

**I Partners dello Studio**

Giorgio Violi

tel: 3386132605

[givioli@gmail.com](mailto:givioli@gmail.com)

Alberto Sant'Unione

tel: 3409125853

[santunionea@gmail.com](mailto:santunionea@gmail.com)

**Qualità   Sicurezza   Privacy   Ambiente   Risk Management**  
**Responsabilità Amministrativa 231   Etica   Consulenza e Audit per la Direzione**

Organizzazione con sistema di gestione certificato secondo la norma ISO 9001: 2015 per Progettazione ed erogazione di servizi di consulenza relativa ai Sistemi di Gestione Aziendale per la Qualità, la Sicurezza negli ambienti di lavoro, la Privacy, l'Ambiente, l'Etica, per i Modelli Organizzativi e Consulenza per la Direzione

**2023 Aprile** *Il nostro punto di vista su...* Anno 16 – 1° sem



**Periodico di informazione  
per i CLIENTI dello STUDIO VIOLI**



**Indice delle NOTIZIE (N)**

- N1) **D.Lgs. 231/01:** D.Lgs. 10 marzo 2023 n.24: Recepimento Dir UE 2019/1937 in materia di “Whistleblowing
- N2) **Privacy:** GDPR, gli errori più comuni che fanno sanzionare le aziende – **MOLTO IMPORTANTE**
- N3) **Privacy:** Mail dipendenti: le linee guida del Garante privacy
- N4) **Privacy:** Stop del Garante a ChatGPT; Ammissibile l'utilizzo del sistema di videosorveglianza per comprovare l'inadempimento disciplinare del lavoratore
- N5) **Ambiente:** Pubblicato il DPCM che approva il MUD 2023. La scadenza per l'invio è l'8 Luglio 2023

**SENTENZE DI CASSAZIONE SUL LAVORO**

- Sul sito <http://www.dottinalavoro.it/argomento/giurisprudenza-c/corte-di-cassazione-c> sono presenti le ultime sentenze di Cassazione relative al lavoro

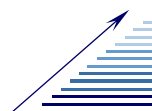


**AFORISMA DEL MESE**

*“La migliore preparazione per domani è fare il tuo meglio oggi”*

*H. Jackson Brown Jr. (scrittore statunitense)*

**Scadenziario di Aprile 2023 sul sito del Sole 24 Ore <http://www.ilsole24ore.com/norme-e-tributi/scadenze.shtml>**



**E-mail:** [info@studiovioli.com](mailto:info@studiovioli.com) **SDI:** [giorgiovioli@pec.it](mailto:giorgiovioli@pec.it)  
**Web:** [www.studiovioli.com](http://www.studiovioli.com) **Fax:** 059 682304

Studio Violi Srl - Via per Capanna Tassone, 1156 41021 Ospitale - Fanano (MO)  
P.I. e C.F. 02836380366 – REA 335410 CCIAA MO – Cap. Soc. € 10.000 I.V.



**“Incendio o soffocamento?”**

## Notizie



### - N1) D.Lgs. 231/01: D.Lgs. 10 marzo 2023 n.24: Recepimento Dir UE 2019/1937 in materia di “Whistleblowing

**Il D.Lgs. 10 marzo 2023 n.24, recependo la Direttiva UE 2019/1937, disciplina anche per il nostro Paese la protezione di persone che, nell’ambito lavorativo pubblico o privato, segnalano, sulla base di fondati sospetti, violazioni di norme nazionali o dell’Unione Europea**

che ledono un interesse pubblico o l’integrità della Pubblica Amministrazione o di un Ente privato, a seguito di informazioni intercettate o raccolte dal lavoratore durante l’esercizio della propria attività professionale.

La pratica di denunciare ad un Ente di controllo sovraordinato, attraverso informazioni circostanziate e adeguatamente protette (**cosiddetto “whistleblowing”, letteralmente “segnalazione” o “soffiata”**) le violazioni che possono ricorrere nel mondo del lavoro, è da tempo ritenuta una componente valoriale dei rapporti di lavoro di molti Paesi dell’Unione Europea, in particolare per impedire fenomeni di corruzione, di mobbing, di danno a interessi o diritti pubblici o **per contrastare comportamenti che possono dar adito alla commissione di reati presupposto da parte di soggetti apicali di un Ente, quali quelli attualmente rubricati nel D.Lgs. 231/01 che disciplina i Modelli Organizzativi.**

Il decreto non si sostituisce all’applicazione di disposizioni in materia di esercizio del diritto dei lavoratori di consultare i propri rappresentanti sindacali nel caso di condotte o atti illeciti posti in essere nei loro confronti, a contrasto delle disposizioni previste nei CCNL, nello Statuto dei Lavoratori o nelle relative norme complementari.

