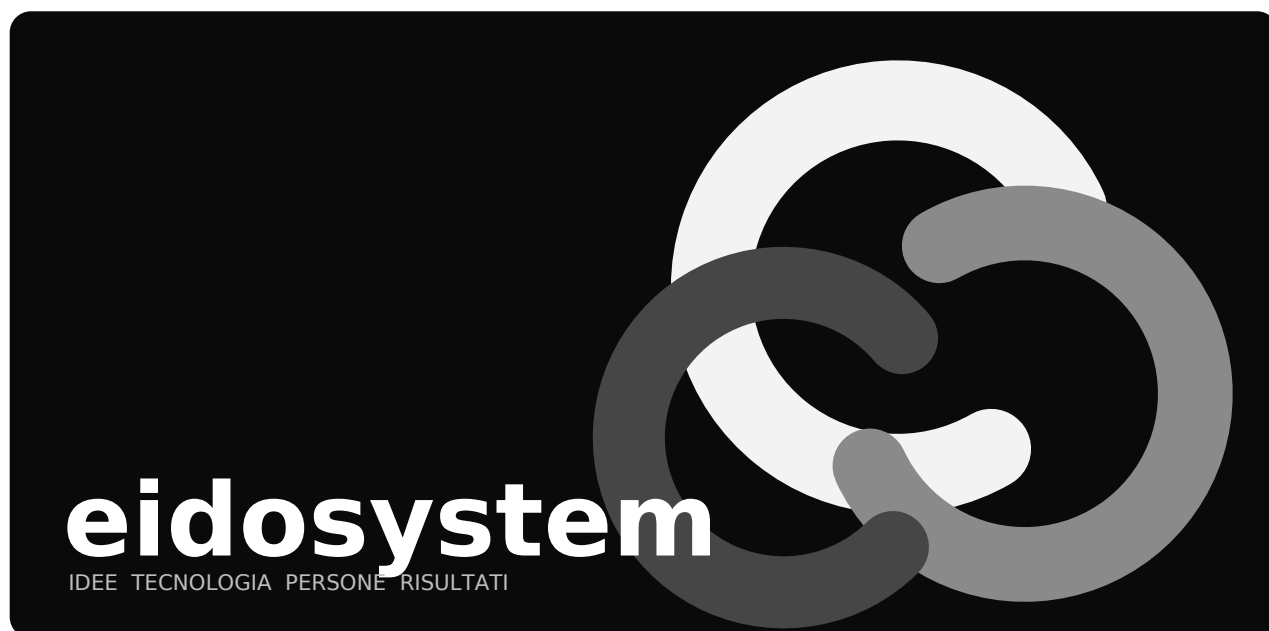


Autovalutazione su dati GDPR NIS2 e AI Act

Protezione dei dati perimetro normativo governance e preparazione

Questo strumento aiuta a individuare lacune organizzative ed evidenze mancanti. GDPR, NIS2 e AI Act hanno ambiti, ruoli e obblighi diversi: per questo il documento restituisce tre risultati separati e utilizza domande filtro. Un punteggio elevato non equivale a una dichiarazione di conformità.



Istruzioni per la compilazione

Rispondi considerando la situazione effettivamente dimostrabile oggi. Quando assegni 2 o 3, indica una prova disponibile: documento, configurazione, verbale, contratto, log o risultato di test. Usa N A solo quando la non applicabilità è motivata.

AZIENDA

SETTORE

NUMERO ADDETTI

DATA

COMPILATO DA FACOLTATIVO

Scala di valutazione

0	Assente o sconosciuto	Il presidio non esiste oppure nessuno sa indicare come funziona.
1	Informale o parziale	Esiste in alcuni casi, dipende dalle persone o non è documentato.
2	Definito e applicato	È documentato e applicato nella maggior parte dei casi rilevanti.
3	Verificato e migliorato	È applicato, testato, misurato e riesaminato periodicamente.
N A	Non applicabile	Escludere dal calcolo soltanto indicando il motivo.

