ACCREDIA
ENTE ITALIANO DI ACCREDITAMENTO

Incontro di aggiornamento

# Congresso Nazionale del Dipartimento Laboratori di prova

## Sessione Laboratori

**21 ottobre 2025**

1

# GDPR e documenti ACCREDIA
# Cyber rischi

2

# Elenco dei documenti ACCREDIA riferito a GDPR

ACCREDIA ha nel proprio sistema di gestione un insieme di procedure dedicate alla gestione degli obblighi previsti dal GDPR:

**CO - Convenzione di Accreditamento tra ACCREDIA e Organismi che svolgono servizi di valutazione della conformità (CABs)**

- GDPR richiede che i soggetti interessati siano informati rispetto ai trattamenti posti in essere dal Titolare;
- La CO contiene l'informativa al trattamento, la modalità di esercizio dei diritti
- I CAB possono riferire le richieste ricevute ai canali riportati nell'informativa (privacy@accredia.it o dpo@accredia.it).

**PG-31 "Gestione delle richieste degli interessati in merito all'esercizio dei diritti previsti dal Regolamento Europeo sulla Protezione dei Dati n. 2016/679".**

- GDPR richiede che vengano gestite eventuali richieste da parte di soggetti interessati al trattamento da parte del Titolare;
- Le richieste devono essere accettate in qualunque forma vengano presentate.



ACCREDIA
ENTE ITALIANO DI ACCREDITAMENTO

3

# Elenco dei documenti ACCREDIA riferito a GDPR

Punti di attenzione:

**PG-32 "Gestione delle Violazioni di dati personali"**

- GDPR richiede la gestione di eventi legati alla sicurezza dei dati personali;
- I dati personali di ACCREDIA sono gestiti sia su sistemi interni che su sistemi in gestione agli ispettori;
- Un evento di sicurezza sui dati personali di ACCREDIA, che si verifica su un dispositivo di un Ispettore, è comunque un evento che coinvolge ACCREDIA come titolare del trattamento.



ACCREDIA
ENTE ITALIANO DI ACCREDITAMENTO

4

## Punti di attenzione relativi alla sicurezza

I laboratori lavorano come struttura autonome; in ragione di questo utilizzano per l'attività dispositivi propri (endpoint).

Quali sono i rischi principali per gli endpoint?

- **Malware**: Software malevolo progettato per compromettere la sicurezza dell'endpoint.
- **Phishing**: Attacchi tramite e-mail o link che rubano credenziali o installano malware.
- **Ransomware**: Blocca l'accesso ai dati finché non viene pagato un riscatto.
- **Accesso non autorizzato**: Uso improprio di credenziali o vulnerabilità nei sistemi.
- **Minacce IoT**: Dispositivi non protetti possono diventare punti di ingresso.



ACCREDIA
ENTE ITALIANO DI ACCREDITAMENTO

5

## Punti di attenzione relativi alla sicurezza

Quali sono le conseguenze dei rischi sugli endpoint?

- **Perdita di dati sensibili**: Furto di informazioni personali o lavorativi (di ACCREDIA o dei Laboratori). Violazioni degli impegni alla riservatezza.
- **Interruzione delle operazioni**: Arresto della produttività per attacchi o malfunzionamenti.
- **Danni reputazionali**: Clienti e partner perdono fiducia.
- **Costi elevati**: Riscatti, ripristino dei sistemi e sanzioni legali.



ACCREDIA
ENTE ITALIANO DI ACCREDITAMENTO

6

## Punti di attenzione relativi alla sicurezza

Come proteggere gli endpoint?

- **Software di sicurezza aggiornato:** Antivirus, firewall e strumenti EDR (Endpoint Detection and Response).
- **Aggiornamenti regolari:** Installare patch per correggere le vulnerabilità.
- **Formazione degli utenti:** Sensibilizzare su phishing e comportamenti sicuri online.
- **Gestione degli accessi:** Utilizzo di autenticazione multi-fattore (MFA).
- **Backup continuo  dei dati**: Garantire l'integrità dei dati mediante soluzione di backup continuo in cloud.
- **Monitoraggio continuo**: Rilevare e rispondere rapidamente alle minacce.



ACCREDIA
ENTE ITALIANO DI ACCREDITAMENTO

7

## Punti di attenzione relativi alla sicurezza

I Laboratori lavorano come strutture autonome; in ragione di questo utilizzano per l'attività dispositivi propri (endpoint).

Strumenti che non costituiscono cyber rischi ma che possono portare a violazioni di dati personali:

- **AI;**
- **Generatori online di documento di testo a partire da PDF;**
- **Servizi online di analisi di documenti per varie finalità;**
- **Connessione a servizi wi-fi pubblici.**



ACCREDIA
ENTE ITALIANO DI ACCREDITAMENTO

8

ACCREDIA
ENTE ITALIANO DI ACCREDITAMENTO

## Grazie per aver partecipato!

9