitori terzi di servizi TIC.

INFORMATION TECHNOLOGY

6 Dicembre 2024 – Agenzia Nazionale per la Cybersicurezza: rilasciati video tutorial dedicati a imprenditori, dipendenti e fornitori delle PMI per favorire una migliore consapevolezza del rischio cyber.

---

3 Dicembre 2024 – Agenzia europea per la cybersicurezza (ENISA): pubblicata la prima relazione in assoluto sullo stato della cybersicurezza in UE.

PROPRIETA' INTELLETTUALE E INDUSTRIALE

8 Dicembre 2024 – In vigore parte del "*Design Package*" della UE, con le nuove norme aggiornate per la protezione giuridica dei disegni e dei modelli.

DATA PROTECTION

10 Dicembre 2024 – Garante privacy: via libera al Codice di condotta per i produttori di software gestionali.

Il Garante Privacy ha dato il via libera al Codice di condotta di Assosoftware, Associazione italiana dei produttori di software in Italia, che riguarda il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione dei software gestionali (SWH).

Tali software, destinati ad aziende, associazioni, professionisti e pubblica amministrazione, vengono utilizzati per l'assolvimento degli obblighi fiscali e previdenziali, assistenziali e gestionali, la redazione dei bilanci, la gestione del personale e gli adempimenti societari, con un impatto dunque notevole sugli aspetti relativi alla protezione dei dati personali.

In particolare, consentono l'automazione dei processi interni delle imprese relativi alla gestione delle fatturazioni, dei rapporti con i clienti, mentre per i professionisti, la gestione delle attività di contabilità, tributarie, lavoristiche, legali.

In considerazione della delicatezza dei dati trattati, il Codice si propone di definire una serie di regole e di misure tecniche ed organizzative affinché i software prodotti e resi disponibili sul mercato dalle imprese aderenti ad Assosoftware siano sviluppati nel rispetto dei principi di protezione dei dati fin dalla progettazione (by design) e per impostazione predefinita (by default).

Ciò al fine di favorire il rispetto del GDPR e di rendere disponibili ai clienti idonei strumenti per adempiere agli obblighi di protezione dei dati riguardo ai trattamenti svolti tramite i software.

Oltre ad approvare il Codice di condotta, l'Autorità ha anche accreditato il relativo Organismo di monitoraggio, composto da esperti nel settore dell'ICT, con particolare riferimento ai profili di protezione dei dati personali.

---

4 Dicembre 2024 – Consiglio UE: raggiunta la posizione comune sulla proposta di Regolamento FiDA (Financial Data Access) per standardizzare la condivisione dei dati finanziari, proteggere i segreti commerciali e regolamentare il consenso.

Il Consiglio dell'Unione Europea ha raggiunto un accordo sulla proposta di Regolamento relativo a un quadro per l'accesso ai dati finanziari (FiDA) presentata dalla Commissione europea nel giugno 2023.

Il Regolamento FIDA stabilisce regole armonizzate sull'accesso, la condivisione e l'uso di determinate categorie di dati (sia personali che non personali) dei clienti nei servizi finanziari. Inoltre, il Regolamento FIDA limita l'ambito di applicazione della condivisione dei dati ai dati grezzi provenienti dalle normali interazioni commerciali, escludendo i dati commerciali riservati e i segreti commerciali. Stabilisce inoltre un periodo di limitazione della conservazione dei dati e impone modalità chiare e non fuorvianti per l'acquisizione presso il cliente del consenso alla condivisione dei dati.

Vengono inoltre introdotte anche modifiche al Regolamento 2022/1925 (Legge sui Mercati Digitali – DMA) per vietare ai *gatekeeper* di combinare i dati dei clienti dei servizi per altri scopi e impongono ai fornitori di servizi di informazione finanziaria di paesi terzi (FISP) di nominare un rappresentante stabilito nella UE.

---

4 Dicembre 2024 – Il Comitato europeo per la protezione dei dati personali (EDPB) adotta una dichiarazione sulla necessità di coerenza della legislazione digitale con il GDPR.