**I reati che dunque si intendono contrastare attraverso una sensibilizzazione della popolazione lavorativa alla tutela degli interessi e diritti comuni sono, ad esempio, quelli che possono essere commessi nei settori degli appalti pubblici, dei servizi e dei prodotti dei mercati finanziari, nelle operazioni di riciclaggio e di finanziamento al terrorismo, della sicurezza e della conformità dei prodotti, della sicurezza dei trasporti, della tutela dell’ambiente e della sicurezza nei luoghi di lavoro, nell’ambito della salute pubblica e della protezione dei consumatori, nell’ambito della tutela della vita privata e della protezione dei dati personali, della sicurezza delle reti e dei sistemi informativi.**

Di fronte alla denuncia effettuata ad una autorità giudiziaria o contabile da una persona segnalante, venuta a conoscenza di violazioni o possibili violazioni nell’ambito del proprio contesto lavorativo, il decreto appronta strumenti di protezione contro possibili comportamenti ritorsivi.

Tra questi strumenti sono previsti canali di segnalazione interna o esterna approntati dagli stessi Enti privati o pubblici, dove l’identità del segnalante rimane criptata in modo da garantire il carattere di riservatezza della comunicazione e della relativa documentazione di supporto. I Modelli di Organizzazione e di Gestione, di cui all’articolo 6, comma 1, lettera a) del D.Lgs. n. 231 del 2001, già prevedono canali di segnalazione interna all’Organismo di Vigilanza (OdV) conformi al presente decreto.

**La gestione del canale di segnalazione deve essere affidata a persona o ufficio interno autonomo dedicato e con personale specificamente formato per la gestione delle segnalazioni, ovvero è affidata a un soggetto esterno, anch'esso autonomo e con personale adeguatamente formato.** Nell'ambito della PA, dove è fatto obbligo di prevedere la figura del Responsabile della prevenzione della corruzione e della trasparenza, ai sensi dell'art. 1, comma 7, della Legge 6 novembre 2012, n. 190, viene affidata a quest'ultimo la gestione del canale di segnalazione. Le modalità di accesso e di fruizione del servizio di comunicazione con l'ufficio preposto alla ricezione delle denunce devono essere rese pubbliche sul sito internet dell'Ente.

**Tra le autorità preposte alla ricezione delle denunce il decreto prevede l'ANAC (l'Autorità Nazionale Anticorruzione), che provvede secondo proprio regolamento alla ricezione e trattazione delle denunce con piattaforma dedicata,** dando opportuno riscontro alla persona segnalante dell'avvenuta ricezione, della eventuale necessità di documentazione integrativa e dell'esito finale dell'inchiesta entro tre mesi dall'avviso di ricevimento della segnalazione. L'ANAC può disporre l'invio delle segnalazioni aventi ad oggetto informazioni sulle violazioni che non rientrano nella propria competenza alla competente autorità amministrativa o giudiziaria, con contestuale avviso alla persona segnalante.

**Ogni trattamento dei dati personali, compresa la comunicazione tra le autorità competenti, previsto dal D.Lgs. 10 marzo 2023 n.24, deve essere effettuato a norma del regolamento (UE) 2016/679, del D.Lgs. 30 giugno 2003, n. 196 e del D.Lgs. 18 maggio 2018, n. 51 (a tutela della riservatezza del segnalante e di protezione e corretto trattamento dei dati trasmessi)**

Le disposizioni di cui al D.Lgs. 10 marzo 2023 n.24 **hanno effetto a decorrere dal 15 luglio 2023 per gli enti pubblici e privati con almeno 250 dipendenti. A decorrere dal 17 dicembre 2023 si prevede l'obbligo di predisporre un canale di segnalazione interna per tutti i soggetti del settore privato che abbiano impiegato nell'ultimo anno fino a 249 (duecentoquarantanove) lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato.**

