AVVERA

2024 gennaio NEWSLETTER

AVVERA

SEDE LEGALE E OPERATIVA
20146 MILANO
VIA SARDEGNA, 21

SEDE OPERATIVA CERTIFICATA
21040 ORIGGIO (VA)
LARGO UMBERTO BOCCIONI, 1

ALTRE SEDI
61211 PESARO (PU)
VIA GIASONE DEL MAINO, 13
33100 UDINE (UD)
VIA G. TULLIO, 22

TELEFONO
+39 0296515401

FAX
0296515499

C.F./P.IVA 06047090961
CAP. SOC. 300.000 EURO I.V.
REG. IMPO. MI
06047090961
REA 1866500

WWW.AVVERA.IT
AVVERA@LEGALMAIL.IT

C.F./P.IVA 06047090961
CAP. SOC. 300.000 EURO I.V.
REG. IMPO. MI
06047090961
REA 1866500

WWW.AVVERA.IT
AVVERA@LEGALMAIL.IT

CSQ ISO 9001 CSQ ISO 45001 CSQ ISO/IEC 27001

01

CNIL E LA BOZZA DI GUIDA PRATICA PER LA REDAZIONE DELLA TIA

In data 8 Gennaio 2024, il Garante francese per la protezione dei dati personali (CNIL) ha pubblicato una bozza di "Guida Pratica" per la redazione del documento di assessment di impatto durante i trasferimenti in Paesi terzi (c.d. "TIA"), invitando ad effettuare commenti pubblici sulla stessa bozza, entro il 12 Febbraio 2024.

Il CNIL avrebbe redatto la Guida Pratica seguendo le Raccomandazioni 01/2020 dell'European Data Protection Board (EDPB) relative "alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE", adottate il 18 Giugno 2021, con lo scopo di supportare l'attività redazionale della TIA per gli esportatori di dati personali.

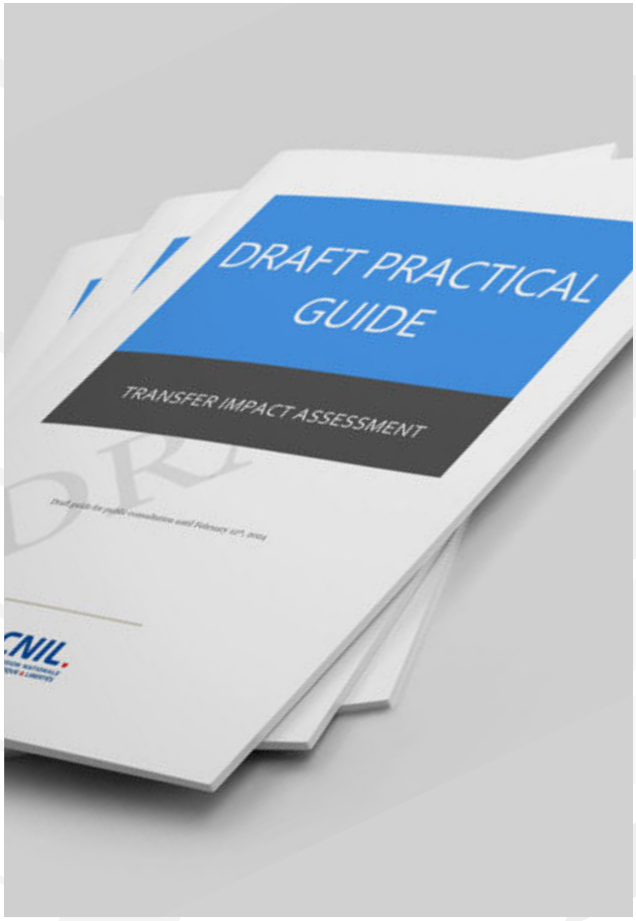
La Guida Pratica include una prima parte di metodologia per la redazione del documento, e una seconda parte di compilazione che prende in considerazione gli elementi essenziali per la redazione di una TIA, seguendo il sistema a "sei passi" come definito nelle Raccomandazioni 01/2020 dell'EDPB. L'uso di questa Guida Pratica non è obbligatorio, in quanto è possibile affidarsi a differenti metodologie che considerando ulteriori elementi, tuttavia è da considerarsi di buon supporto per identificare gli elementi più importanti per effettuare la valutazione di impatto sul trasferimento di dati personali e assicurarsi che il livello di protezione nel Paese Terzo destinatario sia sufficiente.