Il Comitato europeo per la protezione dei dati (EDPB) ha adottato **una dichiarazione sulla seconda relazione della Commissione europea sull'applicazione del Regolamento generale sulla protezione dei dati (GDPR)** ricordando la fondamentale importanza della certezza del diritto e della coerenza della legislazione digitale – oramai ampia e articolata - con il GDPR. In tale prospettiva il Comitato ricorda – ad

esempio - le sue iniziative in corso per chiarire l'interazione tra l'applicazione del GDPR e la legge sull'IA (Regolamento 2024/1689), la strategia dell'UE in materia di dati (Regolamento 2022/868) e il pacchetto sui servizi digitali (Regolamento 2022/2065 – DSA e Regolamento 2022/1925 – DMA).

Infine, l'EDPB ha annunciato che intensificherà la produzione di contenuti per i non esperti, le piccole e medie imprese (PMI) e altri gruppi.

---

4 Dicembre 2024 – Il Comitato europeo per la protezione dei dati personali (EDPB) chiarisce le norme per la condivisione dei dati con le autorità dei paesi terzi e approva la certificazione del sigillo di protezione dei dati dell'UE.

Durante la sua ultima sessione plenaria, il Comitato europeo per la protezione dei dati (EDPB) ha pubblicato **le linee guida sull'articolo 48 del GDPR** sui trasferimenti di dati alle autorità di paesi terzi e ha approvato un nuovo sigillo europeo per la protezione dei dati.

In un mondo altamente interconnesso, le organizzazioni ricevono richieste da parte delle autorità pubbliche di altri paesi per condividere i dati personali. La condivisione dei dati può, ad esempio, essere utile per raccogliere prove in caso di reato, per controllare le transazioni finanziarie o per approvare nuovi farmaci.

Quando un'organizzazione europea riceve una richiesta di trasferimento di dati da un'autorità di un "paese terzo" (ossia di paesi non europei), deve rispettare il Regolamento generale sulla protezione dei dati (GDPR). Nelle sue linee guida, l'EDPB si concentra sull'articolo 48 del GDPR e chiarisce in che modo le organizzazioni possono valutare al meglio le condizioni in cui possono rispondere legalmente a tali richieste. In questo modo, le linee guida aiutano le organizzazioni a prendere una decisione in merito alla possibilità di trasferire legalmente i dati personali alle autorità di paesi terzi quando richiesto.

Le sentenze o le decisioni delle autorità di paesi terzi non possono essere automaticamente riconosciute o eseguite in Europa. Se un'organizzazione risponde a una richiesta di dati personali da parte di un'autorità di un paese terzo, questo flusso di dati costituisce un trasferimento e si applica il GDPR. Un accordo internazionale può prevedere sia una base giuridica che un motivo di trasferimento. Nel caso in cui non esista un accordo internazionale o se l'accordo non preveda una base giuridica o garanzie adeguate, potrebbero essere prese in considerazione, in circostanze eccezionali e caso per caso, altre basi giuridiche o altri motivi per il trasferimento.

Gli orientamenti sono oggetto di consultazione pubblica fino al 27 gennaio 2025.

Nel corso della riunione plenaria, il Comitato ha inoltre adottato un parere che approva i criteri di certificazione della *Brand Compliance* relativi alle attività di trattamento da parte di titolari o responsabili del trattamento. Nel settembre 2023, il Consiglio ha già adottato un parere sull'approvazione dei criteri di certificazione nazionali di *Brand Compliance*. L'approvazione del nuovo parere significa che questi criteri saranno ora applicabili in tutta Europa e come sigillo europeo per la protezione dei dati.

La certificazione GDPR aiuta le organizzazioni a dimostrare la loro conformità alla legge sulla protezione dei dati.

INTELLIGENZA ARTIFICIALE.

10 Dicembre 2024 – EuroHPC ha selezionato sette consorzi per istituire e gestire le prime fabbriche di intelligenza artificiale in tutta Europa.

