

Conformità digitale nell'UE

Guida pratica

Azioni ed evidenze per nove atti normativi dell'UE

SCAI – Swiss Cyber AI | 8 ottobre 2026 | www.swisscyberai.org

Uno strumento per sicurezza, IT, legale, privacy, acquisti e funzioni aziendali. Definire l'ambito, assegnare i responsabili, colmare le lacune urgenti, verificare i controlli e conservare le evidenze.

Utilizzare la guida in tre sessioni di lavoro

Sessione	Attività	Risultato
1 Delimitare 60 minuti	Legale e funzioni aziendali esaminano la tabella normativa e le domande sull'ambito alle pagine 2 e 3.	Una scheda dell'ambito approvata per ciascun soggetto giuridico o servizio.
2 Assegnare 90 minuti	I responsabili individuano le lacune con le pagine 4–16 e la verifica dei fornitori a pagina 20.	Azioni, responsabili, scadenze ed evidenze richieste.
3 Dimostrare Mezza giornata	Simulare le notifiche, ripristinare un servizio e verificare le evidenze a campione. Utilizzare le pagine 17–23.	Risultati dei test e piano di 90 giorni finanziato.

Trovare la sezione utile

Pagine	Strumenti di lavoro
2–6	Tabella normativa con link, applicabilità, responsabilità e controlli comuni
7–16	NIS2 e liste di controllo pratiche per tutti i nove atti
17–19	Gestione degli incidenti e termini di notifica
20–23	Verifica dei fornitori, piano di 90 giorni e schede riutilizzabili
24	Scadenze e fonti ufficiali integrative

Come leggere le azioni: I riferimenti rosa sottolineati aprono l'articolo o il paragrafo su EUR-Lex; le lettere sono indicate nell'etichetta. «Supporta» collega una raccomandazione alla sua finalità normativa, senza rendere obbligatorio il metodo o l'obiettivo. Le citazioni sono brevi estratti ufficiali: leggere la disposizione completa per le condizioni.

Applicare ogni obbligo secondo ambito, ruolo e data di applicazione. Integrare le norme nazionali e settoriali. Responsabili proposti, test e piano di 90 giorni sono raccomandazioni; la guida non certifica la conformità.

Atti normativi UE e link ufficiali

Aprire l'atto nell'ultima colonna. Su EUR-Lex verificare la versione consolidata vigente, le modifiche e gli atti di esecuzione applicabili. Le pagine successive illustrano come attuarli.

Atto	Quando valutarlo	Primo risultato	Testo ufficiale UE
RGPD	Trattamento di dati personali nell'ambito territoriale dell'articolo 3.	Registro dei trattamenti e dei flussi di dati.	Regolamento 2016/679 Art. 3, 5, 24, 28, 30 a 35
NIS2	Settore o servizio incluso, criteri dimensionali ed eccezioni. Attuazione secondo il diritto nazionale.	Classificazione del soggetto e canale locale di notifica.	Direttiva 2022/2555 Art. 2 a 4, 20, 21, 23, 26
DORA	Entità finanziarie incluse. Norme specifiche per i fornitori TIC critici designati.	Quadro TIC e registro dei fornitori.	Regolamento 2022/2554 Art. 2, 5 a 16, 19, 24 a 30
Reg. IA	Fornitura o impiego di IA nell'ambito del regolamento. Ruolo e finalità determinano gli obblighi.	Inventario e classificazione dell'IA.	Regolamento 2024/1689 Art. 2 a 6, 16, 26, 50, 53, 113
CRA	Prodotti hardware o software inclusi, messi a disposizione sul mercato UE.	Ambito del prodotto e procedura di notifica delle vulnerabilità.	Regolamento 2024/2847 Art. 2, 13, 14, 32, 69, 71; allegato I
CER	Soggetti individuati come critici secondo l'attuazione nazionale.	Atto di individuazione e piano dei rischi per tutti i pericoli.	Direttiva 2022/2557 Art. 6, 8, 12 a 15
Data Act	Dati di prodotti connessi, servizi correlati, condivisione dei dati o servizi di trattamento.	Procedura di accesso ai dati e uscita dal cloud verificata.	Regolamento 2023/2854 Art. 1 a 5, 13, 23 a 31, 50
eIDAS	Identità, firme, sigilli elettronici e servizi fiduciari; obblighi secondo il ruolo.	Politica di firma e verifica del servizio fiduciario.	Regolamento 910/2014 Modificato dal regolamento 2024/1183
DSA	Servizi intermediari offerti a destinatari nell'UE; obblighi secondo tipologia e dimensione.	Classificazione del servizio e procedura di segnalazione.	Regolamento 2022/2065 Art. 2, 11 a 18, 19 a 32, 33

Leggere il regolamento IA con il regolamento (UE) 2026/1744, che modifica scadenze e obblighi. Il testo consolidato eIDAS include l'identità digitale europea. Per NIS2 e CER registrare anche la normativa nazionale di recepimento.

Riferimenti normativi [Modifica del regolamento IA 2026/1744](#) | [Modifica eIDAS 2024/1183](#)

Determinare l'applicabilità

Documentare l'ambito per ogni soggetto giuridico e attività pertinente. Una valutazione di gruppo non basta. La sede svizzera non determina la posizione di filiali UE, prodotti commercializzati nell'UE o servizi offerti nell'UE.

Domande in quest'ordine	Da documentare	Rimando
1 Quale soggetto e attività?	Denominazione legale, paese, stabilimento, servizio, prodotto, clienti e legame con l'UE. NIS2 Art. 26 · RGPD Art. 3 · DSA Art. 2(1)	Aprire una scheda a pagina 22.
2 Si trattano dati personali?	Ruolo di titolare o responsabile del trattamento, interessati e analisi territoriale ai sensi dell'articolo 3. RGPD Art. 3 · RGPD Art. 4(7) · RGPD Art. 4(8)	RGPD a pagina 9.
3 Il soggetto opera in un settore incluso?	Servizi effettivi, categoria dell'allegato I o II NIS2, dimensione secondo le regole UE, eccezioni e diritto nazionale. NIS2 Art. 2 · NIS2 allegato I · NIS2 allegato II	NIS2 alle pagine 7 e 8.
4 È un'entità finanziaria regolamentata?	Categoria esatta dell'articolo 2, esclusioni ed eventuale regime semplificato. DORA Art. 2 · DORA Art. 16	DORA a pagina 10.
5 Si fornisce o si utilizza IA?	Finalità, ruolo di fornitore o deployer; divieti, alto rischio, trasparenza e IA per finalità generali (GPAI). Reg. IA Art. 2 · Reg. IA Art. 5 · Reg. IA Art. 6	Regolamento IA a pagina 11.
6 Si vendono prodotti digitali?	Ruolo di fabbricante, importatore o distributore, perimetro del prodotto, esclusioni e immissione sul mercato UE. CRA Art. 2 · CRA Art. 3 · CRA Art. 32	CRA a pagina 12.
7 Esiste una notifica di individuazione come soggetto critico?	Individuazione, data di ricezione, servizio incluso ed esclusioni settoriali. CER Art. 6(3) · CER Art. 8	CER a pagina 13.
8 Quali servizi di dati o online esistono?	Prodotti connessi, cloud, servizi fiduciari, hosting per utenti o funzioni di mercato online. Data Act Art. 1 · eIDAS Art. 2 · DSA Art. 3(g)	Pagine 14–16.

Approvare una conclusione verificabile

Usare quattro esiti: applicabile ora; applicabile da una data; non applicabile con motivazione; da chiarire con revisore e scadenza. Allegare fatti e disposizione a sostegno della conclusione.

Il contratto con il fornitore è una fonte distinta di obblighi. Un cliente regolamentato può imporre requisiti contrattuali anche a fornitori fuori dall'ambito diretto della norma. Valutare il rapporto DORA/NIS2 per l'entità finanziaria e gli obblighi pertinenti.

Rivalutare l'ambito in caso di cambiamenti

- Nuovo paese, acquisizione, servizio, prodotto, finalità IA, segmento di clienti o notifica dell'autorità.
- Modifica rilevante di dimensioni, esternalizzazione, marchio, prodotto o testo normativo.

Riferimenti normativi [NIS2 Art. 2 a 4](#) | [RGPD Art. 3](#) | [DORA Art. 1 e 2](#)

Assegnare responsabilità e criteri di completamento

La direzione resta responsabile degli obblighi attribuiti dalla legge. Il CISO coordina la sicurezza; funzioni aziendali, privacy, legale e responsabili di prodotto assumono i propri compiti. Sostituire i ruoli con nomi effettivi.