La Guida Pratica è organizzata secondo i seguenti punti:

- **Descrizione delle caratteristiche del trasferimento**
- **Descrizione degli strumenti utilizzati per il trasferimento**
- **Valutazione della normativa e delle consuetudini del Paese terzo di destinazione, con la valutazione dell'efficacia degli strumenti utilizzati**
- **Identificazione e adozione delle misure di sicurezza supplementari**
- **Implementazione delle misure di sicurezza supplementari e delle necessarie procedure adottate**
- **Rivalutazione a intervalli appropriati e vigilanza sui potenziali sviluppi che potrebbero impattare sulla natura del trasferimento verso il Paese Terzo destinatario**

Si rilevano alcune differenze rispetto alla metodologia di TIA predisposta dal Garante inglese per la protezione dei dati personali (ICO), disponibile sul proprio sito dalla fine del 2022. La metodologia del CNIL sembra essere applicabile più agevolmente, a prescindere da qualsiasi realtà (grande o piccola), tenendo in maggiore considerazione il livello di trasparenza della legislazione del Paese terzo destinatario, l'applicabilità delle regole democratiche a tutela degli interessati e le misure di sicurezza, tecniche, contrattuali ed organizzative, applicate o comunque da applicare. Inoltre, sono state predisposte delle sezioni apposite per responsabilizzare le persone incaricate di verificare l'applicabilità delle misure di sicurezza e programmare future rivalutazioni.

La metodologia dell'ICO, invece, sembra essere maggiormente strutturata verso un'analisi tecnica di valutazione del rischio, assegnando alle varie categorie di dati personali un valore di rischio (basso, medio oppure alto), rilevando quai diritti fondamentali possano essere a rischio di violazione durante il trasferimento/trattamento e verificando che l'importatore possa essere soggetto a decisioni della corte giurisdizionale (o di arbitrato) provenienti dal Regno Unito.



02

IL REGISTRO DELLE OPPOSIZIONI E IL SERVIZIO WEB DI CONSULTAZIONE AUTOMATICA

È stato recentemente rilasciato il servizio web per la consultazione del Registro pubblico delle opposizioni da parte degli Operatori registrati, tramite l'invio automatico delle liste di numerazioni telefoniche da verificare con il RPO Telefonico e quello Postale, attivabile tramite l'Area riservata, con il profilo del referente amministrativo e presentando un'apposita richiesta.

