Studio Niccoli Drago & Partners

Viale Risorgimento 14 – Via Tito Minniti 22

72100 Brindisi

Circolare per la Clientela - 12.12.2018, n. 22

Pubblicati gli aventi diritto allo Sport bonus –

Gli ultimi chiarimenti su cessione Ecobonus e Sismabonus –

Vietato applicare sovrapprezzi in base allo strumento di pagamento –

L'invio dell'attestazione del bonus asilo nido –

Il divieto per il datore di lavoro di comunicare la nuova sigla di un ex associato all'organismo sindacale –

Il GDPR negli studi medici -

Pubblicato l'elenco delle imprese che potranno beneficiare dello Sport Bonus 2018, l'Agenzia delle Entrate fornisce chiarimenti su cessione ecobonus e sisma bonus, l'Antitrust vieta di applicare sovrapprezzi in base allo strumento di pagamento utilizzato, più semplice l'invio dell'attestazione del bonus asilo nido, il Garante Privacy vieta al datore di lavoro di comunicare la nuova sigla di un ex associato all'organismo sindacale, le norme base per gli studi medici per adeguarsi al GDPR: questi i principali argomenti trattati dalla Circolare

Soggetti interessati

IMPRESE	PROFESSIONISTI	PERSONE FISICHE
- Terminato l'iter di assegnazione dello Sport Bonus 2018 - Cessione Ecobonus e Sisma bonus: gli ultimi chiarimenti dell'ADE - Vietato applicare sovrapprezzi negli acquisti in base allo strumento usato per il pagamento - Vietato per il datore di lavoro comunicare all'organismo sindacale la nuova sigla cui ha aderito un suo ex associato	- Cessione Ecobonus e Sisma bonus: gli ultimi chiarimenti dell'ADE - Vietato applicare sovrapprezzi negli acquisti in base allo strumento usato per il pagamento - Vietato per il datore di lavoro comunicare all'organismo sindacale la nuova sigla cui ha aderito un suo ex associato - GDPR e studi medici: gli adempimenti di base per adeguarsi alle norme sul trattamento di dati personali	- Cessione Ecobonus e Sisma bonus: gli ultimi chiarimenti dell'ADE - Inviare l'attestazione del bonus asilo nido diventa più semplice tramite la nuova funzionalità dell'APP mobile INPS

Tel. 0831 517660/0831 413290 Fax Elettronico 0831 1815084 Fax Digitale 0831 517660

E-mail - studioniccolidrago@gmail.com - dragobr@tin.it

Web - studioniccolidrago.com

SOMMARIO

1. TERMINATO L'ITER DI ASSEGNAZIONE DELLO SPORT BONUS 2018

Con la pubblicazione sul sito dell' Ufficio per lo Sport - Presidenza Consiglio dei Ministri dell'elenco delle imprese (n.55) aventi diritto, si è conclusa la procedura di assegnazione del credito d'imposta 2018 per le erogazioni liberali in denaro effettuate per interventi di restauro o ristrutturazione degli impianti sportivi pubblici, così come previsto dalla Legge di Bilancio 2018.

Lo Sport Bonus è utilizzabile in 3 quote annuali di pari importo rispettivamente nell'anno 2018, 2019 e 2020.

Tale credito può essere utilizzato mediante l'istituto della compensazione direttamente su modello F24 telematico. Tutti i pagamento ove verrà utilizzato il credito spettante dovranno avvenire mediante i canali Entratel/FiscoOnLine.

Si ricorda che il codice tributo da utilizzare nella sezione "Erario" è il 6892, indicando come anno di riferimento il 2018, anno in cui sono state effettuate le erogazioni.

2. CESSIONE ECOBONUS E SISMABONUS: GLI ULTIMI CHIARIMENTI DELL'ADE

Sulla base dei molti quesiti pervenuti in materia di cessione del credito corrispondente alla detrazione spettante per interventi di riqualificazione energetica degli edifici, nonché per quelli finalizzati alla riduzione del rischio sismico, l'Agenzia delle Entrate ha pubblicato la Risoluzione n. 84/E.

