AVVERA

2023 NEWSLETTER GENNAIO

01

SEDE LEGALE E OPERATIVA
20146 Milano
via Sardegna, 21

SEDE OPERATIVA CERTIFICATA
21040 Origgio (VA)
Largo UmbertoBoccioni, 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

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

COOKIEWALL E PAYWALL, UNA BREVE SINTESI

In premessa, è necessario effettuare una distinzione tra il c.d. "cookie wall" e il "paywall".

Il "cookie wall" è un meccanismo applicabile su un sito web, che concede all'utente di accedere soltanto prestando il proprio consenso a tutti i cookie. Questo sistema è generalmente proibito, in quanto, secondo il Considerando 32 del GDPR, il consenso *"dovrebbe essere prestato mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano".* Questo concetto è stato riportato nella definizione di consenso dell'interessato, (art. 4, punto 11 del GDPR) (qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento).

In riferimento ai "cookie wall" si sono espressi:

- l'EDPB, confermando che "affinché il consenso sia prestato liberamente, l'accesso ai servizi e alle funzionalità non deve essere subordinato al consenso dell'utente alla memorizzazione di informazioni o all'ottenimento dell'accesso a informazioni già memorizzate nell'apparecchiatura terminale dell'utente", (Linee Guida 5/2020 sul consenso, Paragrafo 39);
- il Garante per la protezione dei dati personali italiano, confermando che "tale meccanismo non consentendo di qualificare l'eventuale consenso così ottenuto come conforme alle caratteristiche imposte dal Regolamento, […] è da ritenersi illecito, salva l'ipotesi da verificare caso per caso nella quale il titolare del sito offra all'interessato la possibilità di accedere ad un contenuto o a un servizio equivalenti senza prestare il proprio consenso all'installazione e all'uso di cookie o altri strumenti di tracciamento".

Relativamente a questa ipotesi, contenuta nelle Linee Guida del Garante italiano, è opportuno descrivere il c.d. "paywall", un meccanismo applicabile su un sito web, per cui all'utente viene proposta un'alternativa alla prestazione del proprio consenso all'installazione dei cookie per accedere ai contenuti, come un pagamento o un abbonamento.

Il "paywall" è stato applicato da alcune importanti testate giornalistiche italiani ed internazionali, che propongono contenuti online chiedendo il consenso dell'utente per l'installazione di tutti i cookie pubblicitari e di profilazione, oppure comprare un abbonamento, al fine di poter visionare gli articoli caricati sul sito web. Chiaramente l'intento degli editori che usufruiscono di questo sistema di "paywall" è quello di acquisire i dati profilati degli utenti che navigano sul sito web, per rivenderli ai fornitori di pubblicità, con premi più remunerativi della generica pubblicità.

L'attività è giustificata dagli editori come mezzo economico per supportare il lavoro delle proprie redazioni giornalistiche, al fine di fornire un'informazione di maggiore qualità.

