AVVERA SRL

NEWSLETTER 2025

AVVERA

Società Benefit

GENNAIO

IL PREZZO NASCOSTO DEI LIKE E DEI DATI PERSONALI: META NEL MIRINO PER EVASIONE FISCALE

MAXI MULTA DEL GARANTE PRIVACY NEI CONFRONTI DI OPENAI

IL GARANTE SANZIONA PER ILLECITI IN TEMA DI MARKETING

L'AUTORITÀ SANZIONA UN'AZIENDA OSPEDALIERA PER LA MANCATA ADOZIONE DI ADEGUATE MISURE DI SICUREZZA

REVENGE PORN: SEGNALAZIONI E STRUMENTI DI TUTELA

TRASMISSIONE ILLECITA DEI DATI PERSONALI DEI MIGRANTI: FRONTEX AMMONITA DALL'EDPS

IL PREZZO NASCOSTO DEI LIKE E DEI DATI PERSONALI: META NEL MIRINO PER EVASIONE FISCALE

Secondo quanto riportato dai principali organi di stampa italiana, la Procura di Milano ha recentemente chiuso le indagini nei confronti di due rappresentanti legali di Meta Platforms Ireland Limited, titolare, tra gli altri, dei social network Facebook e Instagram, per una presunta evasione fiscale relativa al mancato versamento dell'Iva tra il 2015 e il 2021, pari a 877 milioni di euro su un imponibile di circa 4 miliardi di euro.

Con una nota dello scorso 9 dicembre, il Procuratore Marcello Viola ha chiarito che l'omissione del pagamento dell'Iva sarebbe legata al processo di iscrizione degli utenti alle predette piattaforme. Sebbene l'iscrizione sia gratuita per gli utenti, Meta otterrebbe un beneficio economico significativo attraverso la raccolta, profilazione e utilizzo commerciale dei dati personali e delle attività svolte dagli iscritti. Secondo la Procura, questo scambio, basato su una tesi di "permuta di beni differenti", rappresenterebbe un valore economico che dovrebbe essere soggetto all'Iva al 22%.

La ricostruzione avanzata dai magistrati milanesi è considerata innovativa e potenzialmente rivoluzionaria. Secondo gli inquirenti, i dati personali degli utenti, profilati e diffusamente trattati, sono stati una risorsa di grande valore per Meta, che li ha utilizzati per vendere pubblicità mirata e generare profitti. In questa logica, like, commenti e condivisioni assumono un valore economico quantificabile, che l'azienda indagata avrebbe sottratto al fisco italiano per anni.

Questa vicenda non si limita alla dimensione fiscale, ma riporta al centro del dibattito pubblico la questione della privacy e del valore economico dei dati personali. Da tempo esperti e attivisti denunciano il ruolo cruciale dei dati nella strategia di profitto delle grandi aziende tecnologiche, e l'indagine su Meta sembra confermare, ancora una volta, tali preoccupazioni. I dati degli utenti si configurano sempre più come una delle principali fonti di reddito per i colossi digitali.

Le possibili conseguenze di questa vicenda potrebbero essere rilevanti e avere un impatto su scala globale. Difatti, se la tesi della Procura meneghina venisse confermata, si potrebbe creare un precedente importante, stimolando altri Paesi dell'Unione Europea a verificare le pratiche fiscali delle principali piattaforme tech (e non solo). Inoltre, l'attenzione generata dal caso potrebbe stimolare nuove riflessioni per opportuni adeguamenti alle normative in materia di protezione dei dati personali. Si potrebbe giungere all'introduzione di regole più stringenti per la raccolta e l'uso delle informazioni personali, spingendo le aziende a riconsiderare i propri modelli di business e ad esplorare strategie di ricavo che non si basino esclusivamente sulla monetizzazione dei dati degli utenti.

MAXI MULTA DEL GARANTE PRIVACY NEI CONFRONTI DI OPENAI

Con il Provvedimento n. 755 del 2 novembre 2024, il Garante per la protezione dei dati personali italiano ha inflitto a OpenAI, la società dietro il celebre chatbot ChatGPT, una sanzione amministrativa pecuniaria di complessivi 15 milioni di euro.