Questi alcuni dei quesiti pervenuti:

1. in caso di cessione, da quando il credito diventa utilizzabile per il cessionario?
2. per il suo utilizzo è necessario il preventivo invio della dichiarazione dei redditi del cedente?
3. l'atto di cessione redatto in forma scritta è soggetto ad imposta di registro?

In primis è opportuno ricordare che la legge 63/2013 ha stabilito che i soggetti che sostengono spese per interventi finalizzati alla riqualificazione energetica e/o alla riduzione del rischio sismico nelle zone classificate con i numeri 1,2 e 3, al posto della detrazione, possono optare per la cessione del credito maturato a:

- fornitori che hanno effettuato gli interventi;
- altri soggetti privati a cui è concessa la facoltà di una successiva cessione dello stesso.

Nel caso in cui il soggetto sia un condominio è previsto che possa cedere l'intera detrazione calcolata sulla base:

- della spesa approvata dalla delibera assembleare che ha deliberato l'esecuzione dei lavori;
- delle spese sostenute nel periodo d'imposta di riferimento.

Il condominio, qualora i dati della cessione non siano già indicati nella delibera assembleare, è tenuto a comunicare, entro il 31 dicembre dell'anno in cui è stata sostenuta la spesa, all'amministratore di condominio l'avvenuta cessione del credito, l'accettazione da parte del cessionario ed i dati identificativi di quest'ultimo. Sarà cura dell'amministratore di condominio comunicare i dati della cessione all'Agenzia delle Entrate usando gli appositi software messi a disposizione. L'amministratore dovrà presentare al condominio la certificazione delle spese unitamente al protocollo che attesta la presentazione della pratica all'Agenzia delle Entrate. La mancata comunicazione da parte dell'amministratore dell'avvenuta cessione del credito né comporta la sua inefficacia.

Il credito ceduto diviene utilizzabile per il cessionario a partire dal 10 marzo del periodo d'imposta successivo a quello in cui il condominio ha sostenuto la spesa. Sarà facoltà del cessionario utilizzare completamente il credito o, a sua volta, cederlo in tutto o in parte, dandone apposita comunicazione in formata telematico all'Agenzia delle Entrate.

L'Agenzia delle Entrate ricorda che "non assume rilevanza la forma che viene utilizzata per procedere alla cessione del credito; la normativa in esame non detta, infatti, regole particolari da seguire per il perfezionamento della cessione del credito né contiene prescrizioni in ordine alla forma con la quale la cessione deve essere effettuata. Come detto, è condizione di efficacia della cessione la comunicazione effettuata all'Agenzia delle Entrate da parte dell'amministratore del condominio o, qualora non obbligati alla relativa nomina, del condomino incaricato".

Non vi è obbligo di registrazione per l'atto di cessione del credito anche qualora lo stesso si a redatto in forma di atto pubblico o di scrittura privata autenticata. L'atto di cessione viene assimilato a tutti gli atti e documenti formati per l'applicazione, riduzione, liquidazione, riscossione, rateazione e rimborso di imposte per le quali non è vige l'obbligo di registrazione con il relativo pagamento dell'imposta di registro.

Si ricorda che...	Le modalità attuative ed i chiarimenti in merito all'ambito applicativo della cessione sono stati disciplinati nel: ○ Provvedimento direttoriale dell'8 giugno 2017; ○ Provvedimento direttoriale del 28 agosto 2017; ○ Circolare 11/E del 18 maggio 2018; ○ Circolare 17/E del 23 luglio 2018.

3. VIETATO APPLICARE SOVRAPPREZZI NEGLI ACQUISTI IN BASE ALLO STRUMENTO USATO PER IL PAGAMENTO

L'Autorità Garante della Concorrenza e del Mercato ha vietato alle imprese di applicare supplementi di prezzo negli acquisti effettuati mediante carte di credito / debito, presso esercizi commerciali anche di piccola dimensione, distribuiti su tutto il territorio nazionale.