## - N2) Privacy: GDPR, gli errori più comuni che fanno sanzionare le aziende

**Cosa vuol dire, in pratica “agevolare l’esercizio dei diritti”? E, soprattutto, è davvero così semplice adempiere a tale prescrizione, quando si opera in strutture articolate come le grandi imprese, i gruppi aziendali, gli enti pubblici?**

### Gli errori che possono portare a sanzioni

Il più delle volte la sanzione arriva perché l'azione ispettiva rileva delle malpractices nella gestione delle istanze di esercizio dei diritti. Facciamo alcuni esempi:

#### **1) La richiesta non viene affatto presa in considerazione**

Questo accade per mille ragioni, tra le quali potremmo elencare le seguenti:

Il punto di contatto su cui arriva la richiesta (ad esempio: e-mail, tradizionale o certificata) non è presidiato.

Quanti siti web ospitano account info@\_\_\_ attivi senza che nessuno li monitori? Molti.

Chi presidia l'account non riconosce, nel messaggio ricevuto, una istanza di esercizio dei diritti.

Partendo dal presupposto che non tutti (per fortuna) sono esperti di linguaggio giuridico, è verosimile che l'interessato medio (che guarda caso è proprio quello su cui si deve concentrare l'azione di trasparenza del Titolare) non scriva/dica cose tipo: “ai sensi e per gli effetti dell'art. 15 del Regolamento generale per la protezione dei dati personali, richiedo di ottenere la conferma che sia o meno in corso un trattamento dei dati personali che mi riguardano e, in tale primo caso, di ottenere l'accesso ai dati personali e ...”

No. Qualsiasi privacy specialist sa benissimo che l'interessato medio si divide in due categorie: c'è quello che ha il 'cugino avvocato' o che fa un copia incolla da istanze trovate su internet, e c'è una larga fascia di interessati che scrive in modo molto meno forbito e tecnico cose tipo: “chi siete? Non mi sono mai iscritto alla vostra piattaforma! Cancellate immediatamente tutte le informazioni che avete su di me! Sono stufo di ricevere le vostre e-mail! etc.”.

Siamo sicuri che chi gestisce la pec istituzionale, chi risponde al centralino ufficiale, chi presiede le reception, chi sta a contatto con i lavoratori e li coordina, chi gestisce e monitora i canali social, sappia riconoscere in una simile rimostranza una istanza di esercizio dei diritti?

**Il risultato, comunque, è che l'interessato non riceve riscontro e, in una percentuale di volte sempre più importante, si rivolge all'Autorità di Controllo.**

#### **2) La richiesta non viene processata nei tempi previsti dal GDPR**

Spesso questo accade perché:

Il Referente privacy (o chi è incaricato di dare riscontro) non riceve in tempo le istanze di esercizio dei diritti, poiché le stesse non vengono correttamente incardinate;

Spesso le richieste si fermano sulla e-mail di chi le riceve per giorni, settimane.

Oppure vengono inoltrate all'ufficio sbagliato.

Il Referente privacy (o chi è incaricato di dare riscontro) non riceve dalla struttura le informazioni necessarie a processare l'istanza.

Esempio banale ma incredibilmente comune: la struttura non risponde all'ufficio privacy che chiede contezza dell'esistenza o meno dei dati dell'interessato all'interno dei singoli data base.

In molti casi, questo non accade per inerzia o mala fede, ma semplicemente perché la struttura non è in grado di individuare le informazioni necessarie a dar seguito alla richiesta del Referente privacy.

La struttura non è in grado di identificare l'interessato.

### 3) Il Titolare risponde negativamente senza dimostrare la validità del diniego

Il più delle volte, da casistiche del genere, scaturiscono sanzioni che stigmatizzano comportamenti volutamente contrari all'obbligo di agevolare l'interessato nell'esercizio dei suoi diritti.

Tra questi vado a ricomprendere anche l'eccessiva burocrazia e formalismo in fase di identificazione dell'interessato o la previsione di percorsi non facilmente fruibili per poter presentare l'istanza.

Tutti comportamenti sanzionati. Più volte.

