AVVERA SRL SB

NEWSLETTER 2025

AVVERA | SB Società Benefit

MARZO

LA PSEUDONIMIZZAZIONE NEL GDPR: PRIME CONSIDERAZIONI SULLE LINEE GUIDA DELL'EDPB

LA PARTECIPAZIONE DEL GARANTE AL CEF 2025 SULL'ATTUAZIONE DEL DIRITTO DI CANCELLAZIONE

DIRITTO DI ACCESSO IN PRESENZA DI TRATTAMENTI AUTOMATIZZATI

IMQ CERTIFIED QUALITY MANAGEMENT SYSTEM ISO 9001:2015

IMQ CERTIFIED INFORMATION SECURITY MANAGEMENT SYSTEM ISO/IEC 27001:2022

IMQ CERTIFIED OCCUPATIONAL HEALTH AND SAFETY MANAGEMENT SYSTEM ISO 45001:2018

LA PSEUDONIMIZZAZIONE NEL GDPR: PRIME CONSIDERAZIONI SULLE LINEE GUIDA DELL'EDPB

Il Regolamento (UE) 2016/679 (GDPR) definisce la pseudonimizzazione all'art. 4(5) come una misura che impedisce l'attribuzione diretta dei dati a un interessato specifico senza informazioni aggiuntive, le quali devono essere conservate separatamente e protette da misure di sicurezza. Questa tecnica consente di giustificare determinati trattamenti sulla base del legittimo interesse (art. 6. 1 lett. f GDPR) e non è intesa a escludere altre misure di protezione (Considerando 28 GDPR), in quanto la valutazione delle stesse è comunque rimessa al Titolare in ottica di *accountability*.

Sebbene la pseudonimizzazione non trasformi i dati personali in dati anonimi – considerando che l'attribuzione (a soggetti specifici) rimane possibile mediante l'uso di informazioni aggiuntive –, essa può rappresentare una misura particolarmente efficace per ridurre il rischio di accessi non autorizzati e minimizzare l'esposizione degli interessati a trattamenti che potrebbero avere un impatto significativo sui loro diritti e libertà. L'efficacia del presidio dipende fortemente dal cd. dominio di *pseudonimizzazione*, ossia il contesto entro cui la pseudonimizzazione impedisce l'attribuzione dei dati agli interessati, definito dal Titolare sulla base di un'analisi del rischio, con cui stabilisce misure tecniche e organizzative volte a garantire che le informazioni aggiuntive necessarie per la re-identificazione restino separate e inaccessibili; il dominio quindi può coincidere con un'unità organizzativa interna, con un singolo destinatario esterno o con un insieme di soggetti autorizzati, escludendo ogni terza parte non legittimata ad accedere ai dati.

L'efficacia della pseudonimizzazione dipende dalla capacità del Titolare di impedire che le informazioni identificative accedano al dominio o che i dati pseudonimizzati fuoriescano, un processo che richiede un controllo attento sull'accesso alle informazioni e sulle modalità di segregazione dei dati; il dominio, può essere ristretto a specifiche entità autorizzate o ampliato a soggetti che potrebbero tentare di accedere ai dati senza autorizzazione, necessita di misure di sicurezza rigide e di garanzie contrattuali atte a impedire che le informazioni aggiuntive vengano sfruttate per la re-identificazione degli interessati.

La pseudonimizzazione, in relazione alla sicurezza dei dati ai sensi dell'art. 32 GDPR, può ridurre la gravità di eventuali violazioni ed esonerare dall'obbligo di notifica in caso di violazione ex art. 34, a condizione che il Titolare, previa una corretta separazione tra i dati pseudonimizzati e le informazioni per la re-identificazione, effettui una valutazione accurata sull'effettiva mitigazione dei rischi. Tale valutazione deve considerare in particolare la possibilità che i dati possano essere ricondotti a persone specifiche.

AVVERA | SB Società Benefit

Quanto più il livello di protezione risulta adeguato, tanto minore sarà il rischio per gli interessati, fino a rendere superflua la comunicazione della violazione stessa ai sensi degli artt. 34. 1 e 34. 3 del GDPR, garantendo così un'efficace tutela della riservatezza senza compromettere la conformità normativa.