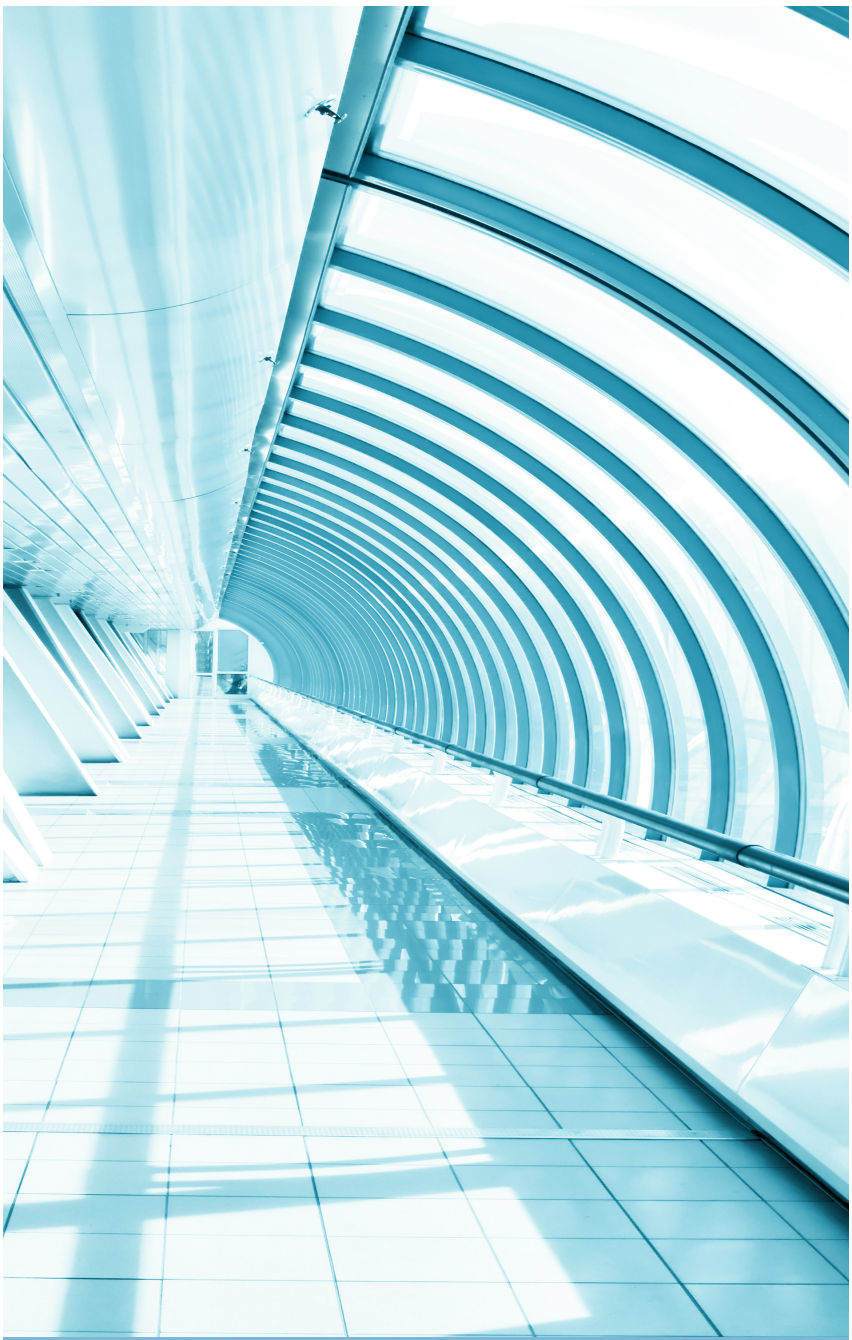
La questione è ancora oggetto di analisi da parte dei Garanti europei, compreso quello italiano che alla data odierna non si è ancora espresso sulla liceità di questa modalità di acquisizione dei dati personali degli utenti. Infatti, in seguito alla sentenza del Consiglio di Stato n. 2631/2021 (caso Facebook), il Garante italiano ha affermato che *"neppure il comitato dei Garanti, tuttavia, arriva ad escludere in maniera assoluta che il consenso al trattamento dei dati personali possa essere qualificato come controprestazione giacché ricorda che tale conclusione è, in realtà, "solo" una "presunzione forte" con la conseguenza che "in un numero molto ristretto di casi" condizionare l'erogazione di un servizio*

COOKIEWALL E PAYWALL, UNA BREVE SINTESI

alla prestazione di un consenso potrebbe non valere a rendere invalido il consenso. Tuttavia, trattandosi di una presunzione, per di più forte, anche in tali limitate ipotesi toccherà al titolare del trattamento, in caso di contestazione, fornire prova della circostanza che il consenso, pur se condizionato può considerarsi espresso liberamente. E non sembra trattarsi di un onere probatorio facilmente soddisfacibile".

Nel comunicato stampa dello scorso 12 novembre 2022 (ultimo in ordine di tempo sull'argomento), il Garante ha informato che sta proseguendo l'attività istruttoria e che è stato richiesto ai titolari di:

- chiarire le modalità di funzionamento del meccanismo in questione;
- fornire tutti gli elementi utili a dimostrare che la normativa in materia di protezione dei dati personali sia stata rispettata;
- produrre considerazioni contenute nelle valutazioni di impatto;
- indicare i criteri adottati per la determinazione del prezzo dell'abbonamento alternativo al servizio disponibile mediante prestazione del consenso.



