PROTEZIONE DEI DATI PERSONALI: LE RECENTI EVOLUZIONI NORMATIVE, ATTUATIVE ED INTERPRETATIVE

Il Garante per la protezione dei dati personali ha verificato la conformità al GDPR dei **codici di deontologia e buona condotta** nonché delle **autorizzazioni generali** che erano stati emanati sulla base della normativa previgente. **Le regole conformi costituiranno disposizioni vincolanti** e la loro violazione sarà soggetta alla sanzione amministrativa più grave (fino a euro 20.000.000 ovvero 4% del fatturato mondiale annuo).

Altre novità hanno caratterizzato il periodo successivo all'entrata in vigore lo scorso settembre del D.Lgs. 101/2018, di adeguamento della normativa nazionale al GDPR ("**Decreto GDPR**"): il Garante ha individuato un elenco di tipologie di trattamenti sicuramente soggetti a **valutazione d'impatto** sulla protezione dei dati e ha sottoscritto un **protocollo d'intesa** con la Procura della Repubblica di Roma per rendere più celeri ed efficaci le azioni di accertamento degli illeciti in materia di protezione dei dati personali.

In evidenza

- Verificata la conformità al GDPR dei codici di deontologia e buona condotta e delle autorizzazioni generali
- La violazione delle regole deontologiche e delle autorizzazioni generali sarà soggetta alla sanzione amministrativa più grave
- Eliminata dalle regole deontologiche la possibilità di differire l'informativa agli interessati in caso di raccolta dei dati presso di loro
- Individuate prescrizioni specifiche sui trattamenti effettuati in fase preassuntiva
- Individuate tipologie di trattamenti da sottoporre alla DPIA
- Nuovo contenzioso *privacy* dei c.d. ciclofattorini Foodora
- Procedure più celeri ed efficaci per l'accertamento di violazioni connesse a reati

LE "NUOVE" REGOLE DEONTOLOGICHE

Con cinque provvedimenti susseguitisi tra novembre e dicembre 2018[1], il Garante per la protezione dei dati personali (il "**Garante**") ha verificato la conformità al Regolamento europeo sulla protezione dei dati personali n. 2016/679 ("**GDPR**") delle disposizioni contenute nei codici di deontologia e buona condotta relativi al trattamento dei dati personali nell'esercizio dell'**attività giornalistica**, per scopi di **ricerca storica, statistici, di ricerca scientifica** e per lo svolgimento di **investigazioni difensive**, finora riportati negli allegati A.1, A.2, A.3, A.4 ed A.6 al D.Lgs. n. 196/2003 ("**Codice Privacy**").

I testi aggiornati con le disposizioni ritenute conformi al GDPR, **rinominati «*regole deontologiche*»** ai sensi del comma 4 dell'art. 20 del Decreto GDPR, sono stati trasmessi al Ministero della Giustizia per essere riportati con decreto nell'**Allegato A) del Codice Privacy** novellato dal Decreto GDPR. Le regole deontologiche sul trattamento nell'esercizio dell'attività giornalistica e per finalità statistiche e di ricerca scientifica sono state pubblicate rispettivamente nella Gazzetta Ufficiale della Repubblica italiana ("**GUCE**")

[1] Provvedimenti n. 491 del 29 novembre 2018 e nn. 512, 513, 514 e 515 del 19 dicembre 2018, disponibili al seguente *link*: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069732.

n. 3 del 4 gennaio 2019 e n. 11 del 14 gennaio 2019, mentre quelle sul trattamento per lo svolgimento di investigazioni difensive sono state pubblicate nel n. 12 del 15 gennaio 2019[2].