Ruolo	Responsabilità operativa	Evidenza del completamento
Sponsor della direzione	Approvare ambito, priorità, risorse e decisioni sui rischi rilevanti. Risolvere le azioni critiche scadute. Supporta: NIS2 Art. 20(1) · DORA Art. 5(2)	Decisioni datate, budget e monitoraggio.
Legale o conformità	Confermare ruoli, norme nazionali, autorità e scadenze; mantenere il registro normativo. Supporta: NIS2 Art. 2 · NIS2 Art. 23 · RGPD Art. 24(1)	Schede dell'ambito e delle notifiche verificate.
CISO e operazioni di sicurezza	Coordinare controlli cyber, rilevamento, risposta e verifiche. Registrare le lacune di copertura. Supporta: NIS2 Art. 21(1) · DORA Art. 5(2)(c)	Responsabili dei controlli, risultati dei test e registri degli incidenti.
CIO e responsabili dei servizi	Gestire asset, accessi, configurazioni, correzioni e ripristino dei servizi. Supporta: DORA Art. 8(1) · DORA Art. 9(4) · DORA Art. 12(1)	Evidenze di copertura e risultati del ripristino.
Responsabile privacy e RPD	Il responsabile privacy gestisce il programma; il RPD, se nominato, fornisce consulenza e sorveglianza in modo indipendente. Supporta: RGPD Art. 24(1) · RGPD Art. 38 · RGPD Art. 39(1)	Registri dei trattamenti, pareri e richieste sui diritti.
Responsabile prodotto o IA	Gestire ciclo di vita del prodotto o finalità IA, rilascio, monitoraggio e assistenza. Supporta: CRA Art. 13 · Reg. IA Art. 16 · Reg. IA Art. 26	Classificazione, approvazione del rilascio e storico delle modifiche.
Acquisti e responsabile del fornitore	Eseguire la dovuta diligenza, ottenere le clausole richieste, monitorare i fornitori e mantenere i piani di uscita. Supporta: NIS2 Art. 21(2)(d) · DORA Art. 28	Scheda fornitore approvata e uscita verificata.
Revisore dei controlli	Verificare le evidenze a campione, ove possibile indipendentemente dall'operatore del controllo; confermare la chiusura. Supporta: NIS2 Art. 21(2)(f) · DORA Art. 6(6)	Rilevi, nuovi test e decisioni di chiusura.

Applicare criteri rigorosi di completamento

- Il controllo ha ambito definito, responsabile nominato e modalità operative documentate.
- L'attuazione copre la popolazione prevista; le esclusioni sono visibili e approvate.
- Un test datato dimostra il risultato richiesto; ogni esito negativo ha un'azione e una scadenza.
- Il link all'evidenza funziona e indica soggetto, sistema, periodo e revisore.

Svolgere una breve revisione mensile

Esaminare nuovi ambiti, azioni ad alto rischio scadute, test falliti e capacità di notifica. Richiedere una decisione precisa alla direzione per finanziare una correzione o accettare un rischio. Si raccomanda una revisione complessiva almeno trimestrale.

Riferimenti normativi [NIS2 Art. 20](#) | [DORA Art. 5](#) | [RGPD Art. 24 e 38](#)

Attuare la base comune di sicurezza

Utilizzare i controlli NIST o altri controlli adatti già esistenti. Le misure seguenti sono una base pratica, non una lista per la certificazione UE. Definire frequenze e obiettivi in base al rischio e applicare eventuali requisiti legali o contrattuali più rigorosi.

Controllo e azione	Responsabile proposto	Evidenza da verificare
01 Inventariare servizi critici, IT, cloud, OT, dati e dipendenze. Confrontare le rilevazioni con il registro. Supporta: NIS2 Art. 21(2)(i) · DORA Art. 8(1)	Responsabili dei servizi	Asset non gestiti e mappa delle dipendenze.
02 Applicare autenticazione forte e privilegi minimi. Separare gli account amministrativi e controllare gli accessi di emergenza. Supporta: NIS2 Art. 21(2)(i)-(j) · DORA Art. 9(4)(c)-(d)	Team identità	Verificare accesso, privilegi e revoca alla cessazione del rapporto.
03 Dare priorità alle vulnerabilità secondo sfruttamento, esposizione e impatto. Limitare nel tempo le eccezioni. Supporta: NIS2 Art. 21(2)(e) · DORA Art. 9(4)(f)	IT e OT	Seguire un rilievo urgente dalla correzione al nuovo test.
04 Applicare configurazioni sicure e protezione degli endpoint. Includere server e dispositivi senza supporto nei rapporti sulle lacune. Supporta: DORA Art. 9(2)-(3) · NIS2 Art. 21(1)	Operazioni IT	Rapporto di copertura e risposta a un rilevamento verificata.
05 Segmentare i sistemi critici e proteggere gli accessi remoti. Verificare accessi dei fornitori e isolamento di emergenza. Supporta: DORA Art. 9(4)(b) · NIS2 Art. 21(1)	Rete e OT	Test dei percorsi consentiti ed esercitazione autorizzata di isolamento.
06 Raccogliere log utili, monitorare gli allarmi e mantenere un canale di risposta fuori orario. Supporta: DORA Art. 10(1)-(3) · NIS2 Art. 21(2)(b)	Operazioni di sicurezza	Registro dal rilevamento alla risposta; escalation presa in carico.
07 Proteggere i backup dalla compromissione della produzione. Ripristinare un servizio aziendale completo. Supporta: NIS2 Art. 21(2)(c) · DORA Art. 12(1)-(3)	Responsabili dei servizi	Tempo effettivo di ripristino, integrità dei dati e approvazione aziendale.
08 Valutare fornitori critici, concentrazione e subfornitori; concordare assistenza rapida in caso di incidente. Supporta: NIS2 Art. 21(2)(d) · DORA Art. 28(4) · DORA Art. 30	Acquisti	Valutazione dei rischi, contratto e canale di contatto verificato.
09 Proteggere i dati sensibili con regole di accesso, cifratura e conservazione controllata. Supporta: RGPD Art. 5(1)(e)-(f) · RGPD Art. 32(1)(a) · NIS2 Art. 21(2)(h)	Responsabili dei dati	Campione di accessi, recupero delle chiavi ed evidenza della cancellazione.
10 Formare personale e direzione; simulare incidenti, continuità e notifiche di legge. Supporta: NIS2 Art. 20(2) · NIS2 Art. 21(2)(g) · DORA Art. 13(6)	HR e CISO	Formazione per ruolo e azioni dell'esercitazione completate.

Dare priorità senza attendere il programma completo

Segnalare subito accessi privilegiati esposti, vulnerabilità sfruttate, backup critici mancanti e canali di notifica inutilizzabili. Assegnare una protezione temporanea e una correzione permanente. Il solo piano approvato non riduce l'esposizione.

Riferimenti normativi [NIS2 Art. 21](#) | [RGPD Art. 32](#) | [DORA Art. 6 a 14](#)

Collegare controlli, obblighi e decisioni

Riutilizzare le evidenze comuni mantenendo distinti requisito normativo e lacuna residua. Un indice di maturità o una certificazione costituisce un supporto nel proprio ambito, non una conformità automatica.

Attività comune	Disposizioni supportate	Mantenere visibili le differenze
Valutazione dei rischi	NIS2 Art. 21(2)(a) · DORA Art. 6(1) · RGPD Art. 35(1) · CER Art. 12 · Reg. IA Art. 9	Rischi dei servizi, danni alle persone, resilienza fisica e rischi IA richiedono valutazioni diverse.
Accesso e ripristino	RGPD Art. 32(1)(b)-(c) · NIS2 Art. 21(2)(c) · DORA Art. 9 · DORA Art. 12	Verificare sistemi inclusi, ripresa aziendale e periodo delle evidenze.
Sviluppo sicuro	CRA Art. 13(1)-(2) · CRA allegato I · NIS2 Art. 21(2)(e) · Reg. IA Art. 9	Valutare separatamente conformità del prodotto e obblighi legati al ruolo IA.
Verifica dei fornitori	RGPD Art. 28(3) · NIS2 Art. 21(2)(d) · DORA Art. 28 · DORA Art. 30 · Data Act Art. 25	Clausole sul trattamento, contratti TIC finanziari e diritti di passaggio differiscono.
Gestione degli incidenti	RGPD Art. 33 · RGPD Art. 34 · NIS2 Art. 23 · DORA Art. 19 · CRA Art. 14 · CER Art. 15	Presupposto, soggetto obbligato, autorità, termine e contenuto differiscono.

Rendere attuabile ogni decisione sul rischio

Registrare scenario, servizio e persone coinvolti, misure esistenti, impatto plausibile e trattamento. Assegnare responsabile e scadenza e definire il test che dimostra la riduzione del rischio. Escalare i rischi non finanziabili o non accettabili legalmente.

Limitare nel tempo le eccezioni

Un'eccezione richiede ambito, motivo, controllo compensativo, approvazione, scadenza e test di chiusura. L'accettazione del rischio non elimina un obbligo legale. Il legale verifica l'ammissibilità della soluzione temporanea.

Esempio di collegamento rigoroso

Un test dimostra il ripristino dell'applicazione A entro l'obiettivo concordato. Collegarlo agli obblighi pertinenti di disponibilità e ripristino. Dipendenze da fornitori mancanti o servizi d'identità non testati restano lacune aperte; non dichiarare soddisfatta l'intera norma.