L'Autorità è intervenuta imponendo tale divieto a seguito di diverse segnalazioni che le sono pervenute, attraverso cui la si informava che, nell'ambito degli acquisti di diverse tipologie di beni e servizi (quali biglietti e abbonamenti del trasporto pubblico, servizi di lavanderia, bevande e alimenti) mediante carta di credito / debito, taluni esercizi commerciali praticava l'operazione illecita. Le segnalazioni informavano che il sovrapprezzo viene altresì praticato da tabaccai che applicano un supplemento solitamente pari a 1€ quando i consumatori acquistano con carta di debito/credito di sigarette, marche da bollo, biglietti per trasporti pubblici.

Applicare supplementi di prezzo in virtù del mezzo di pagamento utilizzato dai consumatori vìola infatti l'art. 62 del Codice del Consumo, secondo cui coloro che vendono beni e servizi ai consumatori finali "non possono imporre ai consumatori, in relazione all'uso di determinati strumenti di pagamento, spese per l'uso di detti strumenti" oltre che la direttiva UE n. 2366 del 2015 relativa ai servizi di pagamento nel mercato interno (c.d. "PSD2"), recepita dal decreto legislativo 15 dicembre 2017, n. 218, che impone il divieto generalizzato per coloro che ricevono un pagamento da un consumatore di imporre al consumatore/pagatore spese aggiuntive, rispetto al costo del bene o del servizio, in relazione all'utilizzo di strumenti di pagamento impiegati dallo stesso.

Di conseguenza, nel rispetto di tali norme, l'Antitrust ricorda che venditori di beni e servizi al dettaglio non possono applicare supplementi sul prezzo dei beni o servizi venduti nei confronti di coloro che utilizzino, per effettuare i propri pagamenti, strumenti come ad esempio carte di credito o di debito, indipendentemente dall'emittente della carta.

L'Autorità è già intervenuta in numerosi settori per sanzionare l'applicazione di supplementi per l'uso di certi mezzi di pagamento, qualificando tale condotta come violazione dei diritti dei consumatori di cui all'art. 62 del Codice del Consumo, così ad esempio:

- nel trasporto aereo, sono state sanzionate compagnie aeree che applicavano un supplemento per il pagamento con carta di credito dei biglietti aerei acquistati online sui propri siti;?
- nella vendita al dettaglio di elettricità e gas naturale, alcuni primari operatori sono stati sanzionati per aver penalizzato il pagamento mediante mezzi diversi dalla domiciliazione bancaria o dall'addebito ricorrente su carta di credito (p.es., bollettino postale) o per aver imposto il pagamento di supplementi per il pagamento con carta di credito sui propri siti Internet;
- nella vendita online di servizi di viaggio, alcune agenzie di viaggio online sono state sanzionate per aver richiesto il pagamento di supplementi per l'acquisto online dei propri servizi mediante carte di credito; sono state inoltre sanzionate, per lo stesso motivo, una agenzia di viaggio specializzata nella vendita di biglietti per trasporti marittimi ed una specializzata nella vendita di biglietti aerei;
- stesso discorso nei servizi di rinnovo degli abbonamenti ai trasporti pubblici e di agenzia automobilistica.

Il divieto, riaffermato dall'Autorità, vale per tutti gli esercenti commerciali, compresi i dettaglianti specializzati, anche di piccola dimensione (tabaccai, ferramenta, lavanderie, macellerie, frutterie ecc.).

L'Antitrust raccomanda dunque a tutti gli esercenti commerciali, anche le piccole ditte, che consentono ai consumatori di utilizzare diversi mezzi di pagamento per l'acquisto dei beni e dei servizi commercializzati, di rispettare il Codice del Consumo e il D.Lgs. 218/2017, rimuovendo ogni sovrapprezzo applicato connesso all'utilizzo da parte dei consumatori di carte di credito o di debito o di altri mezzi di pagamento.