A decorrere dalla pubblicazione nella GUCE, le regole deontologiche integrano una **condizione essenziale per la liceità e la correttezza del trattamento** dei dati personali (art. 2-*quater*, comma 4, del novellato Codice Privacy). La loro violazione è soggetta alla **sanzione amministrativa pecuniaria** fino a euro 20.000.000 ovvero, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 166, comma 2, del novellato Codice Privacy).[3]

Quanto al contenuto delle regole deontologiche, gli interventi del Garante si sono orientati in una duplice direzione, formale e sostanziale:

Modifiche formali	Modifiche sostanziali
Aggiornati i riferimenti normativi e la semantica utilizzata rispetto al rinnovato quadro normativo dettato dal GDPR e dal novellato Codice Privacy. In particolare, non vi sono modifiche sostanziali per i "vecchi" allegati A.1 (*attività giornalistica*), A.2 (*ricerca storica*) e A.6 (*investigazioni difensive*).	Eliminate le disposizioni che consentivano al titolare di fornire informative differite e/o semplificate all'interessato in caso di raccolta di dati personali presso l'interessato stesso. Ciò in quanto l'art. 13 del GDPR non prevede per tale ipotesi alcuna forma di differimento e/o semplificazione degli obblighi informativi.
Eliminato il *Preambolo* di tutti i codici, in quanto l'art. 20 del Decreto GDPR imponeva solo di verificare le "*disposizioni*" contenute nei codici.	Eliminate le disposizioni che obbligavano il titolare, in relazione ai dati personali raccolti presso terzi, a comunicare in via preventiva al Garante le modalità individuate per dare pubblicità all'informativa.
	Eliminate le disposizioni che disciplinavano le condizioni di liceità del trattamento (essendo queste ora disciplinate dagli artt. 6 e 7 del GDPR).
	Eliminate le disposizioni che disciplinavano il trasferimento dei dati personali verso i paesi terzi (essendo ad esso dedicati gli artt. 44 e ss. del GDPR).

Diversa è la sorte dei rimanenti "vecchi" allegati **A.5 ed A.7** al Codice Privacy, rispettivamente relativi ai **sistemi informativi** gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti ed al trattamento di dati effettuato a fini di **informazione commerciale**. Ai sensi del comma 1 dell'art. 20, tali allegati **resteranno in vigore fino al 19 settembre 2019**, a condizione che:

- entro il 19 marzo 2019 le associazioni e gli altri organismi rappresentanti le categorie di titolari ovvero responsabili del trattamento **sottopongano all'approvazione** del Garante dei **codici di condotta** elaborati a norma dell'art. 40, paragrafo 2, GDPR;
- tale **approvazione** avvenga entro i successivi 6 mesi.

[2] Come precisato dal Garante nel comunicato stampa del 28 dicembre 2018, in sede di prima applicazione l'art. 20 del Decreto GDPR stabilisce unicamente che il Garante ripubblichi i "vecchi" codici, emendati dalle disposizioni incompatibili con il GDPR, senza prevedere alcuna consultazione pubblica. Tuttavia, la **consultazione pubblica è prevista per le regole deontologiche che verranno adottate da oggi in poi o per le eventuali ulteriori modifiche ai testi già adottati**. Resta, infatti, ferma la possibilità che il Garante promuova una successiva revisione di tali disposizioni ovvero l'adozione di nuove regole deontologiche, questa volta secondo la procedura di cui all'art. 2-*quater* del novellato Codice Privacy, che prevede una consultazione pubblica per almeno sessanta giorni nell'osservanza del principio di rappresentatività.

[3] Al contempo, i "vecchi" codici di deontologia e di buona condotta di cui agli allegati A.1, A.2, A.3, A.4 ed A.6 al Codice Privacy hanno cessato di produrre effetti, secondo quanto previsto dall'art. 20, comma 3, del Decreto GDPR.

Il mancato rispetto di uno dei predetti termini comporterà la perdita di efficacia delle disposizioni dei richiamati allegati a decorrere dalla scadenza di tale termine.

Al di là delle differenze procedurali stabilite per i due gruppi di allegati, evidenziamo la diversità **strutturale** e **funzionale** delle *regole deontologiche* rispetto ai *codici di condotta* di cui all'art. 40, paragrafo 2, GDPR.

	Regole deontologiche	***Codici di condotta***
Differenze strutturali	Le *regole deontologiche* possono intervenire **unicamente nei settori individuati** dal GDPR e dal Codice Privacy (art. 2-*quater* del Codice Privacy). Ossia nell'ambito dei trattamenti previsti ai sensi degli artt. 6, paragrafo 1, lett. c) ed e), 9, paragrafo 4, e del Capo IX del GDPR: rapporti di lavoro e trattamenti dei dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da registri pubblici, ovvero ai fini di archiviazione nel pubblico interesse o di ricerca storica e ai fini statistici e di ricerca scientifica (artt. 61, 102, 106 e 111 del Codice Privacy).	I *codici di condotta* possono intervenire in **qualsiasi settore**. Solo a titolo esemplificativo e non esaustivo, il paragrafo 2 dell'art. 40 GDPR elenca undici materie in cui viene promossa, a livello europeo, l'elaborazione di codici di condotta.
Differenze funzionali	Le *regole deontologiche* assumono la natura di vere e proprie **regole vincolanti** elaborate dal Garante quali **condizioni di essenziali di liceità e correttezza del trattamento.** Tanto che la loro violazione è soggetta alla sanzione amministrativa più grave (fino a euro 20.000.000 ovvero 4% del fatturato mondiale annuo).	Nella visione del legislatore europeo, i codici di condotta sono uno strumento di autoregolamentazione da parte delle associazioni e/o altri organismi rappresentanti le categorie dei titolari o responsabili del trattamento. Sono approvati dal Garante solo in un secondo momento ed il loro mancato rispetto non determina l'illiceità del trattamento.

LE AUTORIZZAZIONI GENERALI

Con provvedimento del 13 dicembre 2018[4], il Garante ha (i) individuato le prescrizioni contenute nelle autorizzazioni generali adottate ai sensi degli - ormai abrogati - artt. 26 e 40 del Codice Privacy[5] che risultano ancora compatibili con il GDPR e con il Decreto GDPR ed (ii) **avviato una procedura di consultazione pubblica** della durata di 60 giorni, volta ad acquisire osservazioni e proposte riguardo alle suddette prescrizioni.
L'art. 21 del Decreto GDPR, al comma 1, ha limitato l'ambito della verifica alle autorizzazioni generali relative alle situazioni di trattamento di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 2, lettera b) e 4, nonché al Capo IX del GDPR, vale a dire:

- trattamenti necessari per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

[4] Disponibile al *link*: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9068972.
[5] Si ricorda come, ai sensi del previgente art. 26 del Codice Privacy, i dati sensibili (oggi chiamati dal GDPR "*categorie particolari di dati personali*"), per poter costituire oggetto di trattamento necessitavano del (i) consenso scritto dell'interessato e della (ii) preventiva autorizzazione del Garante. Solo in particolari casi – elencati al comma 4 della disposizione citata – era consentito il trattamento in presenza della sola autorizzazione del Garante.

- trattamenti necessari per assolvere gli obblighi ed esercitare specifici diritti del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza e protezione sociale, nonché dati genetici, biometrici e relativi alla salute;
- trattamenti effettuati in ambiti specifici, quali rapporti di lavoro, dati provenienti da archivi, registri, elenchi, atti o documenti tenuti da registri pubblici, trattamenti ai fini di archiviazione nel pubblico interesse o di ricerca storica e ai fini statistici e di ricerca scientifica.

Pertanto, il Garante ha verificato solamente le autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 concernenti, rispettivamente, il trattamento di dati sensibili (*rectius* di categorie particolari di dati personali): nei rapporti di lavoro; da parte di organismi di tipo associativo, fondazioni, chiese, associazioni o comunità religiose; da parte degli investigatori privati; concernenti dati genetici; per scopi di ricerca scientifica.

Il Garante è intervenuto **nel merito** delle autorizzazioni alla luce dei nuovi principi europei. Ad esempio:

- il Garante ha introdotto prescrizioni specifiche per il trattamento di categorie particolari di dati **in fase preassuntiva,** tra l'altro disponendo che:
  - i **questionari preassuntivi** devono riguardare le sole informazioni strettamente pertinenti e limitate a quanto necessario ai fini dell'instaurazione del rapporto di lavoro anche tenendo conto delle particolari mansioni e/o specificità dei profili professionali richiesti (sotto il profilo giuslavoristico, ricordiamo tra l'altro che l'art. 8 L. 300/1970 vieta le indagini su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore);
  - qualora nei **c.v. inviati dai candidati** siano presenti dati non pertinenti rispetto a tale finalità, i selezionatori devono astenersi dall'utilizzare tali informazioni;
  - i **dati genetici non possono essere trattati** al fine di stabilire l'idoneità professionale dell'interessato, neppure con il suo consenso;
- quanto ai trattamenti **nel corso del rapporto di lavoro,** il Garante ha precisato, tra l'altro, che:
  - il datore di lavoro può trattare dati che rivelino le **opinioni politiche o l'appartenenza sindacale** o l'esercizio delle relative funzioni esclusivamente ai fini della fruizione di permessi/aspettative e per consentire l'esercizio dei diritti sindacali (es. trattenute in busta paga);
  - in particolare, richiamando il principio di necessità, il Garante ha disposto che, per la partecipazione ad operazioni elettorali, è sufficiente la certificazione del presidente di seggio, pertanto il datore di lavoro non può richiedere il documento che designa il rappresentante di lista rilevandone l'opinione politica.

  Segnaliamo che nella stessa prospettiva il Garante aveva ritenuto sufficiente per il datore di lavoro comunicare alla rappresentanza sindacale la revoca della precedente affiliazione sindacale di alcuni membri, e quindi dichiarato illegittima la rivelazione della contestuale iscrizione ad altro sindacato (cfr. doc. web n. 9065999 in **newsletter del 7 dicembre 2018**)[6].
- in tutte le autorizzazioni verificate, il Garante ha eliminato le sezioni che si limitavano genericamente a riportare che i dati "*potranno essere conservati per un periodo non superiore a quello necessario (…) per perseguire le finalità ivi menzionate*".

Il comma 5 dell'art. 20 del Decreto GDPR specifica che le violazioni delle prescrizioni contenute nelle autorizzazioni generali sono soggette alla **medesima sanzione amministrativa pecuniaria** prevista in caso

[6] Disponibile al *link*: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9065999.

di violazione delle *regole deontologiche* (come già menzionato, fino a euro 20.000.000 ovvero 4% del fatturato mondiale annuo).

Le altre autorizzazioni generali adottate dal Garante prima del 19 settembre 2018, relative a trattamenti diversi da quelli sopra indicati, hanno **cessato di produrre effetti** in tale data (art. 21, comma 3, Decreto GDPR)[7].

LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Con provvedimento dell'11 ottobre 2018[8], il Garante ha pubblicato l'**elenco delle tipologie di trattamenti di dati personali da sottoporre a valutazione d'impatto sulla protezione dei dati** (**"DPIA"**)[9] ai sensi di quanto disposto dall'art. 35, paragrafo 4, del GDPR. Il Garante ha dato atto di aver recepito le osservazioni del Comitato europeo per la protezione dati e che resta fermo quanto indicato nelle linee guida WP 248, rev. 01[10], in un'ottica di armonizzazione e di applicazione coerente del GDPR e di trattamento transfrontaliero.

Tra i trattamenti elencati dal Garante[11] rientrano:

- quelli che comportano la **profilazione** degli interessati nonché lo svolgimento di attività predittive, tra cui in relazione a rendimento professionale, situazione economica, salute, affidabilità, spostamenti;
- quelli **automatizzati** finalizzati ad assumere decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto (tra essi il Garante include lo *screening* dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi);
- quelli che concernono trattamenti su larga scala di dati aventi carattere **estremamente personale**, tra cui i dati connessi alla vita familiare o privata (quali i dati relativi alle e comunicazioni elettroniche dei quali occorre tutelare la riservatezza), i dati sull'ubicazione, i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti;
- quelli che concernono, più in generale, categorie particolari di dati personali ai sensi dell'art. 9 del GDPR o dati relativi a condanne penali e a reati ex art. 10 del GDPR **interconnessi con altri** dati personali raccolti per finalità diverse;
- quelli che comportano lo scambio **tra diversi titolari** di dati su larga scala con modalità telematiche.

Risulta, dunque, confermata un'applicazione ampia della DPIA, che già si era diffusa nella prassi.

Nel predetto elenco del Garante rientrano anche i trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di **geolocalizzazione**) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti. Ricordiamo che in relazione a tali sistemi è anche richiesto l'accordo con le rappresentanze sindacali e/o l'autorizzazione dell'Ispettorato del Lavoro ex art. 4 L. 300/1970 come novellato dall'art. 23 D.Lgs. 151/2015 (c.d. *Jobs Act*),

---

[7] In particolare, hanno cessato di produrre effetti dal 19 settembre 2018 le autorizzazioni nn. 7/2016 e 2, 4 e 5 del 2016, rispettivamente in tema di: (i) trattamento dei dati giudiziari da parte di privati, enti pubblici economici e soggetti pubblici, (ii) trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, (iii) trattamento dei dati sensibili da parte dei liberi professionisti e (iv) trattamento dei dati sensibili da parte di diverse categorie di titolari.

[8] L'elenco è disponibile al *link*: https://www.garanteprivacy.it/documents/10160/0/ALLEGATO+1+Elenco+delle+tipologie+di+trattamenti+soggetti+al+meccanismo+di+coerenza+da+sottoporre+a+valutazione+di+impatto

[9] La DPIA è la procedura di analisi dei trattamenti eseguiti, dei dati trattati e delle finalità, al fine di valutare i rischi per i diritti e le libertà degli interessati, che è obbligatorio effettuare prima di procedere ad un tipo di trattamento che può presentare un rischio elevato sotto tale profilo.

[10] Disponibile al *link*: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[11] Per espressa previsione del Garante, tale elenco non è esaustivo, potendo lo stesso essere ulteriormente integrato ovvero modificato anche sulla base delle risultanze emerse nel corso della prima fase di applicazione del GDPR.

fatta eccezione per gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e per gli strumenti di lavoro o di registrazione degli accessi e delle presenze.

Sotto questo profilo, segnaliamo i recenti sviluppi della controversia giuslavoristica dei c.d. **ciclofattorini (*rider*) Foodora** che lavoravano tramite ***app* installate sullo *smartphone*.** Gli stessi avevano richiesto un risarcimento danni proprio per violazione dell'art. 4 L. 300/1970, oltre che degli artt. 7, 11 e 171 del Codice Privacy previgente per non aver ricevuto un'informativa chiara e completa sulla natura dei dati trattati, sulle caratteristiche del dispositivo e dei controlli e sulle ipotesi in cui era consentita la disattivazione della funzione di localizzazione nel corso della prestazione lavorativa. In primo grado, tutte le loro domande erano state rigettate dal Tribunale di Torino (sentenza 778/2018).

La Corte d'Appello di Torino, con sentenza 26/2019 dell'11 gennaio 2019 di cui si attendono le motivazioni, ha parzialmente accolto l'appello dei *rider*, riconocendo loro la stessa retribuzione dei dipendenti per effetto dell'equiparazione ex art. 2 D.Lgs. 81/2015, senza riqualificare il loro rapporto in lavoro subordinato. **Sotto il profilo *privacy*, la Corte d'Appello non ha riformato la sentenza di primo grado**, che, tra l'altro, aveva ritenuto che l'informativa fornita ai *rider* non fosse generica e che *"le applicazioni dello smartphone venivano utilizzate dai ricorrenti per rendere la prestazione lavorativa e, in quanto tali, non richiedevano l'accordo con le rappresentanze sindacali".*

I *rider* hanno tuttavia reso noto di aver **presentato nel dicembre 2018 un reclamo al Garante** ex art. 77 GDPR adducendo nuovi argomenti di doglianza, tra cui il controllo e la tracciatura, continui e senza autorizzazione, dei *rider* anche fuori servizio.

IL PROTOCOLLO D'INTESA TRA LA PROCURA DELLA REPUBBLICA E IL GARANTE

Si segnala, inoltre, il **protocollo d'intesa** sottoscritto in data 8 gennaio 2019 (il "**Protocollo**") tra la Procura della Repubblica di Roma ed il Garante per l'attuazione delle nuove norme sulla protezione dei dati personali introdotte dal Decreto GDPR[12]. Il Protocollo ha efficacia biennale ed è rinnovabile tacitamente.

Il Protocollo disciplina le modalità attuative degli artt. 167, comma 4, 167-*bis*, comma 3, e 167-*ter*, comma 2, del Codice Privacy, introdotti dal Decreto GDPR, che impongono al **pubblico ministero di informare "*senza ritardo*" il Garante** qualora abbia notizia di specifici reati in materia di protezione dei dati personali, richiamati dai citati articoli.

Ciò al fine di rendere più celere l'esercizio dell'azione di accertamento degli eventuali illeciti e coordinare nella maniera più efficiente i procedimenti sanzionatori penale e amministrativo.

A tal fine, si prevede in particolare che:

- il **pubblico ministero** assegnatario del procedimento (e non il Procuratore della Repubblica) informi direttamente il Garante, così da assicurare la celerità dell'informazione ed evitare dilazioni burocratiche; e
- a partire dall'avvenuta notifica alla persona sottoposta alle indagini ed al difensore dell'avviso di cui all'art. 415-*bis* c.p.p. (avviso della conclusione delle indagini preliminari), il pubblico ministero è tenuto ad effettuare la comunicazione al Garante degli elementi necessari ai fini dell'accertamento di eventuali illeciti in materia di protezione dei dati personali correlati al fatto di reato[13]. Tale procedura è finalizzata alla maggior efficienza dell'azione del Garante nel rispetto del segreto investigativo in relazione al procedimento penale in corso.

[12] Il testo del Protocollo è disponibile al *link:*https://www.garanteprivacy.it/documents/10160/0/Protocollo+tra+Procura+di+Roma+e+Garante+privacy+-+8+gennaio+2019.

[13] Il comma 2 dell'art. 1 del Protocollo specifica inoltre che «*l'informativa di cui al comma 1 contiene tutti gli elementi necessari ai fini dell'istruzione, da parte del Garante, dei procedimenti amministrativi eventualmente correlati al fatto di reato*».

CLIFFORD
CHANCE

AUTORI

Simonetta Candela
Partner, Milan

T +39 02 8063 4245
E simonetta.candela
@cliffordchance.com

Luciano Di Via
Partner, Rome

T +39 064229 1265
E luciano.divia@
cliffordchance.com

Carlo Felice Giampaolino
Partner, Rome

T +39 064229 1356
E carlofelice.giampaolino
@cliffordchance.com

Fabio Guastadisegni
Partner, Milan

T +39 02 8063 4353
E fabio.guastadisegni
@cliffordchance.com

Marina Mobiglia
Senior Associate, Milan

T +39 02 8063 4339
E marina.mobiglia
@cliffordchance.com

Andrea Tuninetti Ferrari
Senior Associate, Milan

T +39 02 8063 4435
E andrea.tuninettiferrari
@cliffordchance.com

Alessandro Sciarra
Associate, Rome

T +39 064229 1384

E alessandro.sciarra
@cliffordchance.com

Iolanda D'Anselmo
Trainee Lawyer, Milan

T +39 02 8063 4294
E iolanda.danselmo
@cliffordchance.com

NETWORK

Maxime D'Angelo Petrucci
Avocat, Paris

T +33 1 4405 5167
E maxime.dangelopetrucci
@cliffordchance.com

Megan Gordon
Partner, Washington DC

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Jonathan Kewley
Partner, London

T +44 207006 3629
E jonathan.kewley
@cliffordchance.com

Dessislava Savova
Partner, Paris

T +33 1 4405 5483
E dessislava.savova
@cliffordchance.com

Grégory Sroussi
Avocat, Paris

T +33 1 4405 5248
E gregory.sroussi
@cliffordchance.com

Richard Jones
Director of Data Privacy, London

T +44 20 7006 8238
E richard.jones
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, Piazzetta M.Bossi, 3, 20121 Milano, Italia

Clifford Chance Studio Legale Associato

Abu Dhabi • Amsterdam • Barcellona • Pechino • Bruxelles • Bucharest • Casablanca • Dubai • Düsseldorf • Francoforte • Hong Kong • Istanbul • Londra • Lussemburgo • Madrid • Milano • Mosca • Monaco di Baviera • Newcastle • New York • Parigi • Perth • Praga • Roma • San Paolo del Brasile • Seoul • Shanghai • Singapore • Sydney • Tokyo • Varsavia • Washington, D.C.

Clifford Chance ha un accordo di cooperazione con Abuhimed Alsheikh Alhagbani Law Firm a Riad

Clifford Chance ha un rapporto di collaborazione con Redcliffe Partners in Ucraina.