Verifica prima delle modifiche

Prima di nuovi servizi, fornitori, usi IA o rilasci di prodotto: riesaminare ambito e rischi, confermare notifiche o passaggi di conformità, testare i controlli e registrare l'approvazione aziendale. Ripetere se cambia la finalità.

Riferimenti normativi [NIS2 Art. 21](#) | [RGPD Art. 25 e 35](#) | [CRA allegato I](#)

NIS2 ambito e governance

Determinare l'applicabilità per soggetto e servizio. Applicare il recepimento nazionale; non attendere una lettera dell'autorità quando la legge richiede autovalutazione o registrazione.

Dal testo normativo «*approvino le misure di gestione dei rischi di cibersicurezza*» [NIS2 Art. 20\(1\)](#)

L'approvazione della direzione è esplicita nel testo UE; attuarla secondo il diritto nazionale.

Passo	Azione	Risultato richiesto
1 Inquadrare l'attività	Collegare i servizi effettivi agli allegati I o II e alle categorie nazionali: energia, trasporti, salute, acqua, infrastrutture digitali, gestione dei servizi TIC e specifiche attività manifatturiere. NIS2 Art. 2(1) · NIS2 allegato I · NIS2 allegato II	Motivazione per settore e servizio con disposizione precisa.
2 Calcolare la dimensione	Applicare le regole dimensionali UE, incluse le imprese associate e collegate pertinenti. Registrare personale e dati finanziari. Verificare le eccezioni per soggetti più piccoli. NIS2 Art. 2(1)-(2)	Calcolo ed eccezioni verificati dal legale.
3 Classificare il soggetto	Determinare lo status essenziale o importante secondo l'articolo 3 e il diritto nazionale. Verificare individuazioni specifiche e giurisdizione transfrontaliera. NIS2 Art. 3(1)-(2) · NIS2 Art. 26	Classificazione e autorità competente.
4 Registrarsi se richiesto	Confermare scadenze locali, dati di registrazione, accesso al portale e notifiche di modifica. Nominare responsabile e sostituto. NIS2 Art. 3(4) · NIS2 Art. 27(2)-(3)	Ricevuta o motivazione documentata dell'assenza di obbligo.
5 Coinvolgere la direzione	La direzione approva e supervisiona le misure di rischio e segue la formazione richiesta. Documentare decisioni e risorse. NIS2 Art. 20(1)-(2)	Verbalì, evidenze della formazione e responsabili delle azioni.
6 Preparare le notifiche	Definire criteri di significatività e scadenze. Il regolamento 2024/2690 riguarda determinati fornitori digitali. NIS2 Art. 23(3)-(4) · 2024/2690 Art. 3	Procedura locale, canale verificato ed esercitazione.

Domande pratiche di classificazione

- Gestiamo direttamente un servizio incluso o ci limitiamo ad acquistarlo?
- L'attività manifatturiera rientra in una categoria specificamente elencata?
- Un'eccezione dimensionale, l'individuazione come soggetto critico o una norma settoriale modifica l'esito?

Sovrapposizioni: Per le entità finanziarie soggette a DORA, esaminare il rapporto settoriale previsto dall'articolo 4 NIS2. Mantenere nella valutazione RGPD, obblighi sui prodotti e altre norme.

Riferimenti normativi [NIS2 Art. 2 a 4 e 20](#) | [Regole di esecuzione per il settore digitale](#)

NIS2 lista di controllo operativa

L'articolo 21 richiede misure tecniche, operative e organizzative proporzionate. I dieci ambiti verificano la completezza; requisiti nazionali e valutazione dei rischi determinano l'attuazione concreta.

Dal testo normativo «strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza»

[NIS2 Art. 21\(2\)\(f\)](#)

Conservare risultati dei test e azioni correttive, non solo le politiche.

Ambito dell'articolo 21	Azione pratica	Evidenza
Analisi dei rischi e politica di sicurezza	Approvare una valutazione dei rischi per servizio e una politica di sicurezza applicabile. NIS2 Art. 21(2)(a)	Valutazione aggiornata, approvazione e piano di trattamento.
Gestione degli incidenti	Definire triage, autorità di risposta, contenimento e decisioni di notifica. NIS2 Art. 21(2)(b)	Procedura operativa, esercitazione e registro dell'incidente.
Continuità e gestione delle crisi	Definire gli obiettivi di ripristino; proteggere i backup e verificarne il recupero. NIS2 Art. 21(2)(c)	Risultati del ripristino ed esercitazione di crisi.
Sicurezza della catena di approvvigionamento	Valutare fornitori diretti e prestatori di servizi; affrontare vulnerabilità pertinenti e pratiche sicure. NIS2 Art. 21(2)(d)	Registro dei fornitori, decisioni e contratti.
Acquisizione e sviluppo	Integrare la sicurezza in progettazione, modifiche, manutenzione, gestione e divulgazione delle vulnerabilità. NIS2 Art. 21(2)(e)	Evidenze di rilascio e registro delle vulnerabilità.
Valutazione dell'efficacia	Verificare che i controlli funzionino nell'intero ambito dichiarato. NIS2 Art. 21(2)(f)	Risultati a campione, anomalie e nuovi test.
Igiene informatica e formazione	Formare utenti e direzione secondo ruolo e rischi attuali. NIS2 Art. 21(2)(g)	Registri della formazione e verifiche dell'apprendimento.
Crittografia	Definire dove e come cifrare; gestire chiavi e recupero. NIS2 Art. 21(2)(h)	Standard, responsabile delle chiavi e recupero verificato.
Persone, accessi e asset	Gestire ingressi, cambi di ruolo, uscite, privilegi e responsabilità degli asset. NIS2 Art. 21(2)(i)	Revisione degli accessi e riconciliazione degli asset.
Autenticazione e comunicazione	Applicare, ove appropriato, MFA o autenticazione continua e comunicazioni sicure. NIS2 Art. 21(2)(j)	Configurazione, eccezioni e test del canale di emergenza.

Tre risultati da dimostrare nel primo mese

- All'uscita di una persona, gli accessi, inclusi quelli privilegiati e di terzi, sono revocati entro il termine approvato.
- Un servizio critico può essere ripristinato con le dipendenze da identità, rete e fornitori.
- Il team incidenti raggiunge il canale corretto dell'autorità e prepara una pre-notifica tempestiva.

Il regolamento 2024/2690 dettaglia i requisiti per specifici soggetti digitali. La sua lista non è automaticamente vincolante per ogni settore NIS2.

Riferimenti normativi [NIS2 Art. 21](#) | [Regolamento 2024/2690](#)

RGPD lista di controllo pratica

Valutare separatamente titolari e responsabili del trattamento. Dati dei dipendenti e dei contatti professionali sono personali; il B2B non è un'esenzione generale. Il titolare risponde della conformità; il responsabile della protezione dei dati (RPD), se nominato, consiglia e sorveglia.

Dal testo normativo «Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo» [RGPD Art. 5\(2\)](#)

Rendere facilmente reperibili le evidenze di ciascun controllo.

Azioni ed evidenze

Azione	Responsabile proposto	Evidenze da conservare
Identificare finalità, dati, persone, destinatari e conservazione. Documentare basi giuridiche e condizioni per categorie particolari, se necessarie. RGPD Art. 5(1) · RGPD Art. 6 · RGPD Art. 9 · RGPD Art. 30	Funzioni aziendali e privacy	Registro dei trattamenti, base giuridica e mappa dei flussi.
Fornire informative chiare e raccogliere solo i dati necessari. Definire conservazione e cancellazione efficace. RGPD Art. 5(1)(c)-(e) · RGPD Art. 13 · RGPD Art. 14	Responsabili dei dati	Informative pubblicate e risultato di una cancellazione a campione.
Stipulare le clausole dell'articolo 28 con i responsabili. Verificare sub-responsabili, trasferimenti internazionali e garanzie pertinenti. RGPD Art. 28(2)-(3) · RGPD Art. 44 · RGPD Art. 46	Legale e acquisti	Accordi sul trattamento e valutazione dei trasferimenti.
Attuare una sicurezza adeguata al rischio. Valutare la necessità di una DPIA e completarla prima dei trattamenti ad alto rischio. RGPD Art. 32(1) · RGPD Art. 35(1)	CISO e privacy	Risultati dei controlli, DPIA e decisioni di trattamento.
Gestire in sicurezza le richieste sui diritti. Monitorare il termine di un mese e le eventuali proroghe lecite, da motivare entro il primo mese. RGPD Art. 12(3) · RGPD Art. 12(6) · RGPD Art. 15	Operazioni privacy	Verifica dell'identità, risposta e registro delle scadenze.
Preparare decisioni e comunicazioni sulle violazioni. Documentare ogni violazione dei dati, incluse le decisioni di non notificare. RGPD Art. 33(5) · RGPD Art. 34	Responsabile incidenti e privacy	Registro delle violazioni, valutazione dei rischi e ricevute.