L'impresa comune europea per il calcolo ad alte prestazioni (EuroHPC) ha selezionato sette proposte per istituire e gestire le prime fabbriche di intelligenza artificiale in tutta Europa. Si tratta di una pietra miliare per l'Europa nella costruzione di un ecosistema per addestrare modelli di IA avanzati e sviluppare soluzioni di IA.
Con un investimento di 1,5 miliardi di euro, le fabbriche di intelligenza artificiale selezionate coinvolgono 15 Stati Membri r saranno ospitate presso i principali hub di ricerca e tecnologia in tutta Europa, precisamente nelle seguenti città:

Barcellona, Spagna: "BSC AIF" presso il Centro di Supercalcolo di Barcellona
Bologna, Italy: “IT4LIA” at CINECA - Bologna Tecnopolo
Kajaani, Finlandia: "LUMI AIF" e CSC
Bissen, Lussemburgo: "Meluxina-AI" e LuxProvide
Linköping, Svezia: "MIMER" all'Università di Linköping
Stoccarda, Germania: "HammerHAI" all'Università di Stoccarda
Atene, Grecia: "Pharos" al GRNET

Le sette fabbriche di intelligenza artificiale coinvolgono 15 Stati membri e due Stati partecipanti a EuroHPC. Portogallo, Romania e Turchia hanno aderito al BSC AIF; L'Austria e la Slovenia hanno aderito alla ITA4LIA; e Cechia, Danimarca, Estonia, Norvegia e Polonia hanno aderito al FIA UMI.

In cinque dei siti selezionati (Finlandia, Germania, Italia, Lussemburgo e Svezia) si svilupperanno nuovi supercomputer ottimizzati per l'intelligenza artificiale. Le fabbriche di intelligenza artificiale in Spagna e Finlandia saranno inoltre dotate di una piattaforma sperimentale, che fornirà un'infrastruttura all'avanguardia per lo sviluppo e il test di modelli e applicazioni innovative di intelligenza artificiale.

Le fabbriche di intelligenza artificiale raddoppieranno la capacità di calcolo di EuroHPC, rispondendo a esigenze specifiche e potenziando le capacità europee in materia di intelligenza artificiale.

---

10 Dicembre 2024 – Seconda riunione plenaria dell’Ufficio per l’Intelligenza Artificiale della Commissione UE.

L’Ufficio per l’IA è un organismo creato dal Regolamento UE 2024/1689 *(AI Act)* ed ha la specifica funzione di supportare la Commissione UE. Nella sua seconda sessione plenaria sono stati affrontati rilevanti argomenti, tra cui:

- le iniziative di Austria e Norvegia in materia di 'alfabetizzazione in materia di IA;
- le misure nazionali sulla *governance* dell'IA introdotte da Malta, Finlandia e Slovenia;
- la visione strategica per l'IA della nuova Commissione UE;
- aggiornamenti sulle attività internazionali, tra cui: (a) la collaborazione tra Unione Europea e Singapore; (b) la presentazione del rapporto sugli esiti del vertice ministeriale dell'OCSE sul partenariato globale sull'IA; (c) la presentazione del quadro di gestione dei rischi che il Comitato sull'IA del Consiglio d'Europa ha di recente adottato;
- aggiornamento sullo stato dei lavori per l’adozione del codice di buone pratiche per l'IA per uso generale;
- discussione sulle linee guida per le pratiche vietate di IA e sulle definizioni dei sistemi;
- piano d’azione per il 2025.

---

8 Dicembre 2024 – In vigore la Direttiva UE 2853/2024 sulla responsabilità per danno da prodotti difettosi. Novità in materia di prova e nesso di causalità del danno da sistemi di Intelligenza Artificiale.

L'8 dicembre 2024 è entrata in vigore la direttiva del Parlamento europeo e del Consiglio sulla responsabilità per danno da prodotti difettosi e che abroga la direttiva 85/374/CEE del Consiglio (direttiva sulla responsabilità per danno da prodotti difettosi).