Sotto il profilo del data transfer verso i paesi terzi, l'uso della pseudonimizzazione nelle operazioni può rappresentare una misura supplementare efficace, qualora le garanzie offerte dagli strumenti di trasferimento (come le clausole contrattuali standard) risultino insufficienti a garantire un livello di protezione equivalente a quello dell'UE -a condizione che le informazioni necessarie per l'attribuzione rimangano sotto il controllo esclusivo dell'esportatore dei dati all'interno dello Spazio Economico Europeo.

La bozza delle linee guida sulla pseudonimizzazione che l'EDPB ha messo in consultazione identificano due principali classi di trasformazioni:

- algoritmi crittografici e tabelle di sostituzione (lookup tables), basata su un'analisi del rischio che consideri il contesto del trattamento e le possibili minacce alla re-identificazione.
- gestione delle chiavi crittografiche, la segregazione delle informazioni di attribuzione e il controllo degli accessi ai dati pseudonimizzati.

Mentre, per quanto concerne ulteriori profili di criticità affrontati dall'EDPB, l'analisi pone l'accento su:

- i dati pseudonimizzati degli interessati: che restano dati personali (in quanto attribuibili a una persona fisica tramite informazioni aggiuntive) e di conseguenza soggetti ai diritti previsti dal Capitolo III del GDPR. il Titolare è sempre tenuto a fornire indicazioni sulle modalità di accesso e utilizzo degli pseudonimi, comunicando i riferimenti della fonte dei dati pseudonimizzati o del soggetto responsabile della pseudonimizzazione. La ratio di tale processo è finalizzata all'effettivo esercizio dei diritti degli interessati contro l'ipotesi di cui all'art 11 GDPR, in cui il Titolare non riesca più ad identificare l'interessato (ad esempio, perché non dispone più delle informazioni necessarie, o perché non sia in grado di ottenerle in modo lecito).
- rischio di reversibilità della pseudonimizzazione: che subordina il livello di protezione alla gestione dell'ambiente in cui i dati vengono trattati, che potrebbe essere compromessa da una conservazione delle informazioni aggiuntive senza adeguate misure di sicurezza o dall'accesso di terzi non autorizzati ai dati pseudonimizzati che potrebbero combinarli con altre fonti di informazione.

Per questo motivo, l'EDPB suggerisce una valutazione continua dell'efficacia della pseudonimizzazione, integrando misure tecniche e organizzative adeguate, come la segregazione fisica e logica delle informazioni di identificazione, l'uso di strumenti crittografici robusti e la gestione controllata delle chiavi di decrittazione. Si segnala che le linee guida dell'EDPB resteranno in consultazione pubblica fino al 28 febbraio 2025, al termine del quale si attende la definizione di un quadro normativo ulteriore, in ottica di bilanciamento tra innovazione tecnologica e tutela dei diritti fondamentali.

LA PARTECIPAZIONE DEL GARANTE AL CEF 2025 SULL'ATTUAZIONE DEL DIRITTO DI CANCELLAZIONE

Con il comunicato stampa del 7 marzo 2025, il Garante per la protezione dei dati personali ha annunciato la sua partecipazione al Quadro di attuazione coordinata (Coordinated Enforcement Framework) del Comitato europeo per la protezione dei dati (EDPB), nell'ambito della propria strategia per il periodo 2024-2027, volta a razionalizzare l'applicazione e la cooperazione tra le autorità di protezione dei dati.

Al comitato parteciperanno 32 Autorità di protezione dati dello Spazio economico europeo e avrà ad oggetto l'effettiva attuazione del diritto alla cancellazione e all'oblio, ai sensi dell'art. 17 GDPR. Si rileva che il diritto alla cancellazione risulta uno dei diritti più esercitati dagli interessati e frequentemente oggetto di reclamo presso le autorità nazionali di protezione dati.