Test proposti e disposizioni di supporto

- Seguire un record di dipendente o cliente dalla raccolta alla cancellazione, incluse le copie dei fornitori.
- Simulare una richiesta di accesso e una violazione che coinvolga disponibilità e riservatezza.

I test supportano: [RGPD Art. 5\(2\)](#) · [RGPD Art. 12\(3\)](#) · [RGPD Art. 32\(1\)\(d\)](#)

Attenzione: Il consenso non è la base predefinita per ogni attività. I dati cifrati possono restare personali. Una violazione può verificarsi anche senza esfiltrazione confermata.

Riferimenti normativi [RGPD Art. 5 a 6, 12, 28, 30 a 35](#)

DORA lista di controllo pratica

DORA si applica dal 17 gennaio 2025 alle entità finanziarie incluse, con esclusioni e proporzionalità. I normali fornitori TIC rispondono ai contratti dei clienti; i fornitori terzi TIC critici designati hanno un regime distinto di sorveglianza.

Dal testo normativo «*vigila su tale attuazione e ne è responsabile*» [DORA Art. 5\(2\)](#)

Documentare le decisioni della direzione e il monitoraggio del quadro TIC.

Azioni ed evidenze

Azione	Responsabile proposto	Evidenze da conservare
Collegare funzioni essenziali o importanti a sistemi, dati, persone e fornitori. Individuare concentrazioni e singoli punti di guasto. DORA Art. 8(1) · DORA Art. 8(5) · DORA Art. 29(1)	Funzioni aziendali e IT	Mappa delle funzioni e valutazione delle dipendenze.
Mantenere il quadro dei rischi TIC approvato e le misure di continuità, ripristino e comunicazione. DORA Art. 5(2) · DORA Art. 6(1) · DORA Art. 11 · DORA Art. 14	Direzione e rischi	Quadro approvato, revisioni e decisioni di trattamento.
Classificare gli incidenti secondo i criteri applicabili e preparare le notifiche degli incidenti gravi. Distinguere conoscenza e classificazione. DORA Art. 18(1) · DORA Art. 19(1) · 2025/301 Art. 5	Responsabile incidenti	Lista di classificazione e cronologia delle notifiche.
Attuare test di resilienza proporzionati. Determinare se si applicano test avanzati di penetrazione basati sulle minacce. DORA Art. 24(1)-(2) · DORA Art. 26	CISO e rischi	Piano di test, rilievi, nuovi test e decisione TLPT.
Mantenere il registro prescritto degli accordi contrattuali TIC. Considerare diligenza, concentrazione, subappalto e clausole obbligatorie. DORA Art. 28(3)-(4) · DORA Art. 29 · DORA Art. 30	Acquisti e legale	Registro, contratti e valutazioni dei fornitori.
Verificare continuità e uscita per le dipendenze importanti. Confermare esportazioni utilizzabili, competenze sostitutive, capacità e tempi realistici. DORA Art. 11(6) · DORA Art. 28(8)	Responsabili dei servizi	Prova di ripristino o uscita e accettazione aziendale.

Test proposti e disposizioni di supporto

- Simulare la perdita del servizio di identità usato sia dalla produzione sia dal ripristino di emergenza.
- Preparare la notifica di un incidente grave entro i limiti di quattro e 24 ore a pagina 18.

I test supportano: [DORA Art. 11\(6\)](#) · [DORA Art. 24\(1\)](#) · [2025/301 Art. 5](#)

Attenzione: Esternalizzare notifiche o operazioni non trasferisce la responsabilità dell'entità finanziaria. Un elenco generico dei fornitori non sostituisce il registro delle informazioni prescritto.

Riferimenti normativi [DORA Art. 5 a 16, 19, 24 a 30](#) | [Termini di notifica](#)

Regolamento IA lista di controllo pratica

Classificare sistema e uso previsto. Registrare il ruolo di fornitore, deployer, importatore o distributore; distinguere l'applicazione dal modello di IA per finalità generali (GPAI). Rivalutare se cambiano uso o sistema.

Dal testo normativo «*adottano misure volte a sostenere lo sviluppo dell'alfabetizzazione in materia di IA*» [Reg. IA modificato Art. 4\(1\)](#)

È l'articolo 4, paragrafo 1, modificato; adattare le misure di alfabetizzazione agli usi e ai rischi effettivi.

Azioni ed evidenze

Azione	Responsabile proposto	Evidenze da conservare
Inventariare usi IA, responsabili, input, output, interessati, strumenti collegati e fornitori. Verificare le pratiche vietate prima dell'uso. Reg. IA Art. 2(1) · Reg. IA Art. 3(3)-(4) · Reg. IA Art. 5 · Reg. IA modificato Art. 5(1a)	Funzioni aziendali e legale	Registro IA, finalità e verifica dei divieti.
Valutare obblighi per alto rischio, trasparenza e GPAI. Registrare ruolo, motivazione giuridica e data di applicazione; riesaminare modifiche o cambio di marchio. Reg. IA Art. 6 · Reg. IA Art. 25(1) · Reg. IA Art. 50 · Reg. IA Art. 53 · 2026/1744 Art. 1(40)	Governance IA	Classificazione approvata e condizioni di revisione.
Applicare gli obblighi attuali di informazione e alfabetizzazione. Formare su usi e rischi; fornire gli avvisi richiesti su interazioni o contenuti. Reg. IA modificato Art. 4(1) · Reg. IA Art. 50(1)-(4)	Funzioni aziendali e HR	Avvisi, materiali formativi e presenze.
Per gli obblighi pertinenti ad alto rischio, pianificare documentazione, qualità e conformità del fornitore, oppure supervisione e monitoraggio del deployer. Reg. IA Art. 16 · Reg. IA Art. 17 · Reg. IA Art. 26 · Reg. IA Art. 43 · 2026/1744 Art. 1(40)	Prodotto o funzione aziendale	Requisiti ed evidenze secondo il ruolo.
Valutare dati personali ed effetti dannosi. Testare casi rappresentativi, limiti e intervento umano effettivo. RGPD Art. 35(1) · Reg. IA Art. 9 · Reg. IA Art. 14 · Reg. IA Art. 27(1)	Privacy e funzione aziendale	DPIA se richiesta, test e decisione di rilascio.
Per gli agenti, limitare permessi sugli strumenti e accesso ai dati; definire limiti d'azione, approvazioni e arresto verificato. Supporta: Reg. IA Art. 14(4)(d)-(e) · Reg. IA Art. 15(5) · RGPD Art. 32(1)	Ingegneria e CISO	Mappa dei permessi, log delle azioni e test di arresto.

Test proposti e disposizioni di supporto

- Chiedere al responsabile di spiegare finalità, ruolo giuridico e ammissibilità del sistema.
- Testare un output errato e un'istruzione non autorizzata a uno strumento; verificare intervento e recupero.

I test supportano: [Reg. IA Art. 14](#) · [Reg. IA Art. 15](#) · [2026/1744 Art. 1\(40\)](#)

Attenzione: I controlli sugli agenti sono raccomandazioni, non un'architettura obbligatoria. La modifica del 2026 cambia le date per l'alto rischio; vedere pagina 24. Gli altri obblighi applicabili restano validi.

Riferimenti normativi [Reg. IA](#) | [Modifica del 2026](#)

Cyber Resilience Act lista pratica

Verificare se il prodotto con elementi digitali rientra nell'ambito e quale ruolo economico si applica. Le notifiche dell'articolo 14 si applicano dall'11 settembre 2026; la maggior parte dei requisiti dall'11 dicembre 2027.

Dal testo normativo «sono messi a disposizione sul mercato con una configurazione sicura per impostazione predefinita» [CRA allegato I parte I \(2\)\(b\)](#)

Applicare le condizioni di rischio e applicabilità e l'eccezione B2B su misura previste dalla disposizione completa.

Azioni ed evidenze

Azione	Responsabile proposto	Evidenze da conservare
Definire confini del prodotto, trattamento remoto necessario, versioni, immissione sul mercato UE ed esclusioni. Individuare la procedura di conformità. CRA Art. 2 · CRA Art. 3(1)-(2) · CRA Art. 32	Prodotto e legale	Ambito, ruolo e decisione sulla conformità.
Valutare i rischi cyber del prodotto. Integrare la sicurezza in progettazione, impostazioni predefinite, accessi e aggiornamenti. CRA Art. 13(1)-(3) · CRA allegato I parte I	Ingegneria	Valutazione delle minacce, requisiti e test di sicurezza.
Tracciare componenti software e vulnerabilità. Preparare una distinta base software leggibile da macchina e un canale di divulgazione. CRA allegato I parte II (1), (5)-(6)	Sicurezza del prodotto	Inventario dei componenti, SBOM e segnalazioni ricevute.
Finanziare assistenza e aggiornamenti sicuri lungo il ciclo di vita. Motivare la durata del supporto: di norma almeno cinque anni, salvo uso previsto più breve. CRA Art. 13(8) · CRA Art. 13(19) · CRA allegato I parte II (7)-(8)	Gestione del prodotto	Decisione sul supporto, data finale pubblicata e test degli aggiornamenti.
Preparare documentazione tecnica, istruzioni richieste, dichiarazione UE e marcatura CE con la procedura di conformità applicabile. CRA Art. 13(12) · CRA Art. 28 · CRA Art. 30 · CRA Art. 31 · CRA Art. 32	Prodotto e qualità	Dossier di rilascio ed evidenze di conformità.
Attuare già le notifiche per vulnerabilità sfruttate e incidenti gravi pertinenti. Includere i prodotti preesistenti soggetti all'articolo 69. CRA Art. 14(1)-(4) · CRA Art. 69(3) · CRA Art. 71	Team risposta prodotto	Contatto per il termine di 24 ore, classificazione e notifiche.