SANITÀ, RECENTI INTERVENTI DEL GARANTE

Il Garante per la protezione dei dati personali è tornato ad analizzare recentemente tematiche strettamente legate al mondo della sanità, in particolare concentrandosi sul dossier sanitario elettronico DSE.

Il Garante ha reso noto che, nello scorso mese di novembre, ha sanzionato una azienda sanitaria locale. Tale azienda aveva sostanzialmente agevolato un indebito accesso a dati sanitari una paziente mediante il DSE, avendo rimosso le misure di profilazione proprie del DSE stesso e avendo deciso – a motivo dell'emergenza sanitaria pandemica – di sospendere le limitazioni relative alla costituzione del DSE.

Nel dettaglio un'operatrice sanitaria dipendente della stessa azienda lamentava che:

- era stato comunque posto in essere il trattamento dall'azienda, pur avendo lei negato espressamente il consenso al trattamento dei dati attraverso DSE esso;
- una collega, che non l'aveva mai avuta in cura, aveva effettuato ripetuti accessi a informazioni a lei relative.

Il Garante, sanzionando la azienda, ha ribadito che:

- la disciplina introdotta a seguito dell'emergenza Covid ha previsto alcune semplificazioni, ma non ha derogato ai principi generali e alle regole sul trattamento dei dati sulla salute effettuato attraverso il dossier sanitario;
- l'azienda deve dotarsi di strumenti informatici che siano in grado di assicurare la conformità alla normativa e che limiti tecnici degli stessi non possono essere addotti a giustificazione per il mancato rispetto dei citati principi generali.

La sanzione comminata, quantificata in 40.000 euro, è stata comminata tenuto conto della gravità delle trasgressioni, nonché della circostanza che le violazioni si sono protratte nel tempo e hanno coinvolto i dati sulla salute di tutta la popolazione assistita, senza che i pazienti ne fossero informati.

Sempre in tema di sanità, con la newsletter 498 del mese di dicembre, il Garante ha reso noto di aver aggiornato la pagina informativa sul fascicolo sanitario elettronico introducendo una specifica sulla corretta gestione dei risultati di accertamenti diagnostici diretti o indiretti per l'infezione da HIV. L'esito di tali accertamenti, ai sensi della disciplina vigente, può essere dato esclusivamente alla persona cui tali esami sono riferiti.

Solo una volta soddisfatta tale intermediazione, il referto sull'HIV può essere reso disponibile all'interessato tramite il FSE (e ovviamente anche tramite altre modalità di accesso non intermediate eventualmente in uso al paziente).

LAVORO: ILLECITO IL CONTROLLO DI METADATI DELLE E-MAIL DI DIPENDENTI

Con comunicato stampa del 19 dicembre 2022 il Garante per la protezione dei dati personali ha reso noto di aver sanzionato la Regione Lazio per illecito trattamento di dati personali di dipendenti effettuato controllando metadati della posta elettronica.

L'ente aveva dichiarato di aver effettuato il monitoraggio dei metadati della posta elettronica (orari, destinatari, oggetto delle comunicazioni, peso degli allegati). L'ente aveva dichiarato che tali informazioni sono conservate per 180 giorni. L'ente aveva inoltre dichiarato che il controllo, attivato per accertare eventuali comportamenti illeciti del lavoratore dei quali vi era ragionevole sospetto e che risultavano anche lesivi dell'immagine dell'Amministrazione, era avvenuto in maniera isolata e una tantum in assenza di formalismi.

Il Garante, anche mediante attività ispettive, ha accertato che la Regione aveva potuto effettuare il monitoraggio del personale, in particolare dei dipendenti dell'avvocatura che inviavano messaggi a uno specifico sindacato, sfruttando i dati conservati per generiche finalità di sicurezza informatica per 180 giorni, in assenza di idonei presupposti giuridici violando così i principi di protezione dei dati e delle norme sul controllo a distanza.