**Come approcciarsi, quindi, alla questione per evitare di incorrere in sanzioni?** In tutti questi casi entra in gioco alcuni punti fondamentali che ruotano però intorno ad un **unico principio: la privacy by design.**

#### **Primo punto: facilitare la vita agli interessati.**

In linea con quanto disposto dalle Autorità di Controllo (inclusa la nostra Autorità Garante) per quanto riguarda **la gestione delle richieste da parte degli interessati è necessario garantire un approccio teso alla correttezza, alla buona fede e, soprattutto, alla facilità di esercizio dei diritti.**

Sempre in ossequio alle disposizioni sanzionatorie delle Autorità di Controllo in materia, è inoltre importantissimo:

- tenere presente che l'utilizzo di un modulo ad-hoc per l'esercizio dei diritti dovrebbe essere solo alternativo agli altri canali ritenuti più comodi dagli interessati, sempre ovviamente nei limiti della razionalità della scelta.
- individuare misure che, di default, assicurino l'identificazione certa dell'interessato riducendo al minimo la necessità di richiedere documenti di identità. Ad esempio, agevolare la presentazione della richiesta a valle di un log-in a piattaforma o utilizzare canali di identificazione alternativi.
- fornire una prima risposta immediata all'interessato, che lo rassicuri circa la presa in carico della sua richiesta e lo informi delle tempistiche di riscontro, chiedendo ove possibile sin da subito eventuali necessarie ulteriori delucidazioni per ottemperare alla sua istanza.

**Secondo punto: accertarsi di intercettare tutte le istanze.** Quindi, mappare tutti i punti di contatto (ufficiali e non ufficiali) con gli interessati e disattivare i punti di contatto da remoto non presidiati (es: account e-mail/numeri di telefono pubblicati su siti web),

Accertarsi che le istanze vengano riconosciute e correttamente incardinate

**Terzo punto: accertarsi che le istanze vengano riconosciute e correttamente incardinate.** Quindi, individuare chi presidia tali punti di contatto e formarlo in modo da renderlo in grado di:

- riconoscere una istanza anche se non formulata in modo rituale/formale;
- saperla instradare correttamente sino al soggetto che dovrà offrire riscontro.

**Quarto punto: monitoraggio ed accountability.** Quindi, appuntare puntualmente la data di ricezione e la data di evasione delle singole istanze in un apposito registro.

**Quinto punto: non lasciare nulla al caso.** Quindi, redigere una procedura ad hoc.

### - N3) Privacy: Mail dipendenti: le linee guida del Garante privacy

**Il Garante ribadisce il divieto di accesso alla posta elettronica del lavoratore alla cessazione del rapporto di lavoro. Vediamo le indicazioni generali**

**L'accesso alla posta elettronica del lavoratore cessato non è mai giustificato.**

Lo ha ribadito il Garante per la privacy nella newsletter del 15 marzo 2023 in cui viene illustrato il caso di una azienda sanzionata per aver mantenuto attivo e aver visionato l'account di posta elettronica di una collaboratrice dopo la fine del rapporto di lavoro.

Nello specifico la collaborazione si era conclusa con una citazione in giudizio dopo che la collaboratrice aveva raccolto, a nome dell'azienda stessa e tramite una casella mail aperta per l'occasione, i riferimenti di potenziali clienti incontrati a una fiera. La collaboratrice, dipendente di una cooperativa aveva poi iniziato a contattare i nominativi a nome della propria cooperativa e questo aveva portato a un contenzioso giudiziale.

Per questo motivo l'azienda ha visionato le comunicazioni nella posta elettronica e contattato i potenziali clienti per indicare un nuovo dipendente di riferimento.

Il Garante ha affermato nel suo parere che, "né l'esigenza di mantenere i rapporti con i clienti né l'interesse a difendere un proprio diritto in giudizio, legittimano un tale trattamento di dati personali".

**Per salvaguardare i propri interessi economici l'azienda avrebbe dovuto invece attivare un sistema di risposta automatico, con l'indicazione di indirizzi alternativi da contattare senza entrare direttamente nell'account.**

Altro aspetto da sottolineare il fatto che malgrado la collaborazione non fosse stata ufficialmente contrattualizzata l'azienda avrebbe dovuto raccogliere il consenso al trattamento dei dati già nell'ambito delle trattative precontrattuali, sulla base di un principio generale di correttezza.