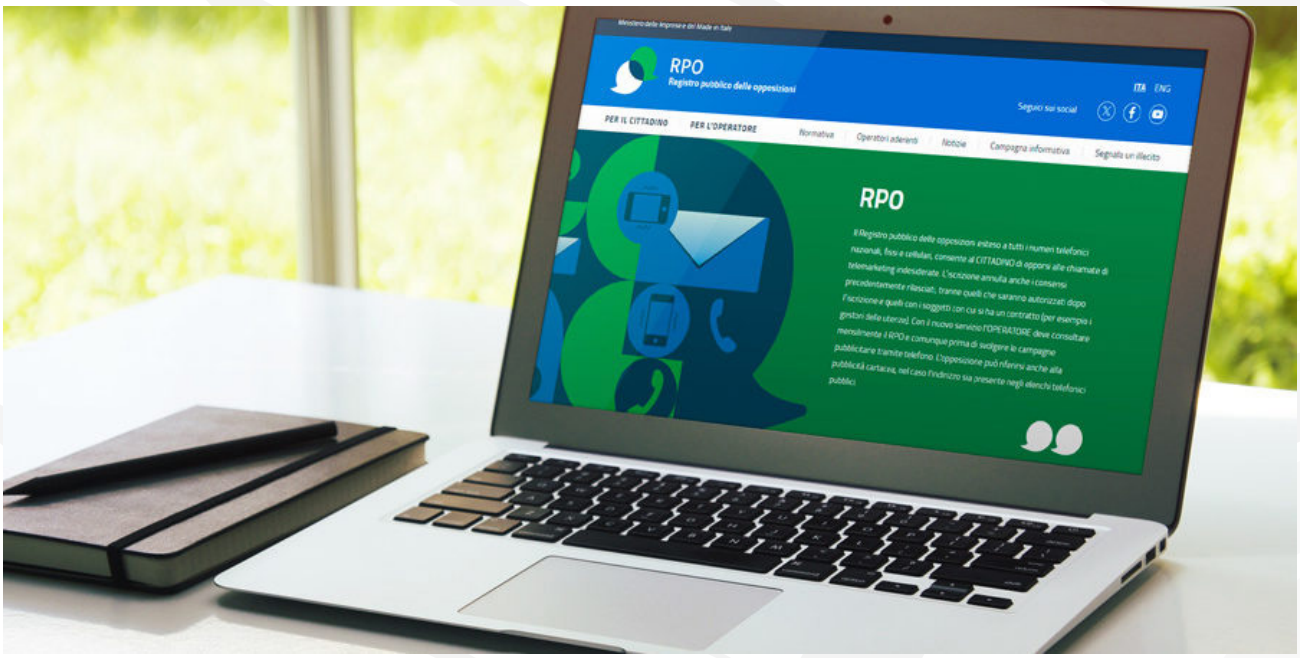
Questo servizio permette agli Operatori di inviare le liste di contatti da verificare e ottenere i risultati aggiornati, senza che sia necessario l'intervento di un operatore umano, permettendo permette l'interoperabilità tra le piattaforme software degli operatori e il sistema del RPO.

È disponibile anche un ambiente di test del servizio per l'invio delle liste. Per accedere all'ambiente di test, l'Operatore deve:

- presentare un'apposita richiesta, indicando la propria ragione sociale e un indirizzo email/PEC per ricevere le credenziali di accesso e le notifiche del servizio, all'indirizzo info.operatori@registrodelleopposizioni.it;
- disporre delle summenzionate credenziali di accesso;
- caricare un certificato digitale lato client, emesso da un'Autorità Certificativa riconosciuta

In fase di accesso all'ambiente di test viene verificata la disponibilità nel client di un certificato digitale secondo le specifiche menzionate, mentre non vengono effettuati controlli sul contenuto dello stesso, che saranno invece attuati in produzione. Anche sulle liste inviate saranno effettuate verifiche sul formato del file, ma non sul loro contenuto.

Lo stato delle liste inserite nell'ambiente di test viene aggiornato automaticamente dal sistema, e alla fine del processo dovrebbe essere restituito un file non correlato ai dati della lista sottomessa.



03

IL GARANTE SPAGNOLO E IL TRATTAMENTO DEI DATI BIOMETRICI NELL'AMBITO LAVORATIVO

In data 23 Novembre 2023, il Garante spagnolo per la protezione dei dati personali ha pubblicato un documento di "Linee Guide" per il trattamento dei dati biometrici durante il controllo delle presenze e l'accesso ai locali, sia durante l'ambito lavorativo che non lavorativo.