Contro coloro che non rispetteranno tali obblighi, l'AGCM eserciterà i poteri sanzionatori conferitigli dall'art. 27 del Codice del Consumo.

5

4. INVIARE L'ATTESTAZIONE DEL BONUS ASILO NIDO DIVENTA PIU' SEMPLICE TRAMITE LA NUOVA FUNZIONALITA' DELL'APP MOBILE INPS

Per ottenere l'agevolazione per la frequenza di asili nido pubblici e privati, ai sensi dell'articolo 3 del D.P.C.M. 17 febbraio 2017, è necessario trasmettere all'INPS la ricevuta di pagamento effettuata in favore degli asili.

In base all'art. articolo 3 del suddetto DPCM è concesso infatti un buono per il pagamento di rette relative alla frequenza di asili nido pubblici e privati del valore di 1000,00 euro parametrato per ogni anno di riferimento a undici mensilità, che viene versato in favore dei genitori in base alla istanza da questi presentata per supportarli nel pagamento della retta relativa alla frequenza di asili nido pubblici o privati autorizzati. L'agevolazione viene erogata mensilmente dall'Istituto nazionale della previdenza sociale mediante un pagamento diretto al genitore che ha presentato istanza, fino a concorrenza dell'importo massimo della quota parte mensile, a seguito di presentazione da parte dello stesso genitore della ricevuta che prova l'avvenuto pagamento della retta per la fruizione del servizio presso l'asilo nido pubblico, o privato autorizzato, selezionato.

Integrando nella sua app mobile una nuova funzionalità che consente ai genitori di trasmettere la ricevuta di pagamento indispensabile per ottenere l'agevolazione, l'INPS ha semplificato tale procedura. Sarà infatti possibile inoltrare la documentazione semplicemente allegando una fotografia dell'attestazione di pagamento dell'asilo tramite smartphone o tablet.

Come chiarito dall'INPS, nel suo messaggio del 28 novembre 2018 n. 4464, mamme e papà per effettuare l'invio dell'attestazione di pagamento e usufruire dell'agevolazione, dovranno accedere all'applicazione INPS Mobile, utilizzando il codice PIN rilasciato dall'INPS o tramite identità digitale SPID e quindi entrando nella nuova area "Bonus nido". Una volta effettuato l'accesso, l'applicazione presenterà al cittadino solo le domande in relazione alle quali è possibile allegare i giustificativi di spesa, ovvero le istanze che si trovino in stato "Protocollata", "Da Istruire" e "Accolta".

Il servizio consente dunque di allegare i documenti di spesa per ogni mensilità richiesta nella domanda.

L'applicazione permette anche di inserire i dati del soggetto che emette l'attestazione di pagamento, nel caso in cui esso sia diverso dalla struttura specificata nella domanda e di modificare, per ciascun allegato, i dati aziendali dell'asilo nido, qualora siano variati rispetto a quelli indicati nella domanda.

I file acquisiti mediante l'applicazione saranno resi disponibili agli operatori delle Strutture territoriali per le operazioni di competenza.

Si ricorda che l'app mobile INPS si può scaricare dagli store ufficiali dei dispositivi mobili Android e Apple.

5. VIETATO PER IL DATORE DI LAVORO COMUNICARE ALL'ORGANISMO SINDACALE LA NUOVA SIGLA CUI HA ADERITO UN SUO EX ASSOCIATO

Il datore di lavoro deve limitarsi a trasmettere al vecchio sindacato aziendale la decisione del lavoratore di non aderire più a quella sigla, senza comunicare la nuova sigla di adesione. Si tratta, infatti, di informazioni che rivelano l'opinione sindacale di una persona e che come tali vanno inquadrate tra i dati personali di natura sensibile (oggi categorie particolari di dati personali ex art. 9 GDPR- Regolamento n. 679/2016), vanno perciò protette e trattate con un'attenzione particolare.