Il Garante, assieme alle altre autorità di protezione dei dati partecipanti, contatterà nel prossimo periodo una serie di titolari del trattamento, del settore pubblico e privato, appartenenti a diversi ambiti, con lo scopo di effettuare delle indagini formali oppure di accertamento dei fatti (in tal caso, il Garante potrebbe anche decidere di intraprendere ulteriori azioni di follow-up, se necessario).

Lo scopo è verificare come i titolari del trattamento gestiscono e rispondono alle richieste di cancellazione che ricevono dagli interessati e la corretta applicazione delle condizioni ed eccezioni per l'esercizio del diritto di cancellazione e oblio. I risultati di queste azioni nazionali saranno oggetto di analisi in forma aggregata per fornire informazioni più approfondite sull'argomento, consentendo follow-up mirati a livello sia nazionale che dello Spazio economico europeo.

AVVERA | SB Società Benefit

DIRITTO DI ACCESSO IN PRESENZA DI TRATTAMENTI AUTOMATIZZATI

La sentenza C-203/22 della Corte di Giustizia dell'Unione Europea (CGUE) del 27 febbraio 2025 ha affrontato un tema di grande rilevanza: il rapporto tra il diritto di accesso ai dati personali, sancito dall'articolo 15 del Regolamento UE 2016/679 (GDPR), e la tutela dei segreti commerciali, disciplinata dalla Direttiva UE 2016/943. La Corte si è pronunciata su un rinvio pregiudiziale sollevato dal Tribunale Amministrativo di Vienna, fornendo un'interpretazione chiara sui requisiti sostanziali delle "informazioni significative" che devono essere comunicate all'interessato quando è sottoposto a **trattamenti automatizzati**, inclusa la profilazione e il cosiddetto "*scoring*" creditizio.