Il Garante infatti ha indicato che la conservazione dei metadati relativi all'utilizzo della posta elettronica dei dipendenti, ancorché sul presupposto della sua necessità per finalità di sicurezza informatica, può comportare un indiretto controllo a distanza dell'attività dei lavoratori, che la legge consente esclusivamente al ricorrere di esigenze organizzative, produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale, e in presenza delle garanzie procedurali previste dall'art. 4, comma 1, della l. n. 300/1970 (accordo sindacale o, in alternativa, autorizzazione pubblica).

Sul tema il Garante ha quindi rilevato un trattamento illecito in quanto i dati personali relativi ai messaggi di posta elettronica, sono stati trattati dalla Regione anche al fine di effettuare verifiche puntuali su specifici dipendenti.

Sull'applicabilità al caso di specie dell'eccezione dei c.d. controlli difensivi, il Garante ha evidenziato che essa è "di pura creazione giurisprudenziale" e "oggetto di applicazioni non univoche".

Il Garante ha ritenuto comunque che tale eccezione non si possa applicare al caso di specie, fondandosi su fatti che in ogni caso non ricorrono.

Il Garante ha infatti evidenziato come i trattamenti di dati personali connessi all'impiego di strumenti dai quali possa derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori devono essere svolti nel rigoroso rispetto dei limiti e delle condizioni previste dalla cornice legislativa di riferimento, che ne costituisce, come detto, la base giuridica. Anche le esigenze di tutela del patrimonio datoriale, state espressamente incluse tra le finalità lecite perseguibili mediante sistemi che possono comportare il controllo indiretto sulla generalità dei dipendenti, sono da considerare subordinate l'installazione e l'utilizzazione all'accordo sindacale o, in alternativa, all'autorizzazione pubblica. Ne consegue, a parere del Garante, che qualunque trattamento debba considerarsi sprovvisto di idonea base giuridica e quindi illecito, qualora non vengano rispettate tali condizioni per il lecito impiego dei predetti sistemi.

Le considerazioni esposte dal Garante sull'applicabilità dei "controlli difensivi", che confermano altre impostazioni molto rigorose di detta Autorità, vanno quindi a arricchire il già ampio spettro di posizioni presenti in tema di c.d. controlli difensivi, richiamando i titolari a presentare sempre una particolare attenzione qualora si intenda operare in tale "scivoloso" ambito.

RILEVAZIONI BIOMETRICHE SUL LUOGO DI LAVORO

Nella newsletter del 22/12/22 il Garante ha reso noto di aver sanzionato per l'ammontare d 20.000 euro un datore di lavoro che aveva installato un sistema di rilevazione biometrica per la rilevazione delle presenze.

Nel corso dell'istruttoria e degli accertamenti ispettivi, effettuati dal Nucleo speciale tutela privacy e frodi tecnologiche della Guardia di Finanza, è emerso che la società aveva effettuato, per quasi quattro anni, la rilevazione delle impronte digitali dei 132 dipendenti senza un'adeguata base normativa.

Con riferimento a questa tematica il Garante ha ricordato che il trattamento di dati biometrici sul posto di lavoro è consentito solo se necessario per adempiere gli obblighi ed esercitare i diritti del datore di lavoro previsti da una disposizione normativa e con adeguate garanzie.

Inoltre, essendo possibili strumenti e soluzioni meno invasive, il Garante ha contestato il mancato rispetto del principio di minimizzazione e proporzionalità.

L'ammontare della sanzione è stato definito anche considerando:

- la natura, gravità e durata della violazione (che si è protratta per poco meno di quattro anni);
- il grado di responsabilità del titolare che non si è conformato alla disciplina in materia di protezione dei dati, relativamente a una pluralità di disposizioni riguardanti anche i principi generali del trattamento (liceità e correttezza).

Ben emerge da tale circostanza come, a parere del Garante, ben poco ci sia da aggiungere a un tema che ben è stato analizzato (e considerato molto critico).

IL GARANTE TORNA SUI "RUOLI PRIVACY"

Con un recente provvedimento il Garante per la protezione dei dati personali ha sanzionato un istituto scolastico a seguito di un reclamo ricevuto da uno studente.

