Successivamente l'Italia, attraverso il d.lgs. 101/2018 art. 2 septiesdecies, ha identificato nell'organismo nazionale di accreditamento (Accredia) designato in virtù del regolamento (CE) 765/2008, il soggetto che dovrà effettuare l'accreditamento pur rimanendo al Garante il potere di accreditare direttamente in alcune materie specifiche (es. Biometria, genetica, ecc.) o lì dove l'Ente di accreditamento risulti inadempiente.

5.8.4 Best practices per il trattamento dei dati personali

- **Ridurre al minimo i dati personali utilizzati -** *Ridurre l'impatto dei rischi limitando la gestione dei dati personali a ciò che è strettamente necessario per raggiungere lo scopo definito.*
  - Comprovare che i dati personali siano sufficienti, pertinenti e non eccessivi rispetto all'intento; diversamente, non raccoglierli.
  - Comprovare che i dati personali non rivelino (direttamente o indirettamente) l'origine razziale o etnica, le opinioni politiche, filosofiche o religiose, l'appartenenza sindacale, le informazioni sulla salute o le informazioni sulla vita sessuale di un individuo, tranne che per circostanze eccezionali.
  - Comprovare che i dati personali non si riferiscano a reati, sentenze penali o misure di sicurezza.
  - Evitare la raccolta di dati personali aggiuntivi.
  - Limitare la trasmissione di documenti elettronici contenenti dati personali allo stretto necessario.
  - Eliminare in caso di necessità se non più utili, i dati personali o le richieste di un soggetto dal sistema in esercizio o dai backup.
- **Gestire i periodi di conservazione dei dati personali -** *Ridurre l'impatto dei rischi assicurando che i dati personali non vengano mantenuti per più di quanto necessario.*
  - Definire periodi di conservazione dei dati personali limitati nel tempo e appropriati allo scopo dell'elaborazione.
  - Verificare che l'elaborazione possa rilevare la scadenza del periodo di conservazione.
  - Verificare che l'elaborazione consenta la cancellazione dei dati personali a scadenza del periodo di conservazione e che il metodo scelto per l'eliminazione sia appropriato ai rischi legati alla libertà civile e alla privacy dei soggetti interessati.
  - Eliminare immediatamente i dati personali quando il periodo di conservazione scade.
- **Informare i soggetti e ottenere il consenso -** *Consentire ai soggetti interessati di effettuare una scelta libera, specifica e informata.*
  - Determinare se l'elaborazione si basa su una base giuridica diversa dal consenso.
  - Determinare i mezzi pratici da attuare per ottenere il consenso degli interessati.
  - Assicurare che il consenso sia ottenuto prima che inizi l'elaborazione.
  - Assicurare che il consenso sia ottenuto liberamente.
  - Assicurare che il consenso sia ottenuto in modo notificato e trasparente in termini di finalità del trattamento.
  - Assicurare che il consenso sia ottenuto per uno scopo specifico.
- **Partizionare i dati personali -** *Ridurre la possibilità che i dati personali possano essere correlati e che possa verificarsi una violazione di questi***.**
  - Identificare i dati personali utili solo al singolo processo (l'identificazione deve essere svolta per ciascun processo dell'organizzazione).
  - Separare in modo logico i dati utili di ciascun processo.
  - Comprovare regolarmente che i dati personali siano partizionati in modo efficace e che i destinatari e le interconnessioni non siano correlabili ai dati stessi.
- **Cifrare i dati personali -** *Rendere incomprensibili i dati personali a chiunque non sia autorizzato all' accesso.*
  - Determinare tutto ciò che deve essere crittografato (inclusi dischi rigidi, file, dati provenienti da un database o canali di comunicazione) in base alla forma in cui sono memorizzati i dati personali, i rischi individuati e le prestazioni richieste.