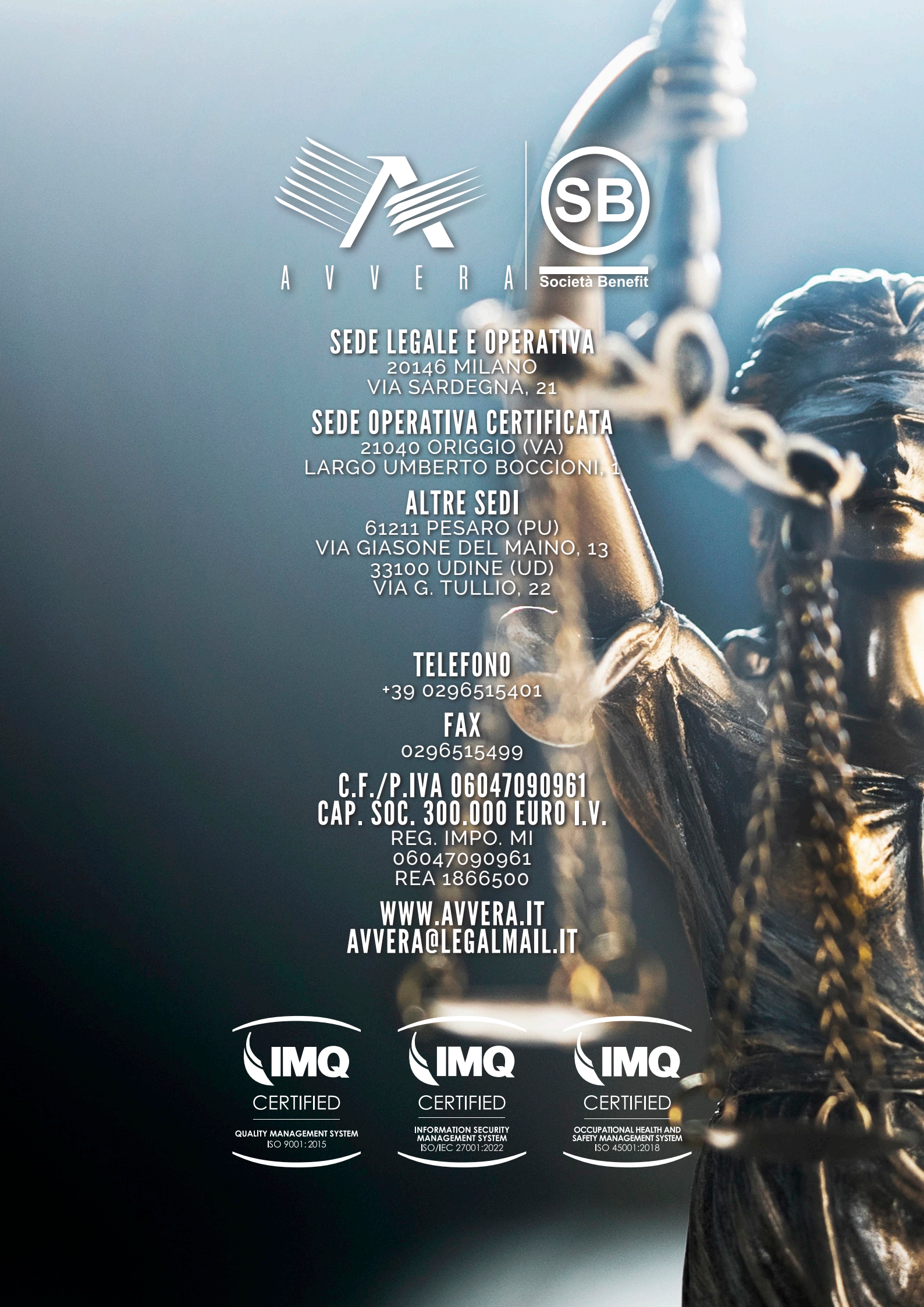
LA QUESTIONE DI FATTO

Il ricorso trae origine da un episodio avvenuto in Austria, dove un operatore di telefonia mobile ha negato a un cliente la stipulazione di un contratto di 10 euro mensili. Il rifiuto era basato su una valutazione automatizzata del merito creditizio effettuata da Dun & Bradstreet Austria GmbH (D&B), una società specializzata nella fornitura di punteggi di affidabilità finanziaria.

Ritenendo il diniego ingiusto, l'interessato ha chiesto alla D&B di accedere ai dettagli relativi alla valutazione, richiedendo informazioni sui dati personali utilizzati, sulla logica del sistema di scoring e sui parametri impiegati per determinare la sua affidabilità finanziaria. Tuttavia, la D&B si è limitata a fornire spiegazioni generiche, rifiutandosi di rivelare dettagli specifici e invocando la protezione del segreto commerciale (disciplinato all' articolo 4, paragrafo 6, del *Datenschutzgesetz* (DSG), la legge austriaca sulla protezione dei dati, secondo cui il diritto di accesso ai dati personali dell'interessato incontrerebbe una una limitazione in presenza di un rischio di compromissione del segreto commerciale).

A seguito del diniego, il ricorrente si è rivolto all'Autorità Austriaca per la Protezione dei Dati, che ha ritenuto la condotta della D&B in violazione dell'obbligo di trasparenza del GDPR ordinando alla società di fornire informazioni più dettagliate sulla logica decisionale adottata. La D&B ha però impugnato la decisione dinanzi alla Corte amministrativa federale austriaca, sostenendo che il proprio modello di valutazione fosse protetto da segreto aziendale e che non vi fosse un obbligo di fornire ulteriori dettagli.

Pur confermando la censura in violazione del GDPR, il Tribunale austriaco non è riuscito a garantire l'esecuzione della decisione: l'amministrazione comunale di Vienna ha infatti ritenuto che la D&B avesse già adempiuto ai propri obblighi informativi. Di fronte a questa situazione di impasse, il Tribunale Amministrativo di Vienna ha sottoposto alla CGUE una serie di quesiti pregiudiziali, chiedendo chiarimenti sull'interpretazione del GDPR e sulla portata del diritto di accesso ai dati personali in presenza di un potenziale conflitto con la tutela del segreto commerciale.



AVVERA | SB Società Benefit

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

IMQ CERTIFIED
QUALITY MANAGEMENT SYSTEM
ISO 9001:2015

IMQ CERTIFIED
INFORMATION SECURITY MANAGEMENT SYSTEM
ISO/IEC 27001:2022

IMQ CERTIFIED
OCCUPATIONAL HEALTH AND SAFETY MANAGEMENT SYSTEM
ISO 45001:2018