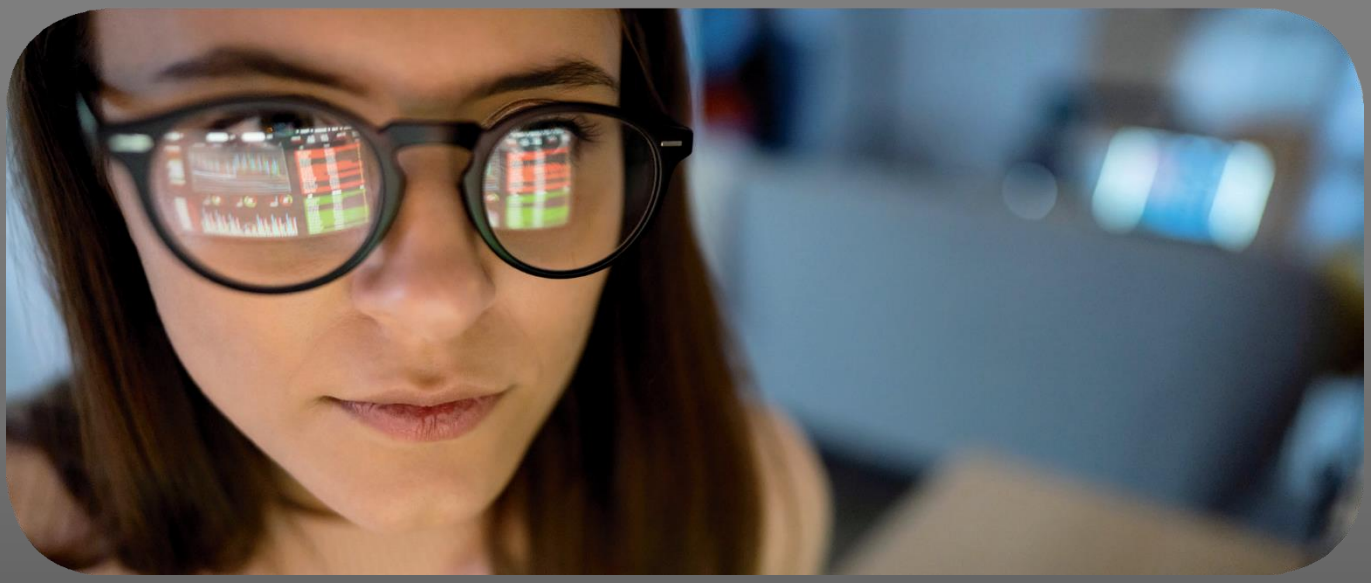
Stiftung
Familienunternehmen

# Oneri normativi e finanziari della legislazione UE in quattro Stati membri: uno studio comparato

## Vol. 4: Oneri dovuti sulla base degli artt. 30 e 33 del Regolamento generale sulla protezione dei dati



**Estratto con sintesi dei risultati principali dello studio** (***in lingua italiana***)

**Per accedere alla versione completa dello studio** (***in lingua inglese***)

# Sintesi dei risultati più significativi

## I principali risultati dell'analisi giuridica (CEP e Alerion)

1. La parte A di questo studio confronta gli oneri normativi relativi alla conformità con due articoli del Regolamento generale sulla protezione dei dati (GDPR) in Austria, Francia, Germania e Italia. Lo studio si concentra sui requisiti giuridici e amministrativi relativi a:
   - lacreazione e la tenuta di un registro delle attività di trattamento ai sensi dell'art. 30 del GDPR
   - irequisiti relativi alla notifica delle violazioni dei dati personali all'autorità di controllo competente ai sensi dell'art. 33 del GDPR.
2. L'articolo 30 del GDPR impone ai titolari e ai responsabili del trattamento dei dati personali di tenere un registro delle attività di trattamento (VVT) con una serie di dettagli sui dati trattati dall'azienda, tra cui
   - il nome e i dati di contatto del responsabile del trattamento,
   - le finalità del trattamento,
   - una descrizione delle categorie di dati trattati e delle categorie di interessati,
   - le categorie di destinatari a cui tali dati sono comunicati,
   - l'indicazione se i dati sono trasferiti a un paese terzo, e
   - ove possibile, i termini per la cancellazione dei dati e una descrizione generale delle misure tecniche e organizzative adottate dall'azienda in relazione ai dati.
3. Poiché le informazioni di cui sopra devono essere fornite per ogni "attività di trattamento", la portata del Registro delle attività di trattamento dipende dalla comprensione del termine "attività di trattamento". Tuttavia, questo termine non è definito nel GDPR. Mentre le autorità di protezione dei dati austriache e italiane non forniscono alcun supporto in merito, le linee guida delle autorità di protezione dei dati francesi e tedesche[1] indicano che non è necessario elencare ogni singola operazione di trattamento nel Registro delle attività di trattamento, ma che

*Nessuna definizione di "attività di trattamento" nell'art. 30 del GDPR.*

1 Il controllo della protezione dei dati in Germania è strutturato a livello federale. È composta dalle autorità per la protezione dei dati del governo federale e dei 16 Länder. Nella misura in cui le Autorità per la protezione dei dati dei Länder appaiono come autorità competenti, questo studio si basa sui modelli e sulle linee guida fornite dal Commissario di Stato per la protezione dei dati e la libertà d'informazione (LfDI) del Baden-Württemberg..