Inoltre a salvaguardia della privacy della collaboratrice avrebbe dovuto dare riscontro alla sua richiesta di cancellazione della casella e-mail

**Linee guida per l'uso della posta elettronica:** In un documento specifico pubblicato dal Garante il 10 marzo 2007, in tema di utilizzo della posta elettronica nel luogo di lavoro il Garante forniva alcune soluzioni utili per contemperare le esigenze dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori:

- renda disponibili anche indirizzi condivisi tra più lavoratori (info@ente.it; urp@ente.it; ufficioreclami@ente.it), rendendo così chiara la natura non privata della corrispondenza;
- valuti la possibilità di attribuire al lavoratore un altro indirizzo (oltre quello di lavoro), destinato ad un uso personale;
- preveda, in caso di assenza del lavoratore, messaggi di risposta automatica con le coordinate di altri lavoratori cui rivolgersi;
- metta in grado il dipendente di delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al titolare quelli ritenuti rilevanti per l'ufficio, ciò in caso di assenza prolungata o non prevista del lavoratore interessato e di improrogabili necessità legate all'attività lavorativa.
- Qualora queste misure preventive non fossero sufficienti a evitare comportamenti anomali, gli eventuali controlli da parte del datore di lavoro devono essere effettuati con gradualità. In prima battuta si dovranno effettuare verifiche di reparto, di ufficio, di gruppo di lavoro, in modo da individuare l'area

da richiamare all'osservanza delle regole. Solo successivamente, ripetendosi l'anomalia, si potrebbe passare a controlli su base individuale.

- Opportuno infine fare sì che i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta policy datoriale.

#### **-N4) Privacy: Stop del Garante a ChatGPT; Ammissibile l'utilizzo del sistema di videosorveglianza per comprovare l'inadempimento disciplinare del lavoratore;**

**Stop del Garante a ChatGPT** in Italia, finché non rispetterà la disciplina privacy. Il Garante per la protezione dei dati personali ha disposto, con effetto immediato, la limitazione provvisoria del trattamento dei dati degli utenti italiani nei confronti di OpenAI, la società statunitense che ha sviluppato e gestisce la piattaforma. L'Autorità ha contestualmente aperto un'istruttoria. Nel provvedimento, il Garante privacy rileva la mancanza di una informativa agli utenti e a tutti gli interessati i cui dati vengono raccolti da OpenAI, ma soprattutto l'assenza di una base giuridica che giustifichi la raccolta e la conservazione massiccia di dati personali, allo scopo di "addestrare" gli algoritmi sottesi al funzionamento della piattaforma. Come peraltro testimoniato dalle verifiche effettuate, le informazioni fornite da ChatGPT non sempre corrispondono al dato reale, determinando quindi un trattamento di dati personali inesatto. Da ultimo, nonostante – secondo i termini pubblicati da OpenAI – il servizio sia rivolto ai maggiori di 13 anni, l'Autorità evidenzia come l'assenza di qualsivoglia filtro per la verifica dell'età degli utenti esponga i minori a risposte assolutamente inadeguate rispetto al loro grado di sviluppo e autoconsapevolezza. OpenAI rischia sanzione fino a 20 milioni di euro o fino al 4% del fatturato globale annuo