Il procedimento trae origine da una attività istruttoria avviata d'ufficio a seguito della pubblicazione di notizie stampa relative ad alcune problematiche tecniche (bug) occorse il giorno 20 marzo 2023 al precitato servizio ChatGPT.

Al centro delle contestazioni del Garante vi è la gestione poco trasparente e poco conforme alle norme sulla protezione dei dati personali da parte di OpenAI. L'Autorità ha rilevato, innanzitutto, una carenza di informazioni fornite agli utenti circa la raccolta e l'utilizzo dei loro dati personali. La privacy policy di ChatGPT, disponibile solo in lingua inglese e non facilmente reperibile sul sito web, risultava insufficiente a garantire un'adeguata consapevolezza degli utenti sui trattamenti effettuati sui loro dati.

Il Garante ha inoltre sottolineato l'assenza di una base giuridica adeguata a giustificare il trattamento dei dati personali degli utenti per l'addestramento dei modelli linguistici su cui si basa ChatGPT. Ha destato particolare preoccupazione anche la mancata verifica dell'età degli utenti, considerata cruciale dato il rischio di esposizione dei minori a contenuti potenzialmente inappropriati generati dal chatbot. L'assenza di adeguati meccanismi di controllo è stata considerata un'ulteriore e grave violazione delle norme a tutela dei minori.

Infine, l'Autorità ha contestato a OpenAI la mancata notifica di una violazione dei dati subita nel marzo 2023, un obbligo previsto dal GDPR in caso di incidenti che potrebbero compromettere i diritti e le libertà degli interessati.

Alla luce di queste gravi violazioni, il Garante ha ritenuto necessario irrogare una sanzione pecuniaria di notevole entità, anche al fine di scoraggiare comportamenti illeciti e di sensibilizzare il mercato sulla necessità di un approccio più responsabile alla protezione dei dati personali, specialmente nel contesto delle nuove tecnologie.

Oltre alla sanzione pecuniaria, il Garante ha ordinato a OpenAI di avviare una campagna informativa per spiegare agli utenti come funzionano i modelli di linguaggio come ChatGPT e quali sono i loro diritti in materia di privacy. La campagna, in particolare, dovrà fornire informazioni sulla raccolta dei dati di utenti e non-utenti per finalità di addestramento dei modelli, e sui diritti esercitabili dagli interessati ai sensi del GDPR.

AVVERA Società Benefit

IL GARANTE SANZIONA PER ILLECITI IN TEMA DI MARKETING

Con provvedimento del 12 settembre 2024 [n. 10076504] l'Autorità Garante ha sanzionato il gestore di una importante piattaforma televisiva per aver agito in spregio a quanto disposto dal Regolamento UE 2016/679 ("GDPR") e dal D. Lgs. 196/2003 (c.d. Codice Privacy); l'Autorità ha contestato alla società di aver trattato dati personali in mancanza di un'idonea base giuridica e di non aver fornito agli interessati un'adeguata informativa.

In particolare, l'Autorità ha riscontrato le seguenti violazioni.

In primo luogo, la società risulta aver contattato numerazioni telefoniche iscritte al registro delle opposizioni per lo svolgimento di attività di telemarketing; ciò ha determinato la violazione dell'art. 130, comma 3 bis, del Codice Privacy (che vieta espressamente tale comportamento) e la violazione dell'art. 5, par. 1, let. a) e dell'art. 6, par. 1, let. a) del Regolamento UE 2016/679, relativi al principio di liceità e alla necessità di un'idonea base giuridica del trattamento (costituita dal consenso per quanto riguarda il trattamento di dati personali per finalità di marketing).

Secondariamente, l'Autorità ha rilevato l'invio di messaggi promozionali in mancanza di un espresso consenso al trattamento dei dati personali per finalità commerciali, con conseguente violazione dell'art. 6, par. 1, let. a) del GDPR.

Inoltre, l'Autorità ha rilevato l'illegittimo trattamento di dati personali da parte di terzi fornitori di servizi, nominati Responsabili del trattamento. Tali fornitori avevano curato l'invio di messaggi contenenti la richiesta agli utenti di ricontatto telefonico se interessati ad offerte della società.