in una certa misura possono essere astratti. Tuttavia, il livello di astrazione non è del tutto chiaro.

4. La quantità di indicazioni e di supporto fornite sui siti web delle autorità nazionali per la protezione dei dati in relazione alla creazione di un Registro delle attività di trattamento differisce in modo significativo nel confronto tra i quattro Stati membri esaminati. Mentre l'autorità austriaca per la protezione dei dati non fornisce un modello e solo poche informazioni sugli obblighi relativi alla creazione di un Registro delle attività di trattamento, le indicazioni e il supporto delle altre autorità sono molto più completi.

5. Mentre il GDPR elenca le informazioni richieste nel Registro delle attività di trattamento senza specificarle, i modelli ufficiali forniti dalle autorità nazionali per la protezione dei dati si discostano in parte da esso. Ad esempio, a differenza dell'Austria (dove non viene fornito alcun template ufficiale) e dell'Italia, i modelli forniti da Germania e Francia elencano chiaramente i dati di contatto esatti che devono essere forniti. Anche se un modello più completo sembra essere più oneroso, è più chiaro per la persona responsabile quale sia la portata delle informazioni richieste.

6. alcuni Stati membri hanno richiesto di fornire informazioni aggiuntive nel Registro delle attività di trattamento, che possono essere considerate come un aggiornamento delle informazioni aggiuntive, ma questo aggiornamento è marginale.

7. l'onere burocratico relativo alla creazione di un Registro delle attività di trattamento dipende anche dalla disponibilità e dalla facilità d'uso dei modelli ufficiali forniti dalle autorità competenti per la protezione dei dati.

8. L'esenzione delle piccole imprese con meno di 250 dipendenti dall'obbligo di tenere un Registro delle attività di trattamento di cui all'art. 30 (5) del GDPR è in gran parte inutile. Poiché le restrizioni sono definite in modo ampio, l'esenzione si applica solo raramente.

*L'esenzione per le piccole imprese si applica raramente.*

9. Sulla base di quanto sopra, formuliamo le seguenti raccomandazioni: L'onere burocratico potrebbe essere ridotto fornendo modelli ufficiali migliori per un Registro delle attività di trattamento che soddisfino i seguenti criteri:

*Potenziale per semplificazione e miglioramento*

   - Sono armonizzati e tradotti nelle rispettive lingue nazionali.
   - Combinano i vantaggi dei modelli esistenti delle autorità nazionali per la protezione dei dati, ad es.,
     - che siano strutturati in modo chiaro,
     - siano autoesplicativi o contengano link diretti a fonti dove vengono fornite ulteriori informazioni e
     - che contengano caselle di spunta almeno per le informazioni più importanti o, preferibilmente, menu a tendina (come il modello dell'autorità francese per la protezione dei dati).