Detto studente, destinatario di contestazioni disciplinari da parte dell'istituto per dichiarazioni pubblicamente rese in una assemblea tenutasi online e organizzata da un'associazione studentesca, contestava la liceità dei trattamenti di dati effettuati per giungere alla contestazione. In particolare detta contestazione aveva fondamento sulla trascrizione di un audiovideo rinvenuto presso l'istituto effettuata da un perito fonico iscritto all'Albo dei Periti presso il Tribunale di Roma.

Tra le altre, per quanto di interesse nella presente analisi, l'istituto sosteneva che il "ruolo privacy" il perito fonico non fosse quello di Responsabile del trattamento (mancando un atto di nomina formale ai sensi dell'art. 28 del GDPR), ma di averlo considerato "istruito ed autorizzato ai sensi dell'art. 29 GDPR".

Il Garante, sul merito di tali riscontri, riteneva invece che, contrariamente a quanto rappresentato dalla parte resistente, non ricorrevano i presupposti per considerare il professionista in questione, soggetto autorizzato ai sensi dell'art. 29 del Regolamento, dovendosi ritenere che il riferimento all'agire "sotto l'autorità diretta del titolare o del responsabile" e l'essere "istruito" in merito all'accesso ai dati, si riferisca a persone appartenenti alla struttura giuridica e organizzativa del titolare o del responsabile come peraltro precisato dal Comitato europeo per la protezione dei dati personali (cfr. "Linee guida 07/2020 sui concetti di titolare e responsabile del trattamento nel GDPR", adottate il 7 luglio 2021 dal Comitato europeo per la protezione dei dati personali, spec. pp. 31-32, par. 88, 89 ove espressamente si fa riferimento a "un dipendente o una persona che occupi una posizione molto simile a quella di un dipendente ad esempio il personale di un'agenzia di lavoro interinale").

Per quanto concerne la mancata nomina del perito fonico quale Responsabile del trattamento, il Garante sottolineava inoltre il rilievo che assume la precisa identificazione dei soggetti che, a diverso titolo, possono trattare i dati personali e la chiara distinzione delle rispettive attribuzioni, in particolare quella tra Titolare e Responsabile del trattamento, il cui rapporto va regolato da un contratto o da altro atto giuridico, stipulato per iscritto che, oltre a vincolare reciprocamente le due figure, consente al Titolare di impartire istruzioni al Responsabile e prevede, in dettaglio, quale sia la materia disciplinata, la durata, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare: da cui discende la legittimazione del Responsabile del trattamento a trattare i dati degli interessati "soltanto su istruzione documentata del Titolare" (art. 28, par. 3, lett. a) GDPR).

Alla luce di quanto nel citato provvedimento pare opportuno procedere sempre con la massima attenzione nel valutare i casi più particolari e considerare non solo la posizione resa nel presente procedimento, ma anche la posizione sullo stesso tema in altri interventi (ad esempio la previsione del ruolo di "autorizzato" per il membro dell'Organismo di Vigilanza ex D.lgs 231/2001.

LA CGUE A PROPOSITO DI OCCHIALI PER I VIDEOTERMINALISTI

La materia della Salute e della Sicurezza dei lavoratori è costantemente oggetto di interesse da parte della Giurisprudenza nazionale ed europea.

In Europa, sempre più frequentemente, i Giudici si esprimono attraverso numerose interpretazioni che sono frutto di uno sviluppo dell'attenzione sempre maggiore a favore della tutela dei milioni di lavoratori.

La Corte di Giustizia dell'Unione Europea ha stabilito, con la sentenza del 22/12/2022 (causa C-392/21), un'interpretazione che ha un significato rilevante in ambito Salute e Sicurezza sul lavoro.

Ebbene, la Corte, rileggendo l'art. 9, par. 3 della direttiva 90/270/CEE del Consiglio, del 29/5/1990 che riguarda le prescrizioni minime in materia di sicurezza e di salute per le attività lavorative svolte su attrezzature munite di videoterminali (quinta direttiva particolare ai sensi dell'articolo 16, paragrafo 1 della direttiva 89/391/CEE), ha stabilito che i «dispositivi speciali di correzione» includono gli occhiali da vista specificamente diretti a correggere e a prevenire disturbi visivi in funzione di un'attività lavorativa che si svolge su attrezzature munite di videoterminali.