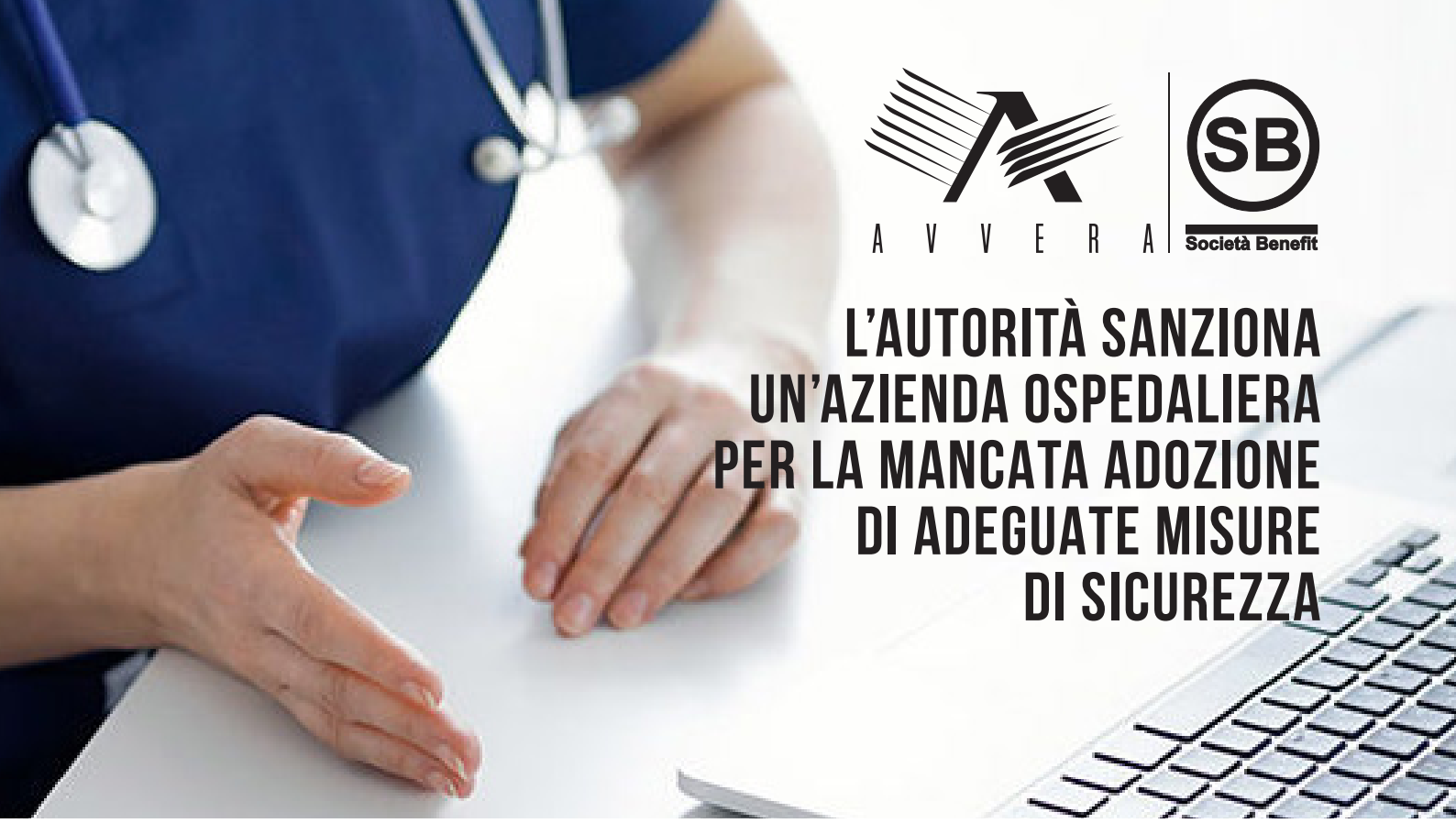
Con riguardo a tali trattamenti, secondo l'Autorità, il titolare avrebbe dovuto controllare tutti gli "anelli" della catena del trattamento, sin dalla prima fase della campagna promozionale. In particolare, l'Autorità ha rilevato la mancata dimostrazione dell'acquisizione di un idoneo consenso al trattamento dei dati personali, da parte dei terzi fornitori Responsabili del trattamento. Ed invero, i file Excel prodotti dal titolare riportanti i dettagli degli sms inviati e dei consensi asseritamente rilasciati dagli interessati difettavano del requisito di immodificabilità e non risultavano per questo motivo idonei a dimostrare la volontà degli interessati. Sul punto il Garante ha in più occasioni sottolineato come la sola indicazione dell'indirizzo IP, abbinato alla data e all'ora di registrazione dell'utente al sito internet, non costituisca alcuna prova dell'espressione di una volontà inequivocabile degli interessati; ciò soprattutto in assenza di ulteriori riscontri probatori che consentano di comprovare la valorizzazione positiva del consenso. Infatti, tutti i file Excel nei quali sarebbero stati registrati i dettagli degli asseriti consensi rilasciati dagli interessati sono risultati modificabili e, in quanto tali, inidonei a comprovare, in modo inequivocabile, la volontà espressa dai medesimi in relazione al trattamento dei loro dati personali. Per quanto riguarda il requisito dell'immodificabilità, elemento essenziale per attestare pienamente l'espressione del consenso degli interessati, l'Autorità ha richiamato le disposizioni, applicabili anche al settore privato, contenute nel Codice dell'Amministrazio-