Calcolo

Somma i punti delle domande applicabili. Il massimo è pari a 3 moltiplicato per il numero di domande applicabili. Percentuale uguale punti ottenuti diviso massimo moltiplicato per 100. Valuta ogni area separatamente: una media generale può nascondere una lacuna critica.

Domande filtro

DOMANDA FILTRO NIS2

L'azienda ha documentato una verifica del proprio eventuale inquadramento NIS2 considerando settore, dimensione, ruolo e filiera?

☐ Sì ☐ No ☐ Non so

Se la risposta è No o Non so, completare comunque la sezione come readiness e richiedere una verifica del perimetro.

DOMANDA FILTRO AI Act

L'azienda utilizza, integra, rivende o sviluppa sistemi di intelligenza artificiale, anche incorporati in software di terzi?

☐ Sì ☐ No ☐ Non so

Se la risposta è Sì o Non so, compilare la sezione AI Act e censire gli strumenti effettivamente utilizzati.

Governance GDPR

Valuta conoscenza dei trattamenti, responsabilità e diritti delle persone.

01 Esiste una mappa aggiornata dei trattamenti, dei dati, delle finalità, delle basi giuridiche e dei tempi di conservazione?

Evidenza utile Registro o mappa, proprietari, categorie di dati e destinatari.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

02 Informative, consensi e procedure per i diritti degli interessati sono aggiornati e verificabili?

Evidenza utile Versioni, registri dei consensi, richieste ricevute e tempi di risposta.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

03 Responsabili esterni, servizi cloud e trasferimenti fuori dallo Spazio economico europeo sono censiti e regolati?

Evidenza utile Contratti, istruzioni, localizzazione e garanzie per i trasferimenti.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

Rischio privacy e data breach

Verifica prevenzione, misure di sicurezza e capacita di gestire una violazione.

04 Nuovi progetti e software applicano protezione dei dati fin dalla progettazione e per impostazione predefinita?

Evidenza utile Checklist progettuale, minimizzazione, configurazioni predefinite e approvazioni.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

05 Viene valutata e documentata la necessita di una DPIA per trattamenti potenzialmente ad alto rischio?

Evidenza utile Criteri di screening, DPIA, rischio residuo e riesami.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

06 Le misure assicurano riservatezza, integrita, disponibilita e ripristino in modo proporzionato al rischio?

Evidenza utile Accessi, autenticazione, cifratura, backup, test e monitoraggio.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

07 Esiste una procedura per valutare, registrare e quando necessario notificare un data breach entro i termini?

Evidenza utile Registro incidenti, ruoli, criteri di rischio e procedura di notifica entro 72 ore.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

Preparazione NIS2

Compilare come valutazione di preparazione. L'applicabilità richiede una verifica specifica.

08 L'inquadramento NIS2 è documentato e, se applicabile, sono gestiti registrazione, referenti e comunicazioni con ACN?

Evidenza utile Analisi del perimetro, decisione motivata, registrazioni e referenti.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

09 Il vertice approva e supervisiona misure su rischi, incidenti, continuità, fornitori, vulnerabilità, formazione e accessi?

Evidenza utile Politiche, responsabilità, formazione degli organi e verifiche di efficacia.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

10 Esiste un flusso di segnalazione capace di rispettare le tempistiche applicabili agli incidenti significativi?

Evidenza utile Criteri, escalation, pre notifica, notifica, relazione finale ed evidenze.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

Preparazione AI Act

Valuta inventario, ruolo, rischio, trasparenza e competenze nell'uso dell'intelligenza artificiale.

11 Esiste un inventario degli strumenti AI, delle finalità, dei fornitori, degli utenti e dei dati impiegati?

Evidenza utile Registro dei sistemi, owner, versioni, dati in ingresso e integrazioni.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

12 Per ogni sistema sono identificati ruolo dell'azienda, livello di rischio, pratiche vietate e obblighi di trasparenza?