Il controllo degli orari e delle presenze è un trattamento che può essere utilizzato per il raggiungimento di diverse finalità ed è soggetto al rispetto della normativa in materia di protezione dei dati personali, fatte salve le specificità della normativa da applicare in ciascun caso. Da un lato, la registrazione delle ore di lavoro è un trattamento che può essere inquadrato all'interno di un rapporto di lavoro, con lo scopo di controllarne l'esecuzione. Dall'altro lato, il controllo delle presenze sarebbe legato allo scopo di sorvegliare l'ingresso e/o l'uscita da determinati locali. Quest'ultimo può essere effettuato o meno nell'ambito del lavoro.

I sistemi di trattamento dei dati biometrici si basano sulla raccolta e sul trattamento di dati personali relativi alle caratteristiche fisiche, fisiologiche o comportamentali delle persone fisiche (comprese le loro caratteristiche neurali), mediante dispositivi o sensori, creando "modelli biometrici" che consentono l'identificazione, il tracciamento o la profilazione di tali persone. Identificare una persona significa determinarne l'identità, direttamente o indirettamente, quindi l'assegnazione di un identificatore è un processo che permette di individuare un individuo e le azioni a lui destinate. Il Garante spagnolo considera il trattamento dei dati biometrici di rischio elevato, sia per le finalità di identificazione che di accesso, in quanto sono inclusi dati particolari, quindi si rende necessario rispettare i requisiti dell'art. 35 GDPR.

L'art. 9, par. 1 GDPR stabilisce una regola generale che vieta il trattamento dei dati personali che rivelano quelle che definisce "categorie particolari di dati personali", tuttavia disciplina che debba sussistere una condizione di legittimità per effettuare il trattamento dei dati particolari. Affinché la deroga dell'art. 9, par. 2, lett. b) GDPR (diritti specifici del Titolare del trattamento in materia di diritto del lavoro) possa trovare applicazione, il Garante spagnolo rileva che debba sussistere una legge che autorizzi specificatamente l'uso dei dati biometrici per la registrazione degli orari e il controllo degli accessi durante l'ambito lavorativo.

Relativamente alla deroga dell'art. 9, par. 2, lett. a) GDPR (consenso dell'interessato), il Garante spagnolo rileva che il consenso non si applica al trattamento della registrazione dell'orario di lavoro in sé, dove non è possibile opporsi, ma ai dati biometrici aggiuntivi, ma potrebbe non rappresentare una valida e lecita circostanza se si considera l'effettiva libertà del consenso. Il Considerando 43 del GDPR stabilisce che per ***"assicurare la libertà di prestare il consenso, è opportuno che il consenso non costituisca un valido fondamento giuridico per il trattamento dei dati personali [..], qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento".***

Anche le Linee Guida 5/2020 dell'EDPB (sul consenso ai sensi del GDPR) rilevano che nel contesto dei rapporti di lavoro esiste uno squilibrio di potere tra dipendente e datore di lavoro, con l'implicazione che tale consenso non potrebbe essere fornito liberamente. L'EDPB, comunque, non esclude che i datori di lavoro possano fare affidamento al consenso come base legittima per il trattamento, in quanto ci possono essere situazioni in cui è possibile per il datore di lavoro dimostrare che il consenso è stato effettivamente dato liberamente, e che la negazione del consenso non comporti delle conseguenze negative.

Ad esempio, nel caso della registrazione dell'orario di lavoro, poiché l'interessato ha l'obbligo di registrare la propria giornata lavorativa, l'esistenza di un libero consenso al trattamento aggiuntivo dei dati biometrici potrebbe essere considerata solo se l'interessato ha una reale alternativa per adempiere a tale obbligo. Tuttavia, per quanto riguarda il requisito delle possibili "opzioni equivalenti", occorre tenere presente che, se esistono alternative al trattamento dei dati biometrici che comportano un rischio minore per i diritti e le libertà delle persone, che consentono a tutti i lavoratori di optare per altre alternative in qualsiasi momento, significa che il trattamento dei dati biometrici **non è più necessario** per l'attuazione del trattamento, facendo venir meno il requisito di necessità, necessario per i trattamenti con rischio elevato (art. 35, par. 7, lett. b) GDPR).