IL GARANTE SANZIONA PER ILLECITI IN TEMA DI MARKETING

ne Digitale (CAD-D.Lgs. 82/2005) come integrate dalle "Linee guida sulla formazione, gestione e conservazione dei documenti informatici" adottate dall'Agid nel maggio 2021 (https://www.agid.gov.it/sites/agid/files/2024-05/linee_guida_sul_documento_informatico.pdf) in base alle quali "le caratteristiche di immodificabilità e di integrità sono determinate da una o più delle seguenti operazioni", tra cui la "registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema; [nonché] produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione" (v. punto 2.1.1. delle citate Linee guida – "Formazione del documento informatico"). Pertanto l'Autorità, rilevato che la documentazione prodotta dal titolare non atteneva a record direttamente estratti dai sistemi informatici aziendali ma consisteva in una mera trasposizione in formato Excel dei dati ivi contenuti, ha ritenuto che tale documentazione non potesse essere valutata sul piano probatorio in quanto priva delle caratteristiche di oggettività, integrità e immodificabilità e, di conseguenza, ha riscontrato la mancanza di un'idonea base giuridica del trattamento.

Da ultimo, con riferimento al servizio di ricontatto fornito attraverso un comparatore, l'Autorità ha rilevato come l'informativa fornita agli interessati al momento della compilazione del form online per ottenere la comparazione delle offerte risultasse inidonea, in quanto indicava un'erronea base giuridica del trattamento; in particolare, l'informativa dichiarava che i dati personali inseriti nel form avrebbe potuto essere utilizzati per l'invio di comunicazioni di marketing sulla base del legittimo interesse della società, mentre l'attività promozionale non poteva che svolgersi sulla base del consenso degli interessati.

In considerazione delle violazioni descritte e tenuto conto della gravità delle stesse, riferite a condotte di sistema in quanto radicate nella procedura societaria, l'Autorità garante ha applicato al Titolare la sanzione amministrativa pecuniaria di euro 842.062,00 ed ha disposto la pubblicazione del provvedimento nel sito dell'Autorità.



L'AUTORITÀ SANZIONA UN'AZIENDA OSPEDALIERA PER LA MANCATA ADOZIONE DI ADEGUATE MISURE DI SICUREZZA

Con provvedimento del 17 ottobre 2024 l'Autorità Garante ha sanzionato un'Azienda Ospedaliero-Universitaria col pagamento di euro 25.000,00, rilevando la mancata adozione di adeguate misure di sicurezza a tutela dei dati personali; circostanza che aveva reso possibile, tramite un attacco ransomware da parte di un gruppo criminale, l'accesso ai dati di dipendenti, consulenti e pazienti.