La Direttiva è importante soprattutto perché aggiorna le norme sulla responsabilità all’era digitale e introduce le disposizioni sulla responsabilità per danno da Intelligenza artificiale.

Illuminante quanto previsto dal Considerando 13 della Direttiva:

(13) I prodotti nell’era digitale possono essere tangibili o intangibili. Sul mercato è sempre più diffuso il software, come i sistemi operativi, il firmware, i programmi per computer, le applicazioni o i sistemi di IA, e la sua importanza a fini di sicurezza dei prodotti è sempre maggiore. Il software può essere immesso

sul mercato come prodotto a sé stante o può essere poi integrato in altri prodotti come componente e può causare danni dovuti al suo funzionamento. Per garantire la certezza del diritto è opportuno chiarire nella presente direttiva che, ai fini dell'applicazione della responsabilità oggettiva, il software è un prodotto, a prescindere dalle modalità con cui viene fornito o usato, e quindi dal fatto che il software sia integrato in un dispositivo, utilizzato tramite una rete di comunicazione o tecnologie cloud oppure sia fornito attraverso un modello software-as-a-service. Le informazioni, invece, non devono invece essere considerate un prodotto e le norme sulla responsabilità per danno da prodotti difettosi non dovrebbero pertanto applicarsi al contenuto dei file digitali, quali file multimediali, e-book o il mero codice sorgente dei software. Il produttore o lo sviluppatore di software, compreso il fornitore di sistemi di IA ai sensi del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio (5), dovrebbe essere considerato un fabbricante.

Dunque, uno sviluppatore o un produttore di software, compresi i sistemi di intelligenza artificiale (IA) ai sensi del Regolamento 2024/1689 (AI Act) sono considerati "fabbricanti", come meglio dall'articolo 4, paragrafo 10, della direttiva:

"fabbricante»: *qualsiasi persona fisica o giuridica che: (a) sviluppa, produce o fabbrica un prodotto; (b) fa progettare o fabbricare un prodotto o che, apponendo il proprio nome, marchio o altre caratteristiche distintive su tale prodotto, si presenta come fabbricante; o (c) sviluppa, produce o fabbrica un prodotto per uso proprio.*

La direttiva sulla responsabilità per danno da prodotti difettosi stabilisce inoltre che, poiché i prodotti possono essere progettati in modo da consentire di apportare modifiche al software, compresi gli aggiornamenti, gli stessi principi si applicano alle modifiche apportate. Di conseguenza, quando una modifica sostanziale è apportata mediante un aggiornamento del software o un aggiornamento dovuto all'apprendimento continuo di un sistema di IA, il prodotto sostanzialmente modificato è considerato messo a disposizione sul mercato o messo in servizio al momento della modifica.

Fondamentali le norme processuali in materia di prova del danno e del nesso di causalità, prova spesso quasi impossibile da fornirsi ad opera del danneggiato, soprattutto in caso di danno creato da sistemi di IA, a causa del cosiddetto effetto di "scatola nera" dell'algoritmo.