Test proposti e disposizioni di supporto

- Per un prodotto rilasciato, identificare versioni coinvolte, componenti, responsabile del supporto e contatto clienti.
- Simulare una vulnerabilità dalla valutazione e notifica alla distribuzione della correzione e alle istruzioni agli utenti.

I test supportano: [CRA Art. 13\(2\)](#) · [CRA Art. 14](#) · [CRA allegato I parte II](#)

Attenzione: Un SaaS autonomo non è automaticamente un prodotto CRA. Il trattamento remoto necessario può far parte del prodotto. Il supporto deve riflettere l'uso previsto; cinque anni non bastano sempre.

Riferimenti normativi [CRA Art. 13, 14, 32, 69 e 71](#)

Resilienza dei soggetti critici lista pratica

CER riguarda la resilienza dei soggetti critici individuati e dei servizi essenziali contro perturbazioni fisiche e di altro tipo. Verificare individuazione e notifica nazionali. Considerare le esclusioni settoriali, anche per banche e infrastrutture finanziarie e digitali.

Dal testo normativo «*misure tecniche, di sicurezza e organizzative adeguate e proporzionate per garantire la propria resilienza*» [CER Art. 13\(1\)](#)

Collegare le misure alla valutazione dei rischi del soggetto e all'attuazione nazionale.

Azioni ed evidenze

Azione	Responsabile proposto	Evidenze da conservare
Registrare notifica, ricezione, servizio, autorità e obblighi. Verificare le eccezioni settoriali e nazionali. CER Art. 6(3) · CER Art. 8	Legale e continuità	Dossier di individuazione e scadenze applicabili.
Valutare pericoli naturali e umani: energia, acqua, accessi, persone, sabotaggio e dipendenze transfrontaliere. CER Art. 12(1)-(2)	Continuità e strutture	Valutazione multirischio.
Proteggere siti e attività in modo proporzionato. Definire accessi, protezioni fisiche e misure sul personale consentite dalla legge. CER Art. 13(1)(a)-(b), (e) · CER Art. 14	Strutture e HR	Controlli, accessi autorizzati e verifiche lecite.
Pianificare continuità, soluzioni alternative e ripristino. Confermare risorse, alternative e livelli minimi sostenibili di servizio. CER Art. 13(1)(c)-(d)	Responsabile aziendale	Piano di resilienza e accordi sulle dipendenze.
Formare il personale e simulare perturbazioni. Nominare un referente e preparare le notifiche degli incidenti significativi. CER Art. 13(1)(f) · CER Art. 13(3) · CER Art. 15(1)	Responsabile continuità	Esercitazione, scheda contatti e procedura di notifica.
Monitorare le scadenze dalla notifica. Valutazione dei rischi entro nove mesi; capitolo III applicabile in generale dopo dieci mesi. CER Art. 6(3) · CER Art. 12(1)	Legale e sponsor	Piano datato collegato alla notifica effettiva.

Test proposti e disposizioni di supporto

- Simulare un'interruzione prolungata di energia o acqua, sito inaccessibile e indisponibilità di un fornitore chiave.
- Dimostrare quale servizio minimo prosegue, per quanto tempo e con quali persone e risorse.

I test supportano: [CER Art. 13\(1\)\(c\)-\(d\), \(f\)](#)

Attenzione: Un piano di ripristino cyber non copre da solo la resilienza fisica. Registrare separatamente classificazioni NIS2/CER e obblighi locali, anche con evidenze condivise.

Riferimenti normativi [CER Art. 6, 8 e 12 a 15](#)

Data Act lista di controllo pratica

Mappare i ruoli: fabbricante di prodotti connessi, fornitore di servizi correlati, utente, titolare o destinatario dei dati, fornitore di servizi di trattamento. Anche il cliente cloud dovrebbe usare le regole di passaggio negli acquisti e nella pianificazione dell'uscita.

Dal testo normativo «*adottano le misure di cui agli articoli 25, 26, 27, 29 e 30*» [Data Act Art. 23](#)

Leggere l'obbligo completo di passaggio, con ruolo, ambito ed eccezioni.

Azioni ed evidenze

Azione	Responsabile proposto	Evidenze da conservare
Identificare dati di prodotti e servizi correlati, metadati, accessi e soggetto che detiene ciascun insieme di dati. Data Act Art. 2(15)-(17) · Data Act Art. 3(1)	Responsabili prodotto e dati	Catalogo dei dati e mappa dei ruoli.
Fornire informazioni precontrattuali e accesso utente richiesti. Verificare identità e autorizzazione senza procedure ostruzionistiche. Data Act Art. 3(2)-(3) · Data Act Art. 4(1)	Prodotto e operazioni	Informazioni, canale di richiesta e campione fornito.
Gestire la condivisione ammissibile con terzi. Verificare RGPD, segreti commerciali, usi consentiti e protezioni necessarie. Data Act Art. 4(6)-(9) · Data Act Art. 5 · Data Act Art. 6	Legale e privacy	Decisione di condivisione, garanzie e condizioni di accesso.
Verificare clausole abusive e trasparenza nei contratti sui dati. Far valutare dal legale le richieste vincolanti degli enti pubblici. Data Act Art. 13 · Data Act Art. 14 · Data Act Art. 17	Legale e acquisti	Revisione del contratto e valutazione della richiesta.
Per cloud e servizi di trattamento inclusi, definire dati esportabili, interfacce, transizione, assistenza, costi e cancellazione. Data Act Art. 25 · Data Act Art. 27 · Data Act Art. 29 · Data Act Art. 30	Responsabile del servizio	Contratto e piano di passaggio attuabile.
Testare l'esportazione in un ambiente alternativo; riconciliare i record e registrare limiti funzionali o di interoperabilità. Supporta: Data Act Art. 23(c)-(d) · Data Act Art. 30	IT e funzione aziendale	Test di esportazione/importazione e azioni di uscita.

Test proposti e disposizioni di supporto

- Richiedere dati rappresentativi di un prodotto connesso; verificare completezza, formato, metadati e autorizzazione.
- Leggere i dati cloud esportati con uno strumento indipendente; misurare tempi e impegno effettivi.

I test supportano: [Data Act Art. 4\(1\)](#) · [Data Act Art. 23\(c\)](#) · [Data Act Art. 30](#)

Attenzione: Il Data Act non dà accesso generale a tutti i dati aziendali e non prevale sul RGPD. L'eliminazione dei costi di passaggio non annulla ogni canone di servizio o penale di recesso anticipato.

Riferimenti normativi [Data Act Art. 3 a 5, 13, 23 a 31 e 50](#)

eIDAS e fiducia digitale lista pratica

Distinguere l'impresa che usa firme o identità elettroniche dal prestatore di servizi fiduciari regolamentati. La lista parte dall'impresa che vi fa affidamento; prestatori e partecipanti ai portafogli hanno ulteriori requisiti specifici.

Dal testo normativo «Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa.»
[eIDAS Art. 25\(2\)](#)

Verificare separatamente poteri di firma e formalità nazionali.

Azioni ed evidenze

Azione	Responsabile proposto	Evidenze da conservare
Elencare transazioni, paesi, parti e requisiti formali. Definire il livello di firma o sigillo necessario per ogni processo. Supporta: eIDAS Art. 2(3) · eIDAS Art. 25 · eIDAS Art. 35	Legale e responsabile del processo	Politica che associa transazioni e livelli di firma.
Scegliere e verificare il servizio. Se è richiesto lo status qualificato, verificare il servizio specifico negli elenchi di fiducia ufficiali. eIDAS Art. 22(1) · eIDAS Art. 32(1)	Acquisti e legale	Verifica datata dello status del servizio.
Verificare identità e poteri di firma. Proteggere le credenziali di firma; definire delega, revoca e gestione delle uscite. Supporta: eIDAS Art. 26 · eIDAS Art. 32(1)	Identità e funzione aziendale	Evidenza dell'identità e potere di firma.
Conservare file firmato, validazione, certificati, riferimenti temporali ed evidenze per verifiche future. Supporta: eIDAS Art. 32(1) · eIDAS Art. 34	Responsabile documentale	Dossier di validazione e conservazione.
Testare la validazione fuori dal portale del fornitore. Assicurare la conservazione delle evidenze dopo la fine del contratto o il fallimento del prestatore. Supporta: eIDAS Art. 32 · eIDAS Art. 34	IT e gestione documentale	Validazione indipendente e test di esportazione.
Se si offrono servizi d'identità o fiduciari, valutare separatamente conformità, vigilanza, incidenti e obblighi dei portafogli EUDI. eIDAS Art. 5a · eIDAS Art. 19a · eIDAS Art. 20 · eIDAS Art. 24	Servizio e legale	Piano di conformità e notifica secondo il ruolo.