Lo ha stabilito il Garante Privacy in un provvedimento emanato a seguito di alcuni reclami presentati davanti all'Autorità da parte dei lavoratori di un'azienda che si sono visti comunicare dal loro datore di lavoro al vecchio organismo sindacale cui erano associati, la loro scelta di non fare più parte della stessa sigla e assieme a tale comunicazione, il nuovo organismo sindacale cui avevano deciso di iscriversi.

La comunicazione da parte del datore di lavoro era avvenuta in seguito alla scissione della sigla del sindacato aziendale in due distinti soggetti, nell'ambito della quale, la vecchia sigla sindacale aveva dato avviso dell'intenzione di continuare ad effettuare il versamento in favore della medesima, in assenza di differente indicazione da parte dei lavoratori. In seguito a tale notifica, alcuni dipendenti avevano chiesto di versare la quota sindacale a favore del nuovo soggetto.

Il datore di lavoro, nella sua difesa davanti al Garante, precisava che la sua comunicazione fosse avvenuta in ragione del "fondato rischio che - mancata tale comunicazione - l'organismo avrebbe continuato ad operare in composizione non più aderente al verificatasi situazione di fatto, con inevitabili ricadute sulla validità della contrattazione aziendale e della correlata azione amministrativa" e che la comunicazione de qua era stata trasmessa esclusivamente alla RSU, organismo unitario, nella persona dei relativi componenti" e che questi ultimi erano autorizzati a trattare i dati personali in argomento dal regolamento delle rappresentanze sindacali unitarie.

Il Garante, nel suo provvedimento, ha ricordato innanzitutto che i dati sindacali appartengono a quella categoria di dati personali che oggi è definita dal Regolamento n. 679/2016 "categoria particolare di dati" (art. 9 GDPR), che nella vecchia formulazione del Codice Privacy erano definiti "dati sensibili", si tratta in altri termini di dati personali che non possono essere trattati, salvo che non sussistano delle condizioni specificamente individuate dalla norma, tra le altre: i) il consenso dell'interessato, ii) un trattamento necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, iii) un trattamento necessario per tutelare il diritto vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso. Si tratta quindi di dati che per essere trattati lecitamente necessitano che sussista almeno una delle specifiche deroghe oggi previste dall'art. 9 del Regolamento n. 679/2016 e che hanno bisogno di un'attenzione particolare rispetto ai dati personali comuni, quali nominativi, indirizzi, recapiti telefonici e simili.

Nel caso di specie, la società datrice di lavoro non si era limitata a comunicare alla Rappresentanza sindacale interessata la revoca dell'affiliazione da parte di alcuni lavoratori, ma aveva inviato a tutti i componenti della citata

sigla sindacale una e-mail che riportava in allegato documenti nei quali era espressamente indicata la contestuale iscrizione di alcuni lavoratori ad altro sindacato. Tale comportamento ha comportato dunque una illecita comunicazione a terzi di dati sensibili, in quanto la comunicazione deve intendersi quale trattamento di dati sensibili per una diversa finalità rispetto a quella principale per cui tali dati vengono raccolti e trattati dal datore di lavoro, un trattamento ulteriore dunque privo di un valido fondamento di legittimità.

L'art. 4 punto 2 del GDPR, che definisce il trattamento di dati personali (come anche la vecchia formulazione del Codice Privacy), menziona espressamente "la comunicazione" tra le operazioni di trattamento; si definisce trattamento di dati personali, infatti, qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la struttu-razione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Ragion per cui l'Autorità ha considerato legittimo il reclamo dei lavoratori, ritenendo che gli stessi abbiano tutto il diritto di agire per ottenere un risarcimento del danno nei confronti del proprio datore di lavoro, qualora ne ricorrano i presupposti, riservandosi di avviare un autonomo procedimento sanzionatorio a livello amministrativo per accertare la contestazione della violazione amministrativa derivante dall'illecita comunicazione di dati personali di natura sensibile.

