L'ITALIA SI ADEGUA AL GDPR

Il **19 settembre 2018** entra in vigore il d.lgs. n. 101/2018 ("**Decreto**"), pubblicato in data 5 settembre 2018, con cui l'Italia ha aggiornato il proprio Codice in materia di protezione dei dati personali (d.lgs. 196/2003, "**Codice**"), a seguito dell'entrata in vigore del Regolamento generale sulla protezione dei dati ("**GDPR**")[1].

La nuova versione del Codice richiama il GDPR quale disciplina di riferimento per il trattamento dei dati personali, che deve avvenire "*nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona*". Il Decreto introduce rilevanti novità, anche in materia di sanzioni amministrative e penali e di definizione agevolata dei procedimenti sanzionatori pendenti.

Aspetti principali

- Sanzione più grave a tutela del consenso dei minori, dei destinatari di "comunicazioni indesiderate", dei dati sensibili
- Età minima di 14 anni per il rilascio del consenso
- Sanzioni penali e definizione agevolata dei contenziosi pendenti
- Regole di condotta per il trattamento dei dati nell'ambito dei rapporti di lavoro
- Specifici obblighi a carico degli operatori di servizi di comunicazione elettronica
- Cumulo degli obblighi di notifica ai sensi del GDPR e della Direttiva NIS

IL NUOVO CODICE PRIVACY

NOVITÀ

- **Minori:** per il rilascio del **consenso all'offerta diretta di servizi della società dell'informazione, 14 anni** è l'età minima stabilita in Italia nell'esercizio della facoltà prevista dal GDPR (art. 8), che fissa i 16 anni quale *standard* minimo europeo ma lascia liberi gli Stati Membri di abbassare tale soglia fino a 13 anni.
- **Dati genetici, biometrici e relativi alla salute:** in attuazione dell'art. 9, comma 4, GDPR, il Decreto prevede l'adozione di **misure di garanzia** per il trattamento dei dati genetici, biometrici e relativi alla salute da parte dell'Autorità Garante per la protezione dei dati personali ("**Garante Privacy**"), da aggiornare con cadenza biennale. Le stesse misure, il cui rispetto costituisce **condizione di liceità del trattamento**, individuano modalità semplificate per la prestazione del consenso, quando richiesto. Inoltre, il Decreto ha introdotto un generale divieto di diffusione dei dati biometrici, genetici e relativi alla salute (divieto già presente nel Codice per

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).[2] A tale categoria di soggetti esentati si aggiungono i fornitori di reti pubbliche di comunicazioni, nonché i fornitori di servizi fiduciari (es., fornitori di servizi di firma elettronica) di cui al regolamento eIDAS (Regolamento (UE) 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE).

quest'ultima categoria di dati). Ciò significa che non è consentito dare conoscenza dei dati personali in questione a soggetti indeterminati, anche attraverso la loro messa a disposizione o consultazione. Il Decreto consente l'uso di dati biometrici per implementare procedure di accesso riservato ai dati personali, nell'ambito delle misure tecniche e organizzative a tutela dei dati personali, che i titolari del trattamento devono implementare ai sensi dell'art. 32 GDPR.