Inoltre la Corte ha stabilito che tali «dispositivi speciali di correzione» non si limitano a dispositivi utilizzati esclusivamente nell'ambito professionale.

Si desume pertanto che l'obbligo imposto al datore di lavoro dalla disposizione citata, ossia quello di fornire ai lavoratori videoterminalisti un dispositivo speciale di correzione, può essere adempiuto da quest'ultimo o mediante fornitura diretta di tale dispositivo ai lavoratori ovvero mediante il rimborso delle spese necessarie ad acquistarlo, sostenute dal lavoratore.

L'ipotesi invece che non sembrerebbe percorribile, al fine di adempiere all'obbligo, sarebbe un alternativo versamento da parte del datore al lavoratore di un premio salariale generale.

IL TITOLARE DEVE INDICARE ALL'INTERESSATO I DESTINATARI DEI SUOI DATI PERSONALI

In una recente sentenza la Corte di Giustizia dell'Unione Europea ha stabilito il principio secondo cui l'interessato che faccia richiesta di accesso ai propri dati personali ha diritto di conoscere esattamente chi sono i destinatari a cui gli stessi sono stati trasferiti.

Tale pronuncia nasce dal ricorso di un cittadino austriaco nei confronti del principale servizio postale del suo paese che comunicava i dati degli utenti a società terze per finalità di marketing. Esercitando il diritto di accesso ai sensi dell'art. 15 GDPR e nonostante diversi tentativi, l'interessato non aveva mai ricevuto l'indicazione puntuale di quali terzi avessero ricevuto i suoi dati personali.

Ed ecco così che il procedimento arrivava fino alla CGUE, dinanzi alla quale il servizio postale eccepiva un mancato obbligo di fornire i dettagli specifici sui terzi che hanno ricevuto i dati, potendo indicarli genericamente, per categorie, seguendo il dettato della lettera dell'art. 15/1 GDPR che pare offrire un'alternativa, priva di condizioni o priorità, tra destinatari o categorie di destinatari.

Pertanto avrebbe rispettato la trasparenza nella misura richiesta dalla normativa europea, senza incorrere in alcuna violazione.

La Corte ha ribattuto con una sua interpretazione netta e contraria, combinando il dato letterale dell'art. 15 GDPR agli altri diritti collegati e domandandosi come potrebbe un interessato esercitare i propri diritti verso terzi destinatari – che hanno ricevuto i dati personali – se il primo titolare, quello d'origine del flusso, omettesse di comunicare i dettagli precisi che identificano tali terzi.

Pertanto, per la CGUE ciò rappresenterebbe una lesione dei diritti riconosciuti dal GDPR e dei principi ad esso sottesi: il diritto di accesso rappresenta il cuore del sistema di protezione, senza il quale verrebbe meno il senso dell'intera tutela normativa, e va pertanto tutelato nella maggior misura possibile.

Con riguardo all'opzione sopra citata tra 'destinatari' e 'categorie di destinatari' la Corte ricostruisce il diritto in parola precisando che, in sede di accesso, l'interessato ha facoltà di scelta, potendo richiedere le categorie così come il dettaglio dei destinatari, con le seguenti eccezioni: la prima eccezione si ha qualora sia "impossibile" identificare i destinatari; la seconda si ha qualora le richieste di accesso dell'interessato siano "manifestamente infondate o eccessive", come previsto dall'art. 12/5 GDPR.

Nelle predette eccezioni si potrà utilizzare la mera categoria di destinatari nel replicare all'interessato, gravando comunque sul titolare l'onere di comprovare i requisiti per l'applicazione delle eventuali eccezioni che, ricordiamo, potrebbero sussistere normativamente a livello nazionale o sovranazionale.

NEWSLETTER 01 GENNAIO

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

CSQ ISO 9001 CSQ ISO 45001 CSQ ISO/IEC 27001