Considerando, invece, le situazioni in cui il controllo degli accessi è effettuato per finalità diverse dall'ambito lavorativo, l'unica base giuridica giustificabile sarebbe il consenso libero, specifico, informato e inequivocabile (art. 9, par. 2, lett. a) GDPR. Anche in questo caso, il Titolare del trattamento dovrebbe stabilire una modalità alternativa per poter effettuare il trattamento di dati per quella medesima finalità, senza che vi siano conseguenze negative per la persona che non desidera il trattamento dei dati biometrici.

Anche in questo caso, occorre dimostrare la necessità e proporzionalità oggettiva (requisito per il trattamento a rischio elevato) e le possibili alternative, in modo tale che per poter trattare tali dati biometrici non vi siano altre alternative che servano a soddisfare l'esigenza individuata e che comportino un rischio minore per i diritti e le libertà delle persone fisiche.

Bisogna anche considerare i vincoli al trattamento dei dati biometrici, quando gli interessati sono sottoposti a decisioni basate unicamente sul trattamento automatizzato che produca effetti giuridici oppure incidano in modo analogo significatamene sulla propria persona (con riferimento all'art. 22, par. 1 GDPR).

In ogni caso vi sia un trattamento di dati biometrici, il Garante spagnolo ritiene che la redazione di una valutazione d'impatto sulla protezione dei dati (art. 35 GDPR) sia un elemento essenziale, da redigere prima che venga svolta l'attività, fornendo le evidenze necessarie per dimostrare che sussistano i requisiti di idoneità, necessità e proporzionalità per effettuare il trattamento.

Infine, il Garante spagnolo fornisce una serie di misure necessarie affinché vi sia una totale conformità ai principi normativi del GDPR:

- Implementazione della protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 GDPR);
- Minimizzazione della raccolta di informazioni biometriche tecniche, con una valutazione oggettiva per stabilire se vengono raccolti dati eccessivi ai fini del trattamento;
- Informazione agli interessati delle caratteristiche del trattamento biometrico, in particolare dell'elevato rischio intrinseco (art. 13 GDPR);
- Implementazione della funzione di mantenere scollegati il modello biometrico e l'identità della persona fisica, per il controllo degli accessi;
- Adozione di adeguate misure di sicurezza per garantire che i modelli biometrici non possano essere utilizzati per altre finalità;
- Ricorso a soluzioni di crittografia dei dati, per proteggere la riservatezza, la disponibilità e l'integrità del modello biometrico;
- Adozione di tecnologie o formattazioni di dati mirate ad impedire l'interconnessione delle banche dati biometriche e la divulgazione non verificata dei dati;
- Cancellazione dei dati biometrici quando non sono correlati alla finalità per cui sono trattati.

A V V E R A

SEDE LEGALE E OPERATIVA
20146 MILANO
VIA SARDEGNA, 21

SEDE OPERATIVA CERTIFICATA
21040 ORIGGIO (VA)
LARGO UMBERTO BOCCIONI, 1

ALTRE SEDI
61211 PESARO (PU)
VIA GIASONE DEL MAINO, 13
33100 UDINE (UD)
VIA G. TULLIO, 22

TELEFONO
+39 0296515401

FAX
0296515499

C.F./P.IVA 06047090961
CAP. SOC. 300.000 EURO I.V.
REG. IMPO. MI
06047090961
REA 1866500

WWW.AVVERA.IT
AVVERA@LEGALMAIL.IT

C.F./P.IVA 06047090961
CAP. SOC. 300.000 EURO I.V.
REG. IMPO. MI
06047090961
REA 1866500

WWW.AVVERA.IT
AVVERA@LEGALMAIL.IT

CSQ ISO 9001 CSQ ISO 45001 CSQ ISO/IEC 27001