Gli potranno dunque presumere il carattere difettoso di un prodotto o il nesso di causalità tra danno e difetto, o entrambi, nel caso in cui, sebbene il fabbricante convenuto abbia divulgato le informazioni pertinenti, risulti eccessivamente difficile per il danneggiato-attore, in particolare a causa della complessità tecnica e scientifica del caso, provare il carattere difettoso del prodotto o l'esistenza del nesso di causalità, o entrambi. Di conseguenza, peer non compromettere il diritto al risarcimento e considerato che i fabbricanti dispongono di conoscenze specialistiche e di migliori informazioni rispetto al danneggiato e al fine di garantire una giusta ripartizione dei rischi evitando l'inversione dell'onere della prova, qualora le sue difficoltà riguardino la prova del carattere difettoso del prodotto l'attore sarà tenuto a dimostrare soltanto che è probabile che il prodotto fosse difettoso o, qualora le sue difficoltà riguardino la prova del nesso di causalità, soltanto che il carattere difettoso del prodotto è una probabile causa del danno. La complessità tecnica o scientifica sarà determinata dagli organi giurisdizionali nazionali caso per caso, tenendo conto di diversi fattori: dalla natura complessa del prodotto, come nel caso di un dispositivo medico innovativo alla natura complessa della tecnologia impiegata, ad esempio l'apprendimento automatico; dalla natura complessa delle informazioni e dei dati che deve analizzare l'attore alla natura complessa del nesso di causalità, ad esempio tra un prodotto farmaceutico o alimentare e il manifestarsi di una patologia, oppure un nesso per la cui prova l'attore sia tenuto a spiegare il funzionamento interno di un sistema di IA. L'attore dovrà fornire argomentazioni per dimostrare l'esistenza delle sopra citate difficoltà eccessive, ma non sarà tenuto a fornire elementi di prova riguardo a tali difficoltà. Ad esempio, in un'azione avente ad oggetto un sistema di IA, affinché l'organo giurisdizionale possa accertare l'esistenza di difficoltà eccessive, l'attore non sarà tenuto a spiegare le caratteristiche specifiche di tale sistema di IA o il modo in cui tali caratteristiche complicano la prova del nesso di causalità. Il convenuto – invece – avrà comunque la possibilità di contestare tutti gli elementi dell'azione, tra cui l'esistenza di difficoltà eccessive.

MERCATI DIGITALI

10 Dicembre 2024 – In vigore il Cyber Resilience Act (CRA) dell'Unione Europea.

Il 10 dicembre 2024 è entrato in vigore il *Cyber Resilience Act* (Regolamento UE 2024/2847 relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali) che ha introdotto requisiti obbligatori di sicurezza informatica per i prodotti hardware e software con elementi digitali.

Il Regolamento sarà applicabile a partire dall'11 dicembre 2027, ad eccezione degli obblighi di comunicazione dei produttori che si applicheranno a partire dall'11 settembre 2026.

La nuova normativa stabilisce che i prodotti con elementi digitali devono soddisfare diversi requisiti per garantire la loro sicurezza informatica e per essere immessi sul mercato, tra cui:

- requisiti di sicurezza relativi alle proprietà di tali prodotti, compreso il fatto che la progettazione, lo sviluppo e la produzione del prodotto devono essere effettuati in modo tale da garantire un livello adeguato di cybersicurezza, con approccio basato sul rischio; e
- requisiti di gestione delle vulnerabilità, come l'individuazione e la documentazione delle vulnerabilità, nonché l'attuazione di test, politiche e misure per facilitare la condivisione delle informazioni.

Inoltre, Il CRA chiarisce – all'articolo 7 - quali prodotti si qualificano come «*prodotti con elementi digitali importanti*» e quali requisiti aggiuntivi devono essere soddisfatti. Sono inoltre previste disposizioni di coordinamento e armonizzazione specifiche con il Regolamento 2024/1689 sull'intelligenza artificiale per i sistemi di intelligenza artificiale (IA) ad alto rischio.

La legge chiarisce gli obblighi imposti ai produttori, che includono:

- garantire il rispetto dei requisiti essenziali per i loro prodotti al momento dell'immissione sul mercato, in particolare effettuando valutazioni della conformità;
- effettuare una valutazione dei rischi per la cybersicurezza e includerla nella documentazione tecnica;
- effettuare una specifica *due diligence* sui componenti provenienti da terzi;
- attuare politiche e procedure adeguate, comprese politiche coordinate di divulgazione delle vulnerabilità;
- garantire che i prodotti rimangano conformi e adottare misure correttive in caso di disallineamento dalla conformità; e
- fornire agli utenti complete informazioni e istruzioni.