A riguardo, l'Autorità ha rilevato, in primo luogo, la mancata adozione di misure adeguate a individuare tempestivamente la violazione dei dati personali. In particolare, l'Azienda Ospedaliera non disponeva di un sistema di log management e si è reso necessario implementare un sistema di Security Information and Event Management.

Secondariamente, è stata rilevata dall'Autorità la mancata adozione di misure adeguate a garantire la sicurezza delle reti e l'obsolescenza dei software di base installati su alcuni sistemi di trattamento. In particolare, l'Azienda Ospedaliera non aveva adottato adeguate misure per segmentare le reti su cui erano attestate le postazioni di lavoro dei propri dipendenti, nonché i sistemi (server) utilizzati per i trattamenti ("la rete era sostanzialmente flat, non vi era una segmentazione logica o fisica" e non erano differenziate a livello di rete le postazioni di lavoro e i server).

Inoltre, nel momento in cui si è verificata la violazione dei dati personali:

- l'accesso remoto, tramite VPN, alla rete, avveniva mediante una procedura di autenticazione informatica basata solo sull'utilizzo di username e password, non essendo in vigore una procedura di autenticazione informatica a più fattori (MFA);
- le utenze di "manutenzione" erano spesso generiche, non individuali, con massimi privilegi amministrativi";
- nonostante fossero state fornite indicazioni al personale circa la scelta della password, ispirate alle buone pratiche di settore, non era prevista alcuna configurazione dei sistemi che recepisse tali indicazioni;
- il firewall perimetrale conteneva delle vulnerabilità e erano "attivi ancora vari protocolli di comunicazione obsoleti".

Alla luce di quanto sopra esposto l'Autorità ha rilevato la violazione dell'art. 5, par. 1, let. f) e dell'art. 32 del Regolamento UE 2026/679, ingiungendo all'Azienda Ospedaliera il pagamento della sanzione amministrativa pecuniaria di euro 25.000,00.

Va rilevato che nel quantificare l'importo della sanzione, l'Autorità ha tenuto conto dell'impegno del Titolare ad implementare misure di sicurezza volte a ridurre la replicabilità dell'evento occorso e la costante cooperazione con l'Autorità in ogni fase dell'istruttoria.

REVENGE PORN: SEGNALAZIONI E STRUMENTI DI TUTELA

Il Garante per la Protezione dei Dati Personali ha predisposto una scheda informativa dedicata alla prevenzione e al contrasto del fenomeno del revenge porn, corredata da un link per accedere a un servizio di segnalazione online. L'espressione revenge porn (traducibile dall'inglese come "pornografia vendicativa") indica la diffusione non autorizzata di contenuti estremamente intimi, come immagini o video, attraverso piattaforme online, applicazioni di messaggistica istantanea o social network, con l'intento di arrecare danno, umiliare o esercitare pressioni sulla persona rappresentata.

L'iniziativa dell'Autorità, pertanto, mira a supportare chiunque tema la diffusione non consensuale di immagini o video a contenuto sessualmente esplicito, fornendo strumenti concreti per proteggere la propria dignità e sfera personale.

La scheda informativa evidenzia l'importanza di adottare misure per la protezione dei dati personali. È fondamentale utilizzare password sicure per dispositivi come laptop, cellulari e tablet, proteggere file sensibili con sistemi di crittografia e installare software antivirus per prevenire accessi non autorizzati. La consapevolezza e la prudenza nella gestione dei dati rimangono strumenti essenziali per ridurre il rischio di esposizione indesiderata.

Oltre a proteggere i propri dati, è cruciale rispettare quelli altrui. In caso di ricezione di immagini non autorizzate, il Garante sottolinea la necessità di evitare qualsiasi forma di diffusione. È opportuno cancellare tali contenuti e, se necessario, segnalare l'accaduto alla Polizia Postale (https://www.commissariatodips.it/).