**Ammissibile l'utilizzo del sistema di videosorveglianza per comprovare l'inadempimento disciplinare del lavoratore** Anche il sistema di videosorveglianza può essere utilizzato per comprovare l'inadempimento disciplinare del dipendente: non ha dubbi in proposito la Corte di Cassazione (Sentenza 8375/2023), che ne ha ritenuto ammissibile l'uso nonostante tale sistema rientri nell'ambito di applicazione dell'articolo 4, comma 2, dello statuto dei lavoratori, nella specie relativa a vicende ricadenti nel testo della norma anteriore alle modifiche apportate dal Jobs act. Per i giudici, in ogni caso, il ricorso alle registrazioni dei sistemi di videosorveglianza va effettuato nel rispetto delle garanzie previste dalla legge 300/1970, oltre che delle esigenze organizzative e produttive e della sicurezza sul lavoro. Nel caso sottoposto all'attenzione della Corte di cassazione, la contestazione disciplinare era stata rivolta nei confronti di un educatore professionale che, a fronte del rifiuto di alcuni studenti di obbedire a delle sue direttive, ne aveva afferrato con forza la maglietta e, successivamente, ne aveva spinto uno, procurandone la caduta. Tutte tali azioni erano state riprese dall'impianto video installato nei locali con finalità di sicurezza, in conformità alle previsioni dell'articolo 4 dello statuto dei lavoratori. Il lavoratore, nel subire il provvedimento disciplinare, aveva contestato, tra le altre cose, il ricorso alle registrazioni, ma il giudice del merito prima e la Corte di cassazione poi, hanno confermato la legittimità della valutazione delle riprese nell'ambito di una più ampia e globale considerazione delle prove raccolte a sostegno della sanzione disciplinare. Nella complessiva valutazione della vicenda erano state vagliate anche la proporzionalità della sanzione al fatto – accertata tenendo conto delle circostanze oggettive e delle modalità soggettive della condotta del lavoratore – e le giustificazioni rese da quest'ultimo – che dimostravano che il licenziamento disciplinare non era viziato, essendosi consentito all'incolpato di esercitare il proprio diritto di difesa. In tale complessivo esame, la valutazione delle riprese del sistema di sorveglianza era un elemento aggiuntivo e del tutto legittimo, anche considerato che lo stesso era chiaramente destinato a esigenze di sicurezza, essendo orientato a spazi accessibili anche a personale non dipendente e che non accolgono postazioni di lavoro ed essendo stato posizionato a seguito di un accordo sindacale.



**- N5) Ambiente: Pubblicato il DPCM che approva il MUD 2023. La scadenza per l'invio è l'8 Luglio 2023**

**È stato pubblicato nella Gazzetta Ufficiale del 10 Marzo 2023, n. 59 il decreto del Presidente del Consiglio dei Ministri che approva il Modello Unico di Dichiarazione Ambientale relativo al 2022.**

Dal 15 marzo imprese, enti, associazioni e consulenti possono operare sui portali messi a disposizione da Unioncamere per la compilazione e la trasmissione del Modello Unico di Dichiarazione ambientale.

Attraverso il portale del MUD Semplificato è possibile compilare la Comunicazione Rifiuti semplificata da inviare poi, via PEC, a [comunicazionemud@pec.it](mailto:comunicazionemud@pec.it) .

Attraverso il portale del MUD Telematico gli utenti possono trasmettere le Comunicazioni Rifiuti, Imballaggi, Rifiuti da apparecchiature elettriche ed elettroniche e Veicoli fuori uso. Sempre dallo stesso portale è possibile scaricare anche le istruzioni dettagliate e i tracciati record da seguire per le dichiarazioni predisposte con altri software nonché accedere al programma per il controllo formale del MUD.

Infine i soggetti istituzionali responsabili del servizio di gestione integrata dei rifiuti urbani accedono alla piattaforma MUD Comuni per la compilazione e trasmissione della Comunicazione Rifiuti urbani e raccolti in convenzione.

Sempre dal 15 marzo sono disponibili le FAQ che Ecocerved ha predisposto per supportare gli utenti nella compilazione del MUD. <https://www.ecocamere.it/faqs/MUD>



**“Auguri di un Serena Pasqua”**

***Voglia gradire i nostri più cordiali saluti***

***ing. Giorgio Violi   ing. Alberto Sant'Unione***

PregandoLa di scusarci per il disturbo eventualmente arrecato, Le comuniciamo che i Suoi dati sono registrati nel Database Studio Violi srl e questo messaggio Le è stato inviato confidando che i temi trattati potessero essere di Suo interesse. In ottemperanza al Reg. 679/2016/UE, qualora non desiderasse più ricevere questo mensile dallo Studio Violi srl (titolare del trattamento dei dati), può comunicarcelo via mail all'indirizzo [info@studiovioli.com](mailto:info@studiovioli.com). Garantiamo in ogni momento il rispetto di tutti i diritti di cui al Reg. 679/2016/UE.

Credits:si ringraziano le società che hanno facilitato la stesura del presente con la fornitura di parte del materiale, in particolare garante privacy, punto sicuro, ats, ipsoa, il sole24ore, tuttoambiente, iae, quotidiano sicurezza.it, privacylawconsulting, la repubblica, italia oggi, epc, postilla, necsi. Può inoltre contare sulla ns disponibilità ad approfondire i temi qui trattati