Il produttore deve, senza indebito ritardo e in ogni caso entro 24 ore dal momento in cui ne viene a conoscenza, notificare al *Computer Security Incident Response Team* (CSIRT) e all'Agenzia dell'Unione europea per la cibersicurezza (ENISA) qualsiasi vulnerabilità attivamente sfruttata rispetto al prodotto con elementi digitali, notificando altresì qualsiasi impatto sulla sicurezza per gli utenti. La notifica dell'incidente deve essere inviata entro 72 ore dal momento in cui si viene a conoscenza dell'incidente. Il CRA consente inoltre la notifica volontaria di eventuali vulnerabilità o minacce informatiche che potrebbero influire sul profilo di rischio di un prodotto. L'ENISA ha il mandato di istituire una piattaforma unica di comunicazione.

Per quanto riguarda gli utenti, i produttori devono informarli, senza indebito ritardo e dopo averne preso conoscenza, in merito a qualsiasi incidente e, se necessario, in merito alle misure correttive che gli utenti possono attuare per attenuare l'impatto dell'incidente.

Le sanzioni previste possono arrivare fino a 15 milioni di euro o, per le imprese, fino al 2,5 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

---

4 Dicembre 2024 - Commissione europea: in dirittura d'arrivo il pacchetto legislativo ViDA (*VAT in the Digital Age)* relativo all'IVA digitale.

Con l'adozione e la promozione della digitalizzazione, il pacchetto ViDA rende il sistema dell'IVA dell'UE più propizio alle imprese e più resiliente alle frodi. Le nuove norme segnano inoltre il primo passo per

affrontare le sfide derivanti dall'economia delle piattaforme e contribuisce a creare la parità di condizioni tra i servizi ricettivi a breve termine e i servizi di trasporto online e tradizionali.

Il pacchetto introduce 3 misure:

1. Il nuovo sistema introduce la comunicazione digitale uniforme in tempo reale ai fini dell'IVA basata sulla fatturazione elettronica per le operazioni transfrontaliere, che fornirà tempestivamente agli Stati membri le informazioni preziose di cui hanno bisogno per intensificare la lotta contro le frodi dell'IVA. La fatturazione elettronica accelererà ulteriormente la trasformazione delle imprese nell'era digitale attraverso la semplificazione delle operazioni, garantendo la conformità e la sicurezza, consentendo un processo decisionale basato sui dati e sostenendo la scalabilità per la crescita e l'innovazione future.

2. Gli operatori dell'economia delle piattaforme nel settore dei servizi di trasporto di passeggeri e dei servizi ricettivi a breve termine diventeranno inoltre responsabili della riscossione dell'IVA e del versamento dell'imposta alle autorità fiscali, se il fornitore indiretto non applica l'IVA. La misura contribuirà a migliorare la parità di condizioni fra i servizi online e tradizionali e agevolerà le attività per gli operatori indiretti che non saranno responsabili dell'IVA.

3. L'iniziativa ridurrà infine l'esigenza di registrarsi più volte nei diversi Stati membri, attraverso l'espansione del modello già esistente di "sportello unico per l'IVA" già in essere per le imprese commerciali.

---

2 Dicembre 2024 – Pubblicato nella Gazzetta Ufficiale dell'Unione Europea il Regolamento di esecuzione (UE) 2024/2956 che stabilisce norme tecniche di attuazione per l'applicazione del Regolamento (UE) 2022/2554 (DORA) per quanto riguarda i modelli standard in relazione al registro delle informazioni degli accordi contrattuali con i fornitori terzi di servizi TIC.

Il Regolamento di esecuzione (UE) 2024/2956 della Commissione UE – applicabile a partire dal prossimo 22 Dicembre 2024 - introduce i modelli standard in relazione al registro delle informazioni sui contratti con fornitori terzi di servizi di tecnologie dell'informazione e della comunicazione (TIC).

L'articolo 28, comma 3, del Regolamento DORA prescrive alle entità finanziarie l'obbligo di mantenere un registro dettagliato di tutti gli accordi contrattuali con fornitori terzi di servizi TIC che rientrano nel perimetro di gestione dei rischi emergenti rappresentati da specifici fornitori di servizi ICT a supporto dei processi commerciali e dei servizi finanziari resi dalle entità finanziarie (banche, assicurazioni, intermediari, etc). Questo registro deve includere informazioni specifiche sui contratti, come la durata, i servizi forniti e le misure di sicurezza adottate.