- **Dati relativi a condanne penali e reati** (quando il trattamento non avviene sotto il controllo dell'autorità pubblica): il trattamento di tali dati è consentito solo se autorizzato da una norma di legge o da un regolamento, se così previsto dalla legge, che prevedano garanzie appropriate per i diritti e le libertà degli interessati. In assenza di tale autorizzazione, il trattamento in questione e le relative garanzie sono determinati da un decreto del Ministro della Giustizia, sentito il Garante Privacy.
- **Limitazioni ai diritti degli interessati** (artt. 15-22 GDPR: accesso, rettifica, "oblio", limitazione del trattamento, portabilità, opposizione, tutele nell'ambito dei trattamenti automatizzati): l'esercizio di tali diritti nei confronti del titolare del trattamento o con reclamo al Garante Privacy è precluso nei limitati casi in cui lo stesso potrebbe pregiudicare altri diritti o interessi rilevanti (es., interessi tutelati dalla normativa antiriciclaggio). Il Decreto prevede che della limitazione, del ritardo o dell'esclusione dall'esercizio di tali diritti deve essere fornita senza ritardo "comunicazione motivata" all'interessato.
- **Delega di funzioni e compiti:** il titolare del trattamento (*controller*) o il responsabile (*processor*), ove designato, possono sotto la propria responsabilità attribuire a persone fisiche che operano sotto la propria autorità compiti e funzioni inerenti al trattamento. Tali figure sostituiscono gli "incaricati al trattamento", previsti dalla precedente versione del Codice e non più regolati dal Codice.
- "***Robinson List***": è confermato il divieto di trattamento per finalità di c.d. "marketing diretto" in relazione ai dati personali contenuti in pubblici elenchi cartacei o elettronici, quando gli interessati abbiano esercitato il proprio diritto di opposizione mediante l'iscrizione nel Registro Pubblico delle Opposizioni.
- **Linee Guida**: il Decreto attribuisce al Garante Privacy il potere di adottare linee guida di indirizzo sulle misure organizzative e tecniche di attuazione dei principi del GDPR, ivi incluso il principio di minimizzazione del trattamento dei dati, nell'esercizio della facoltà prevista per ogni Stato Membro dall'art. 58, comma 6, GDPR.
- **Regole deontologiche nell'ambito del rapporto di lavoro**: al Garante Privacy spetta altresì promuovere l'adozione di regole deontologiche per il trattamento effettuato nell'ambito del rapporto di lavoro, prevedendo anche specifiche modalità per le informazioni da rendere all'interessato, nell'esercizio della facoltà prevista per ogni Stato Membro dall'art. 88 GDPR. Il rispetto delle regole deontologiche, che verranno pubblicate nella Gazzetta Ufficiale della Repubblica Italiana con decreto del Ministro della Giustizia, **costituirà condizione essenziale per la liceità e la correttezza** del trattamento.
- **Trattamento senza necessità di consenso dei dati contenuti nei *cv***: il Decreto prevede espressamente che, nei casi di ricezione dei *curricula*

spontaneamente trasmessi dagli interessati al fine dell'instaurazione di un rapporto di lavoro, l'informativa deve essere fornita solo nel momento del primo contatto utile. Nei limiti delle finalità di esecuzione di misure precontrattuali adottate su richiesta dell'interessato (art. 6, comma 1, lettera b), GDPR), il consenso al trattamento dei dati personali presenti nei curricula non è dovuto.

SANZIONI AMMINISTRATIVE

È prevista la sanzione più grave, fino **a 20.000.000,00 Euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo**, se superiore, per la violazione, tra gli altri:

– delle disposizioni in materia di consenso dei minori;

– delle disposizioni relative alle c.d. "comunicazioni indesiderate";

– delle disposizioni sul trattamento dei dati relativi al traffico di abbonati ed utenti trattati da parte del fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico;

– delle misure di garanzia sul trattamento dei dati genetici, biometrici e relativi alla salute;

– delle regole deontologiche per specifici trattamenti, incluse quelle relative al trattamento dei dati personali nell'ambito di rapporti di lavoro;

– dei provvedimenti IVASS relativi alle procedure e alle modalità di funzionamento della banca dati dei sinistri istituita per la prevenzione e il contrasto di comportamenti fraudolenti nel settore RCA obbligatoria;

– del divieto di comunicare a terzi, trasferire e diffondere dati personali degli iscritti al Registro Pubblico delle Opposizioni per fini di pubblicità o di vendita ovvero per il compimento di ricerche di mercato o di comunicazione commerciale non riferibili alle attività, ai prodotti o ai servizi offerti dal titolare del trattamento.

SANZIONI PENALI

Con riferimento alle sanzioni penali si evidenzia che, nonostante nella prima bozza del Decreto si volesse operare una massiccia depenalizzazione eliminando radicalmente le sanzioni penali, nel nuovo Decreto di adeguamento al GDPR continuano a vivere fattispecie incriminatrici: alcune di esse erano già presenti nel "vecchio" Codice, altre sono di nuova introduzione.

Viene comunque confermata la volontà di **non includere** i reati in materia di protezione dei dati personali nell'elenco dei reati presupposto *ex* d.lgs. n. 231/2001.

- **Trattamento illecito dei dati**

  La disposizione di cui all' art. 167 del Codice è stata mantenuta, ma è attualmente applicabile non solo alle condotte sorrette dalla volontà di trarre profitto come in precedenza, bensì è formulata in modo da includere anche le condotte poste in essere con l'intenzione di arrecare un danno agli altri.

  Il reato è punito con la reclusione da 6 mesi a un anno e 6 mesi. La pena è aumentata, con la reclusione fino a 3 anni, nel caso di trattamento illecito di *categorie particolari di dati* (ai sensi dell'art. 9 GDPR) e dati penali ai sensi dell'art. 10 del Regolamento al fine di trarre profitto per sé o per altri

ovvero di arrecare danno all'interessato, nonché quando i medesimi dati sono trattati in presenza di rischi elevati per l'esecuzione di un compito di interesse pubblico arrecando nocumento all'interessato.

È previsto un flusso informativo tra il Pubblico Ministero e il Garante Privacy tale per cui il Pubblico Ministero informa, senza ritardo, il Garante Privacy quando ha notizia dei reati di cui all'art. 167 del Codice e il Garante Privacy trasmette al Pubblico Ministero, con una relazione motivata, la documentazione raccolta nel corso dell'accertamento qualora presupponga l'esistenza di un reato.

Per evitare che la pena inflitta risulti eccessivamente aspra, qualora risultasse applicabile al caso concreto anche la sanzione amministrativa, la pena dovrà essere diminuita.

- **Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala**

  All'art. 167-*bis* del Codice viene introdotta una nuova fattispecie di reato volta a punire le condotte di diffusione di dati su larga scala in caso di inosservanza di specifici requisiti normativi (ad es. del mancato consenso dell'interessato) quando sorrette dalla volontà di arrecare danno agli altri o di trarre un profitto per sé o per altri.

  Le violazioni sono punite con la reclusione da 1 a 6 anni ma, in caso di applicazione congiunta di una sanzione amministrativa, la pena dovrà essere ridotta.

- **Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala**

  Un'ulteriore disposizione incriminatrice è contenuta nell'art. 167-ter del Codice. Con essa si punisce la condotta di chi, al fine di trarre profitto ovvero di arrecare danno ad altri, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala. La disposizione è strettamente connessa a quella di cui all'art. 167-bis e in questo caso la cornice edittale prevede la reclusione da 1 a 4 anni.

- **Falsità nelle dichiarazioni al Garante Privacy e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante Privacy**

  Si mantiene il previgente art. 168 del Codice, che punisce la dichiarazione o l'attestazione di falso al Garante Privacy con la reclusione da 6 mesi a 3 anni. Inoltre, viene punito con la pena della reclusione fino a 1 anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante Privacy o degli accertamenti dallo stesso svolti.

- **Inosservanza dei provvedimenti del Garante Privacy**

  È stato mantenuto il reato previsto ex art. 170 del Codice, nonostante inizialmente fosse intervenuta una proposta di abrogazione. È prevista la pena della reclusione da 3 mesi a 2 anni.

- **Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori**

  Si mantiene altresì l'art. 171 del Codice in materia di reati per violazioni della normativa lavoristica. Le condotte sanzionate sono l'utilizzo di strumenti finalizzati al controllo dell'attività dei lavoratori o l'installazione di strumenti di controllo c.d. potenziale senza accordo con le rappresentanze

dei lavoratori o autorizzazione dell'Ispettorato del Lavoro (art. 4 l. n. 300/1970, c.d. Statuto dei Lavoratori), nonché le indagini su fatti non rilevanti ai fini della valutazione dell'attitudine professionale dei lavoratori (art. 8 l. n. 300/1970). Salvo che il fatto non costituisca più grave reato, tali condotte sono sanzionate con l'ammenda da 154,00 a 1.549,00 Euro o con l'arresto da 15 giorni ad un anno, oppure, nei casi più gravi, l'applicazione congiunta di ammenda e arresto insieme alla pubblicazione della sentenza penale. Il giudice ha facoltà di aumentare fino al quintuplo l'ammenda se le condizioni economiche del datore di lavoro rendono l'importo esiguo e quindi l'ammenda inefficace.

- ***Favor rei***

  Con riferimento al *favor rei*, l'art. 24 del Decreto precisa che alle violazioni commesse prima del 19 settembre 2018, riferite a reati ormai depenalizzati, si applicano le sanzioni amministrative introdotte in sostituzione di quelle penali purché non sia già intervenuta una sentenza passata in giudicato. In quest'ultimo caso, potrà eventualmente intervenire una revoca da parte del giudice dell'esecuzione perché il fatto non è più previsto dalla legge come reato.

DEFINIZIONE AGEVOLATA DEI CONTENZIOSI

Il Decreto ha previsto la possibilità di definire i procedimenti sanzionatori pendenti al 25 maggio 2018, che non risultino ancora definiti con ordinanza-ingiunzione, con il pagamento in misura ridotta di un importo pari ai 2/5 del minimo edittale.

A tal fine, **il pagamento dovrà essere effettuato entro novanta giorni** dal 19 settembre 2018. Decorso tale termine e in assenza di memorie difensive, il Decreto prevede che gli atti con i quali è stata notificata la violazione o è stata effettuata la contestazione immediata assumono il valore di ordinanza-ingiunzione.

OBBLIGHI PER GLI OPERATORI DI SERVIZI DI COMUNICAZIONE ELETTRONICA ACCESSIBILE AL PUBBLICO

Il Decreto conferma l'obbligo a carico degli operatori attivi nel settore delle comunicazioni elettroniche (es., fornitori di servizi telefonici, fornitori di servizi *internet*) di adottare misure adeguate per la protezione, tra gli altri, dei dati personali relativi al traffico e all'ubicazione, e di garantire l'attuazione di una politica di sicurezza dei dati.

In linea con i principi di chiarezza nelle comunicazioni con gli interessati espressi nel GDPR, viene specificato che l'**informativa agli abbonati** e, ove possibile, agli utenti in merito ad eventuali **rischi di violazione della sicurezza della rete**, già obbligatoria nel "vecchio" Codice, deve essere resa con un **linguaggio chiaro, idoneo e adeguato rispetto alla categoria e alla fascia di età dell'interessato, con particolare attenzione in caso di minori di età**.

Agli operatori di servizi di comunicazione elettronica[2], soggetti a specifici obblighi di settore, non si applicano invece gli **obblighi di notifica degli incidenti di sicurezza** al *Computer Security Incident Response Team*

[2] A tale categoria di soggetti esentati si aggiungono i fornitori di reti pubbliche di comunicazioni, nonché i fornitori di servizi fiduciari (es., fornitori di servizi di firma elettronica) di cui al regolamento eIDAS (Regolamento (UE) 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE).

(CSIRT), imposti dalla c.d. **Direttiva NIS**[3] a carico degli operatori dei servizi essenziali. I servizi essenziali presi in considerazione dalla Direttiva NIS e dal d.lgs. n. 65/2018 di recepimento della stessa sono, tra gli altri, quello bancario, dei mercati finanziari, dell'energia, nei servizi e nelle infrastrutture digitali, dei trasporti, sanitario.

Con riguardo agli altri operatori, il Gruppo di lavoro articolo 29 per la protezione dei dati[4] ha messo in guardia rispetto alla **possibilità che un incidente di sicurezza determini anche una violazione dei dati personali**, con conseguente necessità di una separata notifica al Garante Privacy ai sensi dell'art. 32 GDPR (c.d. *data breach*), in aggiunta a quella ai sensi della Direttiva NIS.

Per una panoramica degli obblighi di notifica degli incidenti di sicurezza e delle violazioni dei dati, anche nell'ambito dei servizi di pagamento, invitiamo a consultare il nostro recente documento di aggiornamento a questo link.

[3] Direttiva (Ue) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. Tale Direttiva è stata attuata in Italia con d.lgs. n. 65/2018, come riportato nel nostro documento di aggiornamento disponibile a questo link.

[4] In merito agli obblighi di notifica delle violazioni dei dati personali (*data breaches*), invitiamo a consultare il nostro documento di aggiornamento a questo link.

CLIFFORD
CHANCE

AUTORI

Carlo Felice Giampaolino
Partner, Rome

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

Simonetta Candela
Partner, Milan

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

Jean-Paule Castagno
Counsel, Milan

T +39 02 8063 4317
E jean-paule.castagno@cliffordchance.com

Pasquale Grella
Senior Associate, Milan

T +39 02 8063 4289
E pasquale.grella@cliffordchance.com

Marina Mobiglia
Senior Associate, Milan

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

Alessandro Sciarra
Lawyer, Rome

T +39 064229 1384
E alessandro.sciarra@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

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.