6. GDPR E STUDI MEDICI: GLI ADEMPIMENTI DI BASE PER ADEGUARSI ALLE NORME SUL TRATTAMENTO DI DATI PERSONALI

Un medico nel suo studio effettua, senza ombra di dubbio, un trattamento di dati personali, anche se non ha dipendenti né collaboratori o non usa strumenti informatici. Non solo. Il professionista medico, tratta anche categorie particolari di dati personali. Se, infatti, nella prima tipologia di dati rientrano informazioni comuni che permettono di identificare direttamente o indirettamente una persona fisica, come anagrafiche, indirizzi email, numeri telefonici, indirizzi di residenza, matricola INPS e simili; nel secondo tipo di dati, rientrano informazioni più delicate, come dati sanitari, informazioni sulla razza, l'etnia, opinioni filosofiche, politiche, religiose, dati biometrici, dati genetici. Si comprende dunque come ogni medico si trova ad aver a che fare nella propria attività professionale con le suindicate tipologie di dati personali, considerando che, nel proprio quotidiano, può raccogliere, registrare, organizzare, conservare, consultare, elaborare, modificare, selezionare, estrarre, raffrontare, usare, interconnettere, bloccare, comunicare, diffondere, cancellare e distruggere dati personali appartenenti a suoi clienti, fornitori, collaboratori, altri colleghi, manualmente e mediante strumenti informatici e telematici; tali operazioni sono infatti tutte quelle incluse nel concetto di "trattamento di dati personali" come definito nel Regolamento UE n. 679/2016 in materia di trattamento di dati personali (anche detto GDPR).

6.1 La fase di assessment o analisi

La prima cosa da fare per uno studio medico è quella di analizzare la propria organizzazione, individuando quali dati vengono trattati, scindendo quelli comuni dalle categorie particolari di dati, individuando a chi appartengono i dati trattati (generalmente pazienti, fornitori, colleghi, dipendenti), il proprio modo di operare sui dati personali trattati, gli strumenti utilizzati per il trattamento (elettronici o manuali), il contesto, i "percorsi" dei dati (dove sono raccolti, come sono comunicati all'interno dello studio e all'esterno, dove sono archiviati, per quanto tempo, quando e come sono distrutti, chi vi ha accesso), i soggetti terzi cui vengono eventualmente comunicati e con cui vengono condivisi.

Fatte queste operazioni, il medico avrà già un quadro più chiaro della propria situazione rispetto ai dati trattati; si tratta, infatti, di attività che gli torneranno utili anche nella predisposizione del Registro dei trattamenti, in cui tali informazioni dovranno poi essere riportate in maniera ordinata, secondo quanto stabilito dal Regolamento all'art. 30.

6.2 Le informazioni da rendere ai pazienti e l'informativa alle altre categorie di interessati

Avendo individuato i soggetti di cui si trattano i dati (cosiddetti interessati), il medico dovrà rendere a tutti un'informativa adeguata il cui contenuto sarà diverso a seconda del soggetto, in quanto innanzitutto la finalità del trattamento sarà diversa da soggetto a soggetto, quindi l'informativa da rendere ai pazienti avrà certamente delle informazioni differenti rispetto a quella indirizzata a dipendenti, collaboratori/colleghi, fornitori, altre persone. A tal proposito, si ricorda che l'art. 78 e seguenti del Codice in materia di trattamento dati personali (D. Lgs. n. 196/2003) come novellato dal decreto n. 101/2018, per il medico di medicina generale o pediatra di libera scelta (ma anche per le strutture pubbliche e private che erogano prestazioni sanitarie e socio sanitarie) definiscono delle regole più specifiche nel trattamento dei dati personali dei pazienti, ad esempio, in relazione all'informativa da rendere ai pazienti, l'art. 78 del novellato decreto parla di informazioni e non di informativa, sebbene il contenuto

sia sempre quello stabilito dall'art. 13 del GDPR; il termine informativa invece ritorna quando si fa riferimento ai dati di fornitori, collaboratori/colleghi, dipendenti, altri soggetti.