Test proposti e disposizioni di supporto

- Verificare un documento firmato senza affidarsi solo a screenshot o e-mail di approvazione del fornitore.
- Verificare che il firmatario fosse autorizzato alla transazione al momento della firma.

I test supportano: [eIDAS Art. 32](#) · [eIDAS Art. 34](#)

Attenzione: Una firma elettronica qualificata ha nell'UE l'effetto di una firma autografa, ma non prova da sola i poteri di rappresentanza né soddisfa ogni formalità nazionale. Il sigillo elettronico è uno strumento diverso.

Riferimenti normativi [eIDAS Art. 22, 25, 32 e 35](#) | [Elenchi di fiducia UE](#)

Digital Services Act lista pratica

Classificare ogni servizio: semplice trasporto, memorizzazione temporanea, hosting, piattaforma, mercato online o servizio designato molto grande. Un sito aziendale con contenuti propri non è automaticamente una piattaforma DSA.

Dal testo normativo «Tali meccanismi sono di facile accesso e uso» [DSA Art. 16\(1\)](#)

Testare il meccanismo di segnalazione dell'hosting con un caso realistico.

Azioni ed evidenze

Azione	Responsabile proposto	Evidenze da conservare
Documentare funzioni, destinatari UE e gestore. Verificare l'ambito esatto delle esenzioni dimensionali. DSA Art. 2(1) · DSA Art. 3(g), (i) · DSA Art. 19(1) · DSA Art. 29	Prodotto e legale	Classificazione del servizio e analisi delle esenzioni.
Pubblicare contatti e condizioni richiesti. Spiegare chiaramente restrizioni dei contenuti e politiche di moderazione. DSA Art. 11(1) · DSA Art. 12(1) · DSA Art. 14(1)	Legale e operazioni	Punti di contatto, condizioni ed evidenza della pubblicazione.
Per l'hosting, attuare segnalazioni utilizzabili di contenuti illegali. Valutare diligentemente i casi, registrare le decisioni e fornire le motivazioni richieste. DSA Art. 16(1)-(6) · DSA Art. 17(1)-(3)	Fiducia e sicurezza	Segnalazione, valutazione, decisione e comunicazione.
Per le piattaforme interessate, gestire i reclami e verificare obblighi su pubblicità, interfacce e tutela dei minori. DSA Art. 20(1) · DSA Art. 25 · DSA Art. 26 · DSA Art. 28	Prodotto e operazioni	Esiti dei reclami e verifiche di progettazione.
Per i mercati online interessati, attuare tracciabilità degli operatori commerciali e conformità fin dalla progettazione. DSA Art. 30(1)-(3) · DSA Art. 31	Responsabile del mercato online	Verifiche degli operatori e test del flusso di pubblicazione delle offerte.
Monitorare numero di destinatari ed eventuale designazione. Se designato molto grande, applicare il regime aggiuntivo sui rischi sistemici e gli audit. DSA Art. 24(2) · DSA Art. 33 · DSA Art. 34 · DSA Art. 37	Conformità	Calcolo degli utenti, designazione e piano di verifica.

Test proposti e disposizioni di supporto

- Presentare una segnalazione realistica di contenuti illegali e seguirla fino a una decisione motivata.
- Testare un reclamo pertinente e verificare che sia possibile correggere un errore precedente.

I test supportano: [DSA Art. 16\(6\)](#) · [DSA Art. 20\(4\)](#)

Attenzione: Le esenzioni per micro e piccole imprese eliminano alcuni obblighi, non l'intero regolamento. L'articolo 18 riguarda specifici sospetti di reati contro vita o sicurezza; il DSA non impone una notifica cyber universale entro 72 ore.

Riferimenti normativi [DSA Art. 11 a 18, 19 a 32 e 33 a 42](#)

Gestire la prima ora di un incidente

Avviare insieme contenimento e valutazione legale. I tempi sotto sono obiettivi interni raccomandati, non termini di legge. Non attendere la conferma della causa per una notifica obbligatoria.

Obiettivo	Azione	Risultato
0–15 minuti	Nominare responsabile e verbalizzante. Tutelare la sicurezza, attivare i contatti e preservare i log. Registrare scoperta e tempi noti degli eventi in UTC. Supporta: NIS2 Art. 21(2)(b) · DORA Art. 17(3)(a)	ID del caso, cronologia e ambito iniziale coinvolto.
15–30 minuti	Contenere secondo procedure autorizzate. In OT, coinvolgere ove possibile sicurezza o responsabile di stabilimento prima di azioni perturbative. Identificare soggetti, servizi, prodotti e dati coinvolti. Supporta: DORA Art. 17(3)(b), (f) · NIS2 Art. 21(2)(b)	Decisioni di contenimento e impatto aziendale.
Entro 30 minuti	Coinvolgere legale, privacy, funzioni aziendali e prodotto secondo necessità. Valutare ogni presupposto di notifica e registrare i tempi di conoscenza o classificazione giuridicamente rilevanti. Supporta: RGPD Art. 33(1) · NIS2 Art. 23(3) · DORA Art. 18(1)	Decisioni e scadenze distinte per ogni notifica.
Entro 60 minuti	Nominare inviante e sostituto per ogni canale. Preparare fatti iniziali, elementi ignoti e protezioni. Confermare comunicazioni ai clienti e obblighi contrattuali. Supporta: RGPD Art. 33(3)-(4) · NIS2 Art. 23(4) · DORA Art. 19(1)	Prime notifiche approvate o decisione documentata di non notificare.

Una cronologia e termini normativi distinti

Registrare rilevamento, conoscenza secondo ogni norma, classificazione grave/significativa, decisioni, invii e ricevute. Un evento può attivare più norme per diversi soggetti del gruppo. Una notifica non soddisfa automaticamente tutti i regimi.

Contenuto minimo del registro dell'incidente

- ID; soggetto giuridico; responsabile e sostituto; servizi, paesi, dati e versioni coinvolti.
- Fatti confermati; ipotesi; impatto su attività e persone; fonti e data/ora di ogni aggiornamento.
- Presupposto per norma; scadenza precisa; destinatario; approvatore; inviante; ricevuta; prossimo aggiornamento.
- Contenimento, ripristino, ubicazione delle evidenze e protezione dei clienti.

Prima della chiusura

Verificare completezza di aggiornamenti e relazioni finali. Registrare causa, recupero di servizi e dati, rischio residuo, azioni, responsabili e nuovi test. Conservare i motivi della mancata notifica e riesaminarli con nuovi fatti.

Riferimenti normativi [RGPD Art. 33 e 34](#) | [NIS2 Art. 23](#) | [Regole di notifica DORA](#)

Principali termini di notifica degli incidenti

Applicare queste regole UE con canale nazionale, soglie, autorità competente e norme tecniche. I termini sono limiti massimi; resta l'obbligo di agire senza ingiustificato ritardo.

Regime e presupposto	Prima notifica	Seguito e destinatario
RGPD titolare del trattamento Violazione dei dati, salvo rischio improbabile per diritti e libertà.	Senza ingiustificato ritardo, ove possibile entro 72 ore dalla conoscenza. Motivare il ritardo.	Autorità di controllo competente. Integrare gradualmente senza ulteriore ritardo ingiustificato. Documentare tutte le violazioni. RGPD Art. 33(1), (3)-(5)
RGPD responsabile e interessati	Responsabile: informare il titolare senza ingiustificato ritardo. Titolare: informare gli interessati senza ingiustificato ritardo in caso di rischio elevato, salve le eccezioni dell'articolo 34.	Non presumere che il responsabile disponga di 72 ore. Monitorare separatamente i termini contrattuali. RGPD Art. 33(2) · RGPD Art. 34(1)-(3)
NIS2 Incidente significativo secondo i criteri applicabili.	Pre-notifica entro 24 ore dalla conoscenza di un incidente significativo; notifica entro 72 ore. Entrambe senza ingiustificato ritardo.	CSIRT o autorità competente. Relazione finale entro un mese dalla notifica; relazione intermedia su richiesta. NIS2 Art. 23(3) · NIS2 Art. 23(4)(a)-(d)
NIS2 incidente in corso e servizi fiduciari	Prestatori fiduciari: notifica degli incidenti pertinenti entro 24 ore anziché 72.	Se l'incidente è ancora in corso alla scadenza finale, inviare un aggiornamento e poi la relazione finale entro un mese dalla gestione dell'incidente. NIS2 Art. 23(4)(b), (e)
DORA Incidente grave connesso alle TIC secondo i criteri applicabili.	Il prima possibile: entro quattro ore dalla classificazione come grave e non oltre 24 ore dalla conoscenza. Se classificato dopo 24 ore, entro quattro ore dalla classificazione.	Autorità finanziaria competente. Relazione intermedia entro 72 ore dalla notifica iniziale; aggiornamento al ripristino. Relazione finale entro un mese dall'intermedia o dal suo ultimo aggiornamento. DORA Art. 19(1) · 2025/301 Art. 5(1)-(4)

Configurare le scadenze prima dell'esercitazione

Per ogni soggetto, compilare portale, autorità, soglie, moduli, inviante e sostituto a pagina 22. Testare l'accesso senza inviare una notifica reale.

DORA prevede regole ed eccezioni per fine settimana e festivi. Adottare una copertura continua; usare una proroga solo dopo aver verificato i presupposti dell'articolo 5 e le eventuali decisioni dell'autorità.

Riferimenti normativi [RGPD Art. 33 e 34](#) | [NIS2 Art. 23](#) | [DORA Regolamento 2025/301 Art. 5](#)

Notifiche sui prodotti e altri canali

Aggiungere questi canali quando attività e ruolo li rendono pertinenti. Verificare date di applicazione e attuazione nazionale; non usare un unico termine generico.

Regime e presupposto	Termine e canale operativo
CRA Vulnerabilità attivamente sfruttata	Il fabbricante notifica tramite la piattaforma unica al CSIRT coordinatore e all'ENISA. Preallarme entro 24 ore dalla conoscenza; notifica della vulnerabilità entro 72 ore. Relazione finale entro 14 giorni dalla disponibilità di una misura correttiva o attenuativa. CRA Art. 14(1)-(2)
CRA Incidente grave che incide sulla sicurezza del prodotto	Stessi destinatari e piattaforma. Preallarme entro 24 ore dalla conoscenza; notifica entro 72 ore. Relazione finale entro un mese dalla notifica. Gestire l'informazione degli utenti interessati ai sensi dell'articolo 14. CRA Art. 14(3)-(4), (8)
CER Perturbazione significativa o potenzialmente significativa dei servizi essenziali	Notificare all'autorità senza ingiustificato ritardo; primo invio entro 24 ore dalla conoscenza, salvo impossibilità operativa. Ove pertinente, relazione dettagliata entro un mese; integrare la norma nazionale nella procedura locale. CER Art. 15(1)
Reg. IA Incidente grave con IA ad alto rischio	Verificare ruolo e transizione. Il fornitore segnala subito al nesso causale o alla sua ragionevole probabilità, entro 15 giorni dalla conoscenza. Violazione diffusa o perturbazione di infrastruttura critica dell'art. 3(49)(b): subito, entro due giorni. Decesso: subito al sospetto nesso, entro dieci giorni. Autorità di vigilanza del mercato o Ufficio per l'IA secondo l'art. 75 modificato. Reg. IA Art. 73(1)-(4) · Reg. IA Art. 26(5) · Reg. IA modificato Art. 75(1a)
eIDAS Violazione di sicurezza o perturbazione di un servizio fiduciario	Prestatori non qualificati: art. 19a, senza ingiustificato ritardo ed entro 24 ore dalla conoscenza. Qualificati: art. 24(2)(fb), senza ingiustificato ritardo ed entro 24 ore dall'incidente. Informare l'organismo di vigilanza e gli altri destinatari previsti. Verificare separatamente NIS2 e RGPD; sono obblighi dei prestatori. eIDAS Art. 19a(1)(b) · eIDAS Art. 24(2)(fb)
DSA Sospetto di specifici reati	Il prestatore di hosting informa tempestivamente l'autorità di contrasto o giudiziaria competente secondo l'articolo 18 quando ricorre il presupposto relativo a vita o sicurezza. È distinto dalle notifiche cyber. DSA Art. 18(1)-(2)

Regola operativa: Registrare versioni, supporto, utenti coinvolti, protezioni e informazioni ancora sensibili. Legale e prodotto coordinano comunicazioni alle autorità e ai clienti. Aggiungere notifiche contrattuali, assicurative e settoriali alla stessa cronologia.

Riferimenti normativi [CRA Art. 14](#) | [CER Art. 15](#) | [Regolamento IA Art. 73](#) | [Modifica IA](#) | [eIDAS](#) | [DSA Art. 18](#)

Unificare la verifica di fornitori e acquisti

Verificare in selezione, rinnovo e modifiche rilevanti. Adeguare l'impegno a impatto, dati, accessi e ruolo giuridico, non solo alla spesa. Approfondire la verifica di piccoli fornitori con accessi privilegiati a sistemi critici.

Decisione	Domanda al fornitore o responsabile	Evidenze da ottenere
Ambito e impatto	Quale soggetto fornisce il servizio? Quali funzioni, dati e sistemi ne dipendono? Supporta: DORA Art. 28(3)-(4) · RGPD Art. 28(1)	Descrizione del servizio, ubicazioni e mappa delle dipendenze.
Accesso e dati	Chi amministra? Quali sub-responsabili o ubicazioni trattano i dati? Come si controllano accessi e cancellazione? Supporta: RGPD Art. 28(2)-(3) · RGPD Art. 44	Modello di accesso, clausole sul trattamento e flussi di dati.
Sicurezza e resilienza	Cosa viene testato? Quali esclusioni restano? Il fornitore può ripristinare il servizio secondo le nostre esigenze? Supporta: NIS2 Art. 21(2)(d) · DORA Art. 28(4)(c)-(d)	Rapporto di verifica pertinente, rilievi aperti ed evidenze di ripristino.
Cooperazione negli incidenti	In quanto tempo, da chi e con quali fatti saremo informati? È disponibile assistenza fuori orario? Supporta: RGPD Art. 28(3)(f) · DORA Art. 30(2)(f), (3)(b)	Obblighi di notifica concordati e canale di contatto verificato.
Audit e modifiche	Possiamo ottenere evidenze? Quali modifiche, subfornitori o interruzioni devono essere notificati? Supporta: RGPD Art. 28(3)(h) · DORA Art. 30(2)(a), (3)	Clausole, diritti sulle modifiche e matrice delle responsabilità.
Uscita e portabilità	Possiamo esportare dati utilizzabili, trasferire il servizio e confermare la cancellazione? Quali tempi, costi e dipendenze restano? Supporta: DORA Art. 28(8) · Data Act Art. 25(2)	Piano di uscita, esportazione di prova e condizioni di recesso.
Clausole specifiche per norma	È coinvolto un trattamento RGPD? DORA si applica al cliente? Sono pertinenti Data Act, IA o obblighi sui prodotti? Supporta: RGPD Art. 28(3) · DORA Art. 30(2)-(3) · Data Act Art. 25	Lista normativa completata secondo le condizioni applicabili.

Adottare una decisione esplicita di approvazione

Approvare, approvare con condizioni e scadenze, oppure rifiutare/sospendere. Allegare lacune, misure compensative, responsabile aziendale e data di revisione. Escalare i requisiti obbligatori contrattuali o legali non soddisfacenti.

Test di accettazione

Scegliere un fornitore critico. Contattare l'escalation, esaminare l'ambito del rapporto, esportare dati rappresentativi e individuare un'opzione valida di continuità o uscita. Registrare le anomalie come azioni, non limitarsi ad archiviare il questionario.

Riferimenti normativi [RGPD Art. 28](#) | [NIS2 Art. 21](#) | [DORA Art. 28 a 30](#) | [Data Act capo VI](#)

Attuare i primi 90 giorni

Piano di attuazione proposto. Scadenze legali, incidenti attivi ed esposizioni critiche hanno priorità. Avviare subito gli obblighi scaduti senza rinviarli a fasi successive.

Quando	Attività	Responsabile	Criteri di accettazione
Giorni 1–10	Confermare ambito di soggetti e attività. Individuare norme nazionali, autorità e obblighi di notifica. Supporta: NIS2 Art. 2 · RGPD Art. 3 · DORA Art. 2	Sponsor e legale	Ogni soggetto prioritario ha un ambito verificato o una questione aperta con scadenza.
Giorni 1–15	Correggere lacune urgenti di accesso ed esposizione; verificare backup critici e contatti per gli incidenti. Supporta: NIS2 Art. 21(2)(c), (i)-(j) · NIS2 Art. 23	CIO e CISO	Esposizioni critiche corrette o protette; canale di notifica utilizzabile.
Giorni 11–30	Assegnare responsabili dei controlli e delle norme. Creare indice delle evidenze e registro prioritario delle azioni. Supporta: NIS2 Art. 20(1) · DORA Art. 5(2)(c) · RGPD Art. 24(1)	Responsabile programma	Ogni lacuna prioritaria ha responsabile, scadenza e test di chiusura.
Giorni 16–45	Verificare fornitori critici e flussi di dati personali. Classificare attività IA e di prodotto. Supporta: DORA Art. 28(4) · RGPD Art. 30 · Reg. IA Art. 6 · CRA Art. 2	Funzioni e specialisti	Contratti, classificazioni e lacune operative registrati.
Giorni 31–60	Attuare controlli prioritari; testare ripristino, accessi privilegiati e notifiche. Supporta: NIS2 Art. 21(2)(f) · DORA Art. 11(6)	Responsabili dei servizi	Test con risultati effettivi; correzioni delle anomalie finanziate.
Giorni 61–75	Ritestare le correzioni. Verificare evidenze a campione e modifiche normative nazionali. Supporta: NIS2 Art. 21(2)(f) · DORA Art. 6(5)-(6)	Verifica e legale	Chiusure supportate da evidenze; applicabilità aggiornata.
Giorni 76–90	La direzione valuta rischi residui, risorse e trimestre successivo. Supporta: NIS2 Art. 20(1) · DORA Art. 5(2)(g)	Sponsor della direzione	Decisioni, budget, prossime tappe e questioni legali aperte sono espliciti.

Regola di priorità

Priorità 1: violazione legale attiva, notifica imminente o esposizione operativa critica. Priorità 2: lacune rilevanti che incidono su servizi importanti o persone. Priorità 3: miglioramenti dopo aver controllato le prime due categorie. Riclassificare al mutare dei fatti.

Presentare decisioni anziché conteggi di attività

Mostrare cosa può fallire, quale obbligo è coinvolto, chi corregge, quando si testa e quale decisione serve. Molte politiche o sessioni formative non dimostrano da sole l'efficacia operativa.

Schede riutilizzabili di ambito e autorità

Copiare i campi nel registro esistente. Creare una scheda per soggetto e attività, con evidenze e decisione del revisore. I campi tra parentesi quadre sono da compilare.

Le schede proposte supportano: [NIS2 Art. 2](#) · [NIS2 Art. 23\(4\)](#) · [RGPD Art. 33\(3\)](#)

Scheda dell'ambito

Campo	Da compilare
Scheda e oggetto	[ID scheda] [Soggetto giuridico] [Paese] [Attività o prodotto]
Ruolo aziendale e giuridico	[Servizio e clienti] [Legame UE] [Titolare/fornitore/deployer/altro ruolo]
Base normativa	[Norma] [Articolo] [Link al recepimento nazionale] [Versione verificata]
Fatti e conclusione	[Dimensione e settore] [Eccezioni] [Applicabile ora / dopo / no / da chiarire]
Date di applicazione	[Inizio dell'obbligo] [Scadenza registrazione] [Ricezione dell'individuazione, se pertinente]
Decisione e revisione	[Responsabile] [Revisore legale] [Approvazione] [Prossima revisione] [Condizione di revisione]

Scheda autorità e notifiche

Campo	Da compilare per ogni canale
Canale e presupposto	[Soggetto] [Norma] [Fonte della soglia] [Decorrenza e durata del termine]
Autorità	[Autorità o CSIRT] [URL portale ufficiale] [Telefono alternativo]
Persone	[Inviante e cellulare] [Sostituto e cellulare] [Approvatore ed escalation]
Accesso e invio	[Gestore account] [Autenticazione] [Modello] [Ubicazione delle ricevute]
Test	[Ultimo test d'accesso] [Risultato] [Questione aperta e responsabile]

Prima di completare la scheda

- Il legale ha verificato soggetto, ruolo, norma nazionale e data di applicazione.
- Inviante e sostituto accedono al portale; i contatti alternativi sono disponibili offline.
- Le credenziali sono in un archivio sicuro approvato, non in questa scheda.

Controllo qualità: Se mancano fatti, usare «da chiarire». Assegnare responsabile e scadenza anziché presumere un'esenzione.

Schede riutilizzabili di azioni ed evidenze

Creare un'azione per lacuna, collegata a requisito e controllo. Conservare le evidenze sensibili in ubicazioni controllate; il registro le richiama senza duplicarle.

Campo della scheda	Contenuto da inserire
Requisito e lacuna	[ID azione] [Soggetto] [Norma e articolo] [Lacuna specifica e impatto]
Azione e responsabilità	[Azione] [Responsabile nominato] [Team attuativo] [Priorità] [Scadenza]
Trattamento temporaneo	[Controllo compensativo] [Approvazione] [Scadenza] [Ammissibilità legale verificata]
Test di chiusura	[Popolazione e metodo] [Risultato atteso] [Data test] [Revisore]
Evidenza e stato	[Link evidenza] [Ambito e periodo] [Risultato effettivo] [Aperto / in corso / testato / chiuso]

Esempio compilato

Lacuna: accesso privilegiato di un fornitore a un servizio critico senza autenticazione forte. Azione: imporre l'autenticazione approvata ed eliminare gli account inutilizzati. Responsabile: servizio identità. Chiusura: testare ogni accesso e riconciliare gli account attivi. Evidenze: configurazione datata, test ed eccezioni approvate. Collegare al requisito specifico senza dichiarare soddisfatta l'intera norma.

Le schede e gli obiettivi proposti supportano: [NIS2 Art. 21\(2\)\(f\)](#) · [DORA Art. 6\(5\)-\(6\)](#) · [RGPD Art. 24\(1\)](#)

Cruscotto mensile della direzione

Indicatore	Obiettivo proposto	Escalare se
Soggetti prioritari con ambito approvato	100% dell'ambito prioritario	Un'attività regolamentata è irrisolta o scaduta.
Azioni di priorità 1 scadute	0	Un'azione resta scaduta.
Servizi critici che superano i test di ripristino	100% dei test programmati	Un servizio non raggiunge l'obiettivo di ripristino.
Accessi critici conformi allo standard	100% o trattamento temporaneo approvato	Un accesso esposto non ha protezioni adeguate.
Canali di notifica con accesso testato e sostituito	100% dei canali applicabili	Un canale richiesto non è utilizzabile.
Azioni chiuse con evidenza verificata indipendentemente	100% delle chiusure campionate	Una chiusura si basa solo su una politica o un'affermazione.

Gli obiettivi sono raccomandazioni gestionali, non esenzioni legali. Definire denominatori, periodo e fonti delle evidenze. Distinguere obbligo, copertura del controllo e risultato operativo.

Monitorare scadenze e modifiche normative

Riferimento normativo: 8 ottobre 2026. Verificare modifiche e attuazione nazionale prima di decisioni rilevanti su ambito o notifiche. Conservare versione e data di applicazione nel registro normativo.

Atto	Data o presupposto	Azione pratica
NIS2	Termine di recepimento UE: 17 ottobre 2024.	Verificare diritto nazionale, registrazione e regole locali di notifica. NIS2 Art. 41(1)
DORA	Applicabile dal 17 gennaio 2025.	Attuare già il quadro e le norme tecniche vigenti. DORA Art. 64
CRA	Notifiche dall'11 settembre 2026; requisiti principali dall'11 dicembre 2027.	Attuare le notifiche dell'articolo 14; pianificare conformità del prodotto ed evidenze del ciclo di vita. CRA Art. 71 · CRA Art. 69(3)
Reg. IA	Applicazione generale dal 2 agosto 2026, con eccezioni scaglionate e modificate.	Attuare gli obblighi applicabili di alfabetizzazione, divieti, GPAl e trasparenza. 2026/1744 Art. 1(40) · Reg. IA modificato Art. 4(1)
IA ad alto rischio	2 dicembre 2027 per gli obblighi pertinenti dell'allegato III; 2 agosto 2028 per l'allegato I.	Usare l'articolo 113 modificato e verificare le transizioni dei sistemi preesistenti. 2026/1744 Art. 1(40)
Transizione IA	Specifici nuovi divieti e transizione per la marcatura dei sistemi esistenti: 2 dicembre 2026.	Verificare l'ambito esatto degli articoli 5 e 50 modificati. Reg. IA modificato Art. 111(4) · 2026/1744 Art. 1(40)
Data Act	Applicazione generale dal 12 settembre 2025. L'articolo 3(1) riguarda prodotti e servizi correlati immessi sul mercato dopo il 12 settembre 2026.	Verificare l'accesso ai dati fin dalla progettazione per i nuovi prodotti. Data Act Art. 50
Data Act passaggio	Eliminazione dei costi di passaggio dal 12 gennaio 2027.	Rivedere le clausole di uscita e distinguere altri costi consentiti. Data Act Art. 29(1)
CER ed eIDAS	I termini CER dipendono dalla notifica di individuazione. Gli obblighi dei portafogli dipendono da ruolo e atti di esecuzione.	Registrare presupposti e scadenze effettivi; evitare una data unica per tutto il gruppo. CER Art. 6(3) · CER Art. 12(1) · eIDAS Art. 5a(1) · eIDAS Art. 5f

Fonti ufficiali integrative

Riferimenti normativi [Esecuzione NIS2 Regolamento 2024/2690](#) | [Notifiche DORA Regolamento 2025/301](#) | [Modifica IA 2026/1744](#) | [Modifica eIDAS 2024/1183](#)

RGPD e DSA sono già generalmente applicabili. Integrare le norme nazionali e settoriali pertinenti. Fanno fede i testi ufficiali; responsabili proposti, test e piano offrono un metodo pratico per attuare i requisiti individuati.