Un'attenzione particolare deve essere posta alla tutela dei minori. È importante monitorare l'utilizzo dei dispositivi digitali da parte dei più giovani, spiegare loro i rischi connessi alla diffusione di contenuti personali online e promuovere comportamenti responsabili nell'interazione sui social network.

In caso di timori fondati sulla possibile diffusione di contenuti personali, è possibile presentare una segnalazione al Garante tramite il modulo disponibile sul sito istituzionale dell'Autorità (https://servizi.gpdp.it/diritti/s/revenge-porn-scelta-auth). Nel modulo è necessario indicare le piattaforme coinvolte e le ragioni del timore, trasmettendo eventuali contenuti sensibili tramite un link sicuro fornito dal Garante. Valutate le circostanze, l'Autorità potrà adottare provvedimenti volti a contrastare la diffusione dei contenuti non autorizzati.

Questo servizio, disponibile per adulti e minori ultraquattordicenni, può essere integrato con le azioni della Polizia Postale nei casi in cui siano ravvisabili reati quali minacce o richieste estorsive.

Rimane essenziale mantenere alto il livello di prudenza nella condivisione di materiale sensibile, poiché l'intervento del Garante non garantisce una protezione assoluta dalla diffusione non autorizzata. La prevenzione, attraverso comportamenti responsabili, resta la migliore forma di tutela.

Per maggiori informazioni è possibile consultare la pagina informativa sul sito del Garante per la Protezione dei Dati Personali (https://www.gpdp.it/web/guest/temi/revengeporn).

TRASMISSIONE ILLECITA DEI DATI PERSONALI DEI MIGRANTI: FRONTEX AMMONITA DALL'EDPS

Il Garante europeo della protezione dei dati (EDPS) ha rivolto un ammonimento a Frontex (Agenzia europea della guardia di frontiera e costiera) per aver trasmesso a Europol (Agenzia dell'UE per la cooperazione nell'attività di contrasto) dati personali di indagati per reati transfrontalieri, in violazione del Regolamento UE 2019/1896 (c.d. Regolamento Frontex).

È quanto si apprende da un comunicato dell'EDPS dell'8 gennaio 2025, secondo cui, nell'ottobre 2022, la predetta Autorità ha effettuato un audit sulle attività di Frontex nelle operazioni congiunte di supporto agli Stati membri lungo le frontiere esterne dell'UE. L'audit si è concentrato sui colloqui di debriefing condotti dall'Agenzia con le persone fermate in occasione dell'attraversamento delle frontiere.

In particolare, l'EDPS ha constatato che Frontex, durante tali colloqui, raccoglieva informazioni su indagati di reati transfrontalieri, fondandosi sulle testimonianze degli intervistati. Inoltre, l'Agenzia inviava queste informazioni a Europol in modo continuativo, senza però compiere una valutazione preventiva sulla reale necessità di tale condivisione, contrariamente a quanto richiesto dall'art. 90 del Regolamento Frontex. Tale disposizione prevede che i dati personali raccolti durante il monitoraggio dei flussi migratori, lo svolgimento di analisi dei rischi o durante le operazioni volte a identificare persone sospettate di criminalità transfrontaliera possono essere scambiati da Frontex con Europol solo se strettamente necessari per lo svolgimento del mandato di quest'ultima.

Pertanto, considerando i rischi per gli interessati derivanti dalla possibile inattendibilità o inesattezza delle informazioni personali raccolte, l'EDPS ha avviato un'indagine maggiormente approfondita che, confermando la mancata analisi preliminare sulla pertinenza dei dati trasmessi rispetto al mandato di Europol, ha accertato la violazione del Regolamento UE 2019/1896 da parte di Frontex.

Pur riconoscendo la gravità di tale circostanza, l'EDPS ha deciso di limitarsi a rivolgere un ammonimento a Frontex. Tale scelta è stata motivata dal fatto che l'Agenzia ha prontamente interrotto la trasmissione delle suddette informazioni personali a Europol e ha avviato discussioni con quest'ultima per definire i criteri di valutazione della necessità dei dati raccolti, nonché per stabilire regole precise sulla loro condivisione.

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

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