Il regolamento di esecuzione introduce dunque modelli standard per la registrazione delle informazioni, garantendo uniformità e coerenza nella raccolta e nella gestione dei dati. Questi modelli aiutano a facilitare la supervisione e la gestione dei rischi informatici rappresentati da fornitori terzi di servizi TIC. Le informazioni raccolte nel registro sono essenziali per la gestione interna dei rischi informatici delle entità finanziarie e per l'efficace vigilanza da parte delle autorità competenti. Le autorità di vigilanza europee (EBA, EIOPA, ESMA) utilizzeranno queste informazioni per i propri compiti di ispezione e monitoraggio e per designare i fornitori terzi *critici* di servizi TIC, designazione che sarà appunto basata sulle informazioni raccolte nei registri da parte delle entità finanziarie.

Per ridurre i costi amministrativi, i gruppi finanziari possono mantenere un registro unico delle informazioni su base sub consolidata e consolidata, purché sia consentito a ciascuna entità finanziaria di adempiere agli obblighi di mantenimento e aggiornamento delle informazioni.

INFORMATION TECHNOLOGY

6 Dicembre 2024 – Agenzia Nazionale per la Cybersicurezza (ACN): rilasciati video tutorial dedicati a imprenditori, dipendenti e fornitori delle PMI per favorire una migliore consapevolezza del rischio cyber.

L'ACN ha realizzato tre video tutorial per favorire una migliore consapevolezza del rischio cibernetico. I tutorial si rivolgono a tre distinte categorie di utenti: imprenditori, dirigenti e impiegati, e sono incentrati sulla valorizzazione della cybersicurezza nella programmazione strategica aziendale. Forniscono inoltre suggerimenti per aumentare la consapevolezza dei dipendenti; aiutare consulenti e fornitori a interfacciarsi in maniera sicura ed efficace con le piccole e medie imprese.

I tutorial sono stati espressamente concepiti come elemento della campagna "*Accendiamo la cybersicurezza. Proteggiamo le nostre imprese*" dedicata alle piccole e medie imprese (PMI) e hanno l'obiettivo di informare gli operatori economici e i loro clienti dell'importanza di essere preparati per affrontare i rischi cibernetici, riducendo l'esposizione alle minacce informatiche e mitigando gli impatti di eventuali attacchi cyber.

La campagna attua la misura #71 della Strategia Nazionale per la Cybersicurezza 2022 – 2026 sulla "*Promozione della cultura della sicurezza cibernetica*" I link di riferimento sono riportati di seguito: (i) consigli di ACN per le PMI (ii) video tutorial della campagna "Accediamo la cybersicurezza. Proteggiamo le nostre imprese."

---

3 Dicembre 2024 – Agenzia europea per la cybersicurezza (ENISA): pubblicata la prima relazione in assoluto sullo stato della cybersicurezza in UE.

A norma dell'articolo 18 della direttiva NIS 2, l'ENISA ha reso pubblica la prima relazione biennale sullo stato della cybersicurezza nell'Unione europea.

La relazione fornisce una panoramica basata sull'esame di dati concreti dello stato della cybersicurezza europea e una valutazione delle capacità di cybersicurezza in tutta Europa. La relazione contiene anche raccomandazioni strategiche per affrontare le carenze individuate e aumentare il livello di cibersicurezza nell'UE.