Evidenza utile Classificazione, provider o deployer, pubblico interessato e comunicazioni.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

13 Le persone che acquistano, configurano o utilizzano AI ricevono formazione, istruzioni e regole interne adeguate?

Evidenza utile Programma di AI literacy, policy, formazione e controlli d'uso.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

14 Per eventuali sistemi ad alto rischio sono previsti supervisione umana, registri, monitoraggio e gestione degli incidenti?

Evidenza utile Istruzioni, competenze del supervisore, log, controlli e azioni correttive.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

Lettura del risultato

Calcola ogni area separatamente. I livelli descrivono la preparazione osservata e non attestano conformità o sicurezza assoluta.

AREA	PUNTI	MASSIMO	PERCENTUALE
Governance GDPR			
Sicurezza e data breach			
Preparazione NIS2			
Preparazione AI Act			

Livelli di preparazione

0-24 Non presidato 25-49 Gestione reattiva 50-74 Gestione strutturata 75-100 Gestione misurata e migliorata

Segnali prioritari

Se una delle condizioni seguenti è vera, trattala come prioritaria anche in presenza di un punteggio complessivo elevato.

- ☐ Non esiste una mappa affidabile dei trattamenti e dei dati personali.
- ☐ Manca una procedura utilizzabile per valutare e gestire un data breach.
- ☐ Non è stata documentata la verifica del perimetro NIS2.
- ☐ Sono utilizzati strumenti AI senza inventario, proprietario o regole interne.

Dai punteggi alle decisioni

Scegli poche azioni verificabili. Ogni intervento dovrebbe avere un responsabile, una scadenza, un risultato atteso e una prova di completamento.

ENTRO 30 GIORNI

ENTRO 90 GIORNI

ENTRO 180 GIORNI

Quando chiedere un approfondimento

Richiedi una verifica guidata quando una risposta non è nota, quando un controllo esiste solo informalmente, quando manca una prova recente o quando una lacuna coinvolge un servizio critico, dati personali, obblighi di notifica o coperture assicurative.

Parla con un esperto www.eidosystem.com

Riferimenti ufficiali

Il questionario sintetizza principi e aree di controllo ricavati dalle fonti seguenti. Le fonti prevalgono sempre su questa autovalutazione e devono essere consultate nella versione vigente.

EDPB Data protection guide for small business Be compliant
Accountability, registro, privacy by design e valutazione di impatto.
https://www.edpb.europa.eu/sme/be-compliant/be-compliant_en

EDPB Data protection guide for small business Secure personal data
Misure tecniche e organizzative adeguate al rischio.
https://www.edpb.europa.eu/sme/be-compliant/secure-personal-data_en

Garante per la protezione dei dati personali Data breach
Valutazione, documentazione e notifica delle violazioni dei dati personali.
<https://www.garanteprivacy.it/data-breach>

Unione europea Direttiva NIS2 2022 2555
Gestione del rischio, continuità, filiera e segnalazione degli incidenti.
<https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

Agenzia per la cybersicurezza nazionale Ambito NIS
Inquadramento italiano dei soggetti NIS.
<https://www.acn.gov.it/portale/nis/ambito>

Agenzia per la cybersicurezza nazionale Misure di sicurezza di base
Modalità e specifiche di base per gli obblighi nazionali.
<https://www.acn.gov.it/portale/nis/modalita-specifiche-base>

Commissione europea Quadro normativo sull'intelligenza artificiale
Approccio basato sul rischio, ruoli, trasparenza e calendario di applicazione.
<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

Unione europea Regolamento AI Act 2024 1689
Testo ufficiale del regolamento europeo sull'intelligenza artificiale.
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

Limiti dello strumento

Strumento informativo e orientativo. Non costituisce audit, certificazione, parere legale o dichiarazione di conformità. Applicabilità e adempimenti devono essere verificati sul caso concreto.

Documento predisposto da Eidosystem Versione 1.0 17 settembre 2026