6.3 Ma quali sono le "informazioni" che il medico dovrà rendere ai pazienti?

Secondo quanto stabilito all'art. 13 del GDPR, le informazioni, che vanno rese nel momento della raccolta del dato e dovranno essere formulate in un linguaggio semplice e chiaro preferibilmente in forma scritta (si veda l'art. 78 comma 3 decreto n. 196/2003 novellato), dovranno riguardare:

i) i dati di contatto del Titolare del trattamento, quindi del professionista titolare dello Studio;

ii) i dati di contatto del/i Responsabile/i del trattamento dei dati (se presenti);

iii) la/le finalità del trattamento dei dati;

iv) le modalità di trattamento dei dati;

v) il tempo di conservazione dei dati;

vi) i soggetti a cui i dati vengono comunicati;

vii) l'eventuale trasferimento all'estero dei dati;

viii) i diritti dell'interessato (diritto di richiedere informazioni sul trattamento, diritto di accesso, modifica, opposizione, cancellazione, limitazione, portabilità dei dati, diritto di proporre reclamo all'Autorità di controllo) e come egli potrà esercitarli nei confronti del titolare;

ix) i dati di contatto del Responsabile della protezione dei dati - DPO (se si rientra nei casi in cui è obbligatoria la nomina, ma per un piccolo studio professionale generalmente non è necessario).

Le suindicate informazioni devono essere riportate anche nell'informativa da rendere a colleghi, collaboratori, dipendenti, fornitori e altri soggetti, naturalmente definendo con precisione il contenuto.

Ora, soffermandosi alle informazioni da fornire ai pazienti, circa la/le finalità di trattamento dovranno essere menzionati gli scopi del trattamento dei dati, ovviamente la finalità di trattamento principale è quella di fornire il servizio di prestazione sanitaria richiesto dal paziente che per un medico si sostanzia nell'individuazione della malattia, quindi nella diagnosi, nell'assistenza e nella terapia sanitarie, nella riabilitazione o cura; oltre a tale finalità, ve ne sono da individuare altre strettamente connesse alla principale, come il trattamento dei dati per la comunicazione degli stessi - obbligatoria per legge - ad enti pubblici o autorità (si pensi alla comunicazione dei dati al sistema tessera sanitaria dell'Agenzia delle Entrate) o per la difesa dei propri diritti in un eventuale giudizio; altre finalità, collegate alla principale, possono essere anche richieste dal paziente, come la comunicazione dei dati ad enti privati per finalità assicurative o mutualistiche. Accanto a tali finalità di trattamento, ciascun medico può individuarne altre eventuali che dovranno essere comunque indicate nell'ambito delle informazioni da rendere al paziente. Così se ad esempio il medico tratta i dati per finalità di analisi statistica per fini di ricerca scientifica nel settore sanitario, dovrà renderlo noto nelle informazioni che rende ex art. 13 e chiedere il consenso al trattamento,

al pari se tratta i dati personali per inviare ad esempio una newsletter informativa ai pazienti su iniziative organizzate dallo studio, attività redazionale o altro.

Per quanto riguarda invece le modalità di trattamento, dovranno essere indicati i modi attraverso cui i dati sono trattati e conservati, quindi se il trattamento viene effettuato in modalità cartacea e/o elettronica, se vi sono soggetti (dipendenti/collaboratori) che trattano i dati personali specificando che sono stati istruiti e formati su comportamenti da assumere rispetto ai dati trattati, e che sono abilitati ad accedere solo ai dati necessari per lo svolgimento delle loro mansioni, oltre ad essere tenuti al rispetto degli obblighi di riservatezza. Le informazioni rese al paziente devono evidenziare inoltre in maniera analitica eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati:

a) per fini di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente;

b) nell'ambito della teleassistenza o telemedicina;

c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica;

d) ai fini dell'implementazione del fascicolo sanitario elettronico di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221;

e) ai fini dei sistemi di sorveglianza e dei registri di cui all'articolo 12 del decreto - legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221.