- Forniscono maggiore supporto alle piccole e medie imprese sulle modalità di preparazione di un Registro delle attività di trattamento semplificato.

10. L'articolo 33 del GDPR obbliga i responsabili del trattamento a registrare le violazioni dei dati personali e a notificare le violazioni specifiche all'autorità competente per la protezione dei dati. La notifica deve essere effettuata "senza indebito ritardo" e "ove possibile" entro 72 ore dal momento in cui la violazione è "divenuta nota" al responsabile del trattamento.

11. Il GDPR definisce "violazione dei dati personali" una violazione della sicurezza che comporta, accidentalmente o illegalmente, la distruzione, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o altrimenti trattati.

Ai sensi dell'art. 33 del GDPR, la notifica deve contenere almeno le seguenti informazioni:

- descrizione della natura della violazione dei dati personali;
- il nome e i dati di contatto del responsabile della protezione dei dati o di un altro punto di contatto per ulteriori informazioni;
- una descrizione delle probabili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o proposte dal responsabile del trattamento per far fronte alla violazione dei dati personali.

12. Inoltre, Francia, Germania[2] e Italia chiedono alcune informazioni che non sono richieste dal GDPR. Ad esempio, Francia e Italia chiedono, tra le altre cose, le misure adottate prima della violazione dei dati e la stima della gravità. Riteniamo che questi requisiti siano una sorta di *"goldplating*".

*Francia, Germania e Italia richiedono un "goldplating"*

13. È interessante notare che non tutti i moduli di notifica richiedono tutte le informazioni richieste dall'articolo 33 del GDPR. Ad esempio, il modulo di notifica online tedesco non richiede il nome e i dati di contatto del responsabile della protezione dei dati.

14. Nel complesso, le informazioni da presentare nella notifica variano notevolmente in termini di livello di accuratezza. Il modulo austriaco è quello che richiede meno informazioni, seguito da quelli tedesco, francese e italiano. Tuttavia, va anche considerato che il modulo italiano utilizza principalmente caselle da spuntare, a differenza delle informazioni richieste nei moduli austriaco e tedesco,

2 Per la Germania, è stato analizzato il modulo di rendicontazione dell'LfDI Baden-Württemberg.

che prevedono principalmente campi di testo aperti. Sebbene l'Italia richieda più informazioni rispetto agli altri tre Stati membri, vi sono anche riferimenti ad alcuni aspetti che non vengono approfonditi negli altri Stati membri, come ad esempio in relazione alle misure adottate o proposte dal responsabile del trattamento per affrontare la violazione dei dati personali.

15. Sulla base di quanto sopra esposto, formuliamo le seguenti raccomandazioni:
    - Gli Stati membri devono astenersi dal richiedere informazioni che non sono richieste dal GDPR; e
    - I moduli di segnalazione dovrebbero essere resi più facili da usare, ad esempio utilizzando caselle da spuntare invece di campi di testo aperti.

*Si raccomanda di rinunciare al "gold plating" e di utilizzare moduli di segnalazione di facile utilizzo.*

## I principali risultati della valutazione degli oneri normativi (Stime AG e CSIL)

### Procedura

1. La parte B di questo studio confronta gli oneri normativi associati all'attuazione degli articoli 30 e 33 del **Regolamento generale sulla protezione dei dati** (GDPR) in quattro Stati membri dell'UE utilizzando il concetto di costi di conformità. La valutazione empirica è stata effettuata sulla base di un totale di 67 interviste approfondite condotte con aziende ed esperti in tutti e quattro gli Stati membri.