Il rapporto identifica quattro aree prioritarie: 1) attuazione delle politiche, 2) gestione delle crisi informatiche, 3) catena di approvvigionamento e 4) competenze e in questo quadro fornisce sei raccomandazioni politiche:

- Rafforzare il sostegno tecnico e finanziario fornito alle istituzioni, agli organi e alle agenzie dell'Unione europea (istituzioni, organi e organismi dell'Unione europea) e alle autorità nazionali competenti e ai soggetti che rientrano nell'ambito di applicazione della direttiva NIS 2 per **garantire un'attuazione armonizzata, globale, tempestiva e coerente dell'evoluzione del quadro strategico dell'UE in materia di cibersicurezza** utilizzando strutture già esistenti a livello dell'UE come il gruppo di cooperazione NIS; Rete di CSIRT e Agenzie dell'UE.
- Come richiesto dal Consiglio, **rivedere il piano dell'UE per una risposta coordinata agli incidenti informatici su larga scala,** tenendo conto di tutti i più recenti sviluppi della politica dell'UE in materia di cibersicurezza. Il piano dell'UE riveduto dovrebbe **promuovere ulteriormente l'armonizzazione e l'ottimizzazione della cibersicurezza dell'UE, nonché rafforzare le capacità di cibersicurezza sia nazionali che dell'UE** per aumentare la resilienza della cibersicurezza a livello nazionale ed europeo.
- **Rafforzare la forza lavoro cibernetica dell'UE** attraverso l'attuazione **dell'Accademia delle competenze in materia di cibersicurezza** e in particolare definendo un **approccio comune dell'UE alla formazione in materia di cibersicurezza**, individuando le future esigenze in materia di competenze, sviluppando un **approccio coordinato dell'UE al coinvolgimento dei portatori di interessi** per colmare il **divario di competenze in materia di competenze** e istituendo un **sistema europeo di attestazione delle competenze in materia di cibersicurezza.**

- Affrontare il problema della sicurezza della catena di approvvigionamento nell'UE **intensificando le valutazioni coordinate dei rischi a livello dell'UE** e **lo sviluppo di un quadro strategico orizzontale dell'UE per la sicurezza della catena di approvvigionamento** volto ad affrontare le sfide in materia di cibersicurezza affrontate sia dal settore pubblico che da quello privato.
- **Migliorare la comprensione delle specificità e delle esigenze settoriali, migliorare il livello di maturità della cibersicurezza dei settori contemplati dalla direttiva NIS2 e utilizzare il futuro meccanismo di emergenza per la cibersicurezza da istituire a norma della legge sulla solidarietà informatica** per la preparazione e la resilienza settoriali, con particolare attenzione ai settori deboli o sensibili e ai rischi individuati attraverso valutazioni dei rischi a livello dell'UE.
- Promuovere un **approccio unificato** basandosi sulle iniziative politiche esistenti e armonizzando gli sforzi nazionali per raggiungere un **elevato livello comune di consapevolezza in materia di cibersicurezza e igiene informatica tra i professionisti e i cittadini,** indipendentemente dalle caratteristiche demografiche.

PROPRIETA' INTELLETTUALE E INDUSTRIALE

8 Dicembre 2024 – In vigore parte del "*Design Package*" della UE, con le nuove norme aggiornate per la protezione giuridica dei disegni e dei modelli.

Sono entrati in vigore l'8 Dicembre 2024 i due atti normativi del c.d. "Design package" con il quale la Commissione UE ha inteso aggiornare e ammodernare le norme esistenti (per affrontare sfide di tecnologie emergenti come la stampa 3D, il metaverso e l'intelligenza artificiale), nonché rendere la tutela dei disegni e dei modelli più adeguata ai nuovi prodotti.

Il Design Package si compone:

- della Direttiva (UE) 2024/2823 del 23 ottobre 2024 sulla protezione giuridica dei disegni e modelli

- del Regolamento (UE) 2024/2822 che modifica il Regolamento (CE) n. 6/2002 su disegni e modelli comunitari e abroga il Regolamento (CE) n. 2246/2002.

Il nuovo Regolamento sui disegni e modelli europei sarà applicabile dal 1° maggio 2025, mentre le disposizioni che richiedono leggi aggiuntive entreranno in vigore dal 1° luglio 2026.

La Direttiva sui disegni e modelli entrerà in vigore l'8 dicembre 2024, ma gli Stati membri avranno tempo fino al 9 dicembre 2027 per adattare la loro legislazione nazionale (nel caso dell'Italia: il Codice della Proprietà Industriale).