Nei confronti di un minore le informazioni sono rese ai genitori o a chi esercita la potestà genitoriale, tuttavia, dopo il raggiungimento della maggiore età esse vanno fornite all'interessato nel caso in cui non siano state fornite in precedenza.

6.4 Il Consenso è ancora necessario?

Alla domanda, il medico deve chiedere il consenso espresso al trattamento dei dati sanitari per finalità di diagnosi, cura, assistenza sanitaria quando rende le informazioni ex art. 13 del GDPR?

Si deve rispondere no. Ai sensi dell'art. 9 lett. h, infatti, non è necessario il consenso per il trattamento dei dati per "finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità". Dunque, una volta che il paziente ha scelto di sottoporsi ad una cura o richiesto assistenza sanitaria, non occorre il consenso al trattamento dei suoi dati per tali finalità. Resta il fatto che il regolamento ha lasciato liberi gli Stati di intervenire per disciplinare tale materia con maggiore dettaglio, così il nostro Stato, in linea con quanto stabilito dal Regolamento, ha abrogato la parte del Codice privacy riferita alla richiesta di consenso in materia di trattamento di dati sanitari per finalità di cura e assistenza (art. 81 Prestazione del consenso - abrogato), ma ha stabilito che con cadenza biennale l'autorità di controllo, il Garante Privacy, detti regole deontologiche e misure di garanzia in tale

ambito cui i medici dovranno attenersi. Se però il medico intende utilizzare i dati personali del paziente per finalità diverse e ulteriori rispetto a quelle connesse alle prestazioni assistenziali da questi richieste, come ad esempio per sperimentazione scientifica oppure per inviti ad iniziative dello studio o ancora per inviare newsletter) sono necessari specifici consensi espressi, in relazione ai quali deve essere sempre data la possibilità al paziente di ritirare i permessi manifestati. Resta salvo, ovviamente, il consenso informato necessario alla prestazione sanitaria, che nulla ha a che fare con il consenso al trattamento dei dati personali per finalità di assistenza sanitaria richiesta dal paziente.

Ma se ci si trova in una situazione di urgenza e il paziente è impossibilitato per incapacità fisica, incapacità di agire o di intendere o di volere, a ricevere le informazioni sul trattamento dei dati sanitari o quando non è possibile rendere le informazioni, come si procede?

In tali circostanze particolari, le informazioni di cui agli articoli 13 (o 14 nel caso in cui i dati non siano stati raccolti presso l'interessato, ma siano pervenuti al titolare da altra fonte, ad esempio raccolti dal FSE) del GDPR, ai sensi dell'art. 82 del Codice Privacy modificato, possono essere rese senza ritardo successivamente alla prestazione, a chi esercita legalmente la rappresentanza, o a un prossimo congiunto, a un familiare, a un convivente o unito civilmente ovvero a un fiduciario ai sensi della legge 219/2017 o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato. Ciò si verifica anche nei casi in cui sussista un rischio grave, imminente ed irreparabile perla salute o l'incolumità fisica dell'interessato. Le informazioni possono essere rese anche dopo la prestazione, senza ritardo anche in caso di prestazione medica che può essere pregiudicata dal loro preventivo rilascio, in termini di tempestività o efficacia.

6.5 Soggetti autorizzati al trattamento, segretari, infermieri, colleghi collaboratori dello studio medico

Oltre alle informazioni da fornire ai pazienti e all'informativa da rendere a colleghi, collaboratori, dipendenti, fornitori e a tutti gli altri soggetti di cui si trattano eventualmente dati personali, il GDPR richiede al titolare del trattamento di autorizzare i soggetti che nel contesto organizzativo trattano dati personali e in particolare richiede di formarli e istruirli in merito ai comportamenti da adottare nel trattamento dei dati personali. Ciò significa che se nello studio medico vi sono dipendenti, come può essere una segretaria o altri collaboratori ad esempio, colleghi junior, stagisti, infermieri è doveroso che il titolare