### Gestione corrente

2. **L'articolo 30 del GDPR impone alle aziende di registrare tutte le attività di trattamento dei dati personali in un registro delle attività di trattamento**. In caso di violazione dei dati, le aziende sono obbligate, ai sensi dell'articolo 33, a informare l'autorità di vigilanza entro 72 ore. Tutte le aziende esaminate, eccetto una, avevano attuato i requisiti degli articoli 30 e 33.
3. **In pratica,le aziende non possono avvalersi dell'esenzione per le piccole e medie imprese** ai sensi dell'articolo 30 (5), poiché praticamente tutte le aziende trattano categorie speciali di dati personali ai sensi dell'articolo 9 (1) (ad esempio, la contabilità delle retribuzioni) e sono quindi obbligate a creare e mantenere un registro delle attività di trattamento.
4. **La notifica ai sensi dell'art. 33 può essere effettuata in forma digitale.** In Francia e in Italia, la notifica deve essere inviata all'autorità tramite un modulo elettronico, in Austria per posta o per e-mail e in Germania - a seconda delle disposizioni delle autorità di protezione dei dati dei singoli Stati federali - spesso come modulo elettronico e in alternativa per e-mail o per telefono.

5. **L'attuazione e il rispetto degli artt. 30 e 33 comportano notevoli oneri per le imprese .**Nello studio comparativo non sono state riscontrate differenze tra i vari Paesi per quanto riguarda gli oneri imposti. Gli oneri corrispondono piuttosto alle dimensioni dell'azienda e al numero di attività di trattamento.

6. **A causa dell'insufficiente definizione dei termini giuridici, le aziende fanno molto affidamento sulle informazioni ufficiali e sui modelli per conformarsi all'articolo 30 del GDPR.** Poiché il termine "attività di trattamento" non è definito nel GDPR, ma è inclusa solo una definizione molto ampia di "trattamento", ossia qualsiasi operazione effettuata in relazione ai dati personali, le aziende in tutti gli Stati membri hanno utilizzato modelli forniti dalle autorità pubbliche, da consulenti o - in rari casi - dalle aziende stesse.

*Le incertezze dovute a termini giuridici non adeguatamente definiti modellano la prassi aziendale.*

7. **Le disposizioni dell'art. 30 del GDPR interessano in particolare le grandi e le microimprese.** Le microimprese spesso non dispongono di risorse e/o competenze sufficienti e sono quindi particolarmente dipendenti da fornitori di servizi esterni, il che comporta costi aggiuntivi. D'altra parte, le grandi imprese hanno spesso modelli di business più complessi che lavorano con i dati personali.

8. **Lo studio mostra l'ampio ricorso a consulenze esterne per integrare le misure interne**. Le competenze esterne erano necessarie per garantire una conformità tempestiva e appropriata, evitando al contempo sanzioni e danni all'immagine del marchio delle aziende.

9. **Le aziende con modelli di business B2C devono affrontare oneri significativi a causa dell'articolo 30 del GDPR**, poiché in questo caso si verifica un numero particolarmente elevato di attività di trattamento.

10. **La manutenzione e l'aggiornamento del registro delle attività di trattamento comportano una spesa annuale considerevole, che viene percepita come un onere significativo.** Le aziende spendono in media un'ora all'anno per ogni attività di lavorazione per mantenere le informazioni contenute nel registro delle attività di trattamento. Non sono state riscontrate differenze nel confronto tra i Paesi. Ad esempio, i costi di conformità dipendono dalle dimensioni dell'azienda e dal registro delle attività di trattamento, variando da 30 a 40 ore per le micro e piccole imprese e da 92 a 297 ore per le medie e grandi imprese. La maggioranza ha sottolineato che il registro delle attività di trattamentoviene utilizzato esclusivamente a fini di conformità. Di conseguenza, l'impegno richiesto per mantenerlo e aggiornarlo è percepito come un onere particolare.

*La manutenzione e l'aggiornamento del registro delle attività di trattamento non presentano differenze specifiche per ogni Paese; tuttavia, questo lavoro comporta costi considerevoli.*

11. **Quando si segnalano le violazioni della protezione dei dati, la maggior parte del tempo e dell'impegno richiesto dalle aziende è dedicato ai processi interni e alla valutazione del rischio.** Il responsabile della protezione dei dati deve essere informato dell'incidente, deve effettuare una valutazione del rischio e decidere se l'incidente deve essere segnalato all'autorità.

Poiché i rischi non possono essere determinati con precisione, sono spesso associati a un elevato sforzo di valutazione, che viene percepito come un onere.

12. **L'implementazione del processo di *reporting* non rappresenta un particolare onere, ad eccezione della Francia**. Il modulo online in Francia è un onere perché mancano l'orientamento dell'~~utente~~ ~~e una buona~~ "user experience" (ad esempio, attraverso un'interfaccia utente intuitiva, istruzioni chiare e la possibilità di salvare le voci ricorrenti). Ad esempio, non è possibile salvare le voci per un uso successivo o tornare alle pagine precedenti per le correzioni. I portali online esistono anche in Italia e in alcuni Länder tedeschi, ma non sono stati citati come un onere. Per il resto, le segnalazioni avvengono via e-mail o tramite moduli predefiniti da inviare alle autorità. In Austria esiste l'obbligo di utilizzare il modulo prescritto.

**Proposte per ridurre gli oneri amministrativi**

13. **Definizioni più precise di termini giuridici indeterminati.** I termini giuridici indefiniti creano incertezza, sforzi aggiuntivi e costi di consulenza. Il GDPR dovrebbe essere integrato o modificato con commenti in modo da definire chiaramente i termini utilizzati. Ciò consentirebbe anche di armonizzare e standardizzare i modelli di elenchi di attività di trattamento per tutti gli Stati membri.

14. **Applicazione della clausola di apertura per le piccole e medie imprese.** L'attuazione pratica dell'esenzione per le piccole e medie imprese ridurrebbe significativamente l'onere per le imprese. Ciò richiede una chiara definizione di quali dati soggetti a particolare protezione ai sensi dell'art. 9 (1) del GDPR possono essere trattati senza l'obbligo di istituire un registro delle attività di trattamento.

*Le PMI necessitano di maggiore certezze legali nell'uso della clausola di apertura*

15. **Migliore sostegno da parte delle autorità.** Servizi di consulenza, esempi di buone pratiche, modelli e informazioni particolarmente orientati alla pratica e che offrono quindi un valore aggiunto diretto alle aziende interessate.

16. **Procedura di notifica uniforme presso le autorità di protezione de~~i dati, che tenga~~ conto della ~~centralità~~ dell'utente, ~~di una "user~~ experience" agevole e dell'automazione.** L'attuazione amministrativa dell'art. 33 dovrebbe essere standardizzata come soluzione online per ridurre i tempi di notifica. La notifica tramite una piattaforma online automatizzata e di facile utilizzo consente di risparmiare tempo, soprattutto quando è possibile memorizzare i dati aziendali e/o recuperare casi tipici.

# Impressum

**Editore**:

Stiftung Familienunternehmen

Prinzregentenstraße 50

80538 München

Telefon:+49(0)89/127640002

Telefax:+49(0)89/127640009

E-Mail: info@familienunternehmen.de

www.familienunternehmen.de

**Parte A a cura di:**

cep

Kaiser-Joseph-Straße 266

79098 Freiburg im Breisgau

Dr.Lukas Harta,

LL.M.Dr. Anja Hoffmann

Dr. Matthias Kullas

Prof.Dr. Andrea de Petris

Alerion

137 rue del'Université

75007 Parigi

Carole Bui

Caroline Leroy-Blanvillain

Corinne Thierache

**Parte B a cura di:**

Prognos AG

Goethestraße 85

10623 Berlino

Jan Tiessen

Michael Schaaf

Jan-Felix Czichon

CSIL

Corso Monforte 15

20122 Milano

Jessica Catalano

Sara Banfi

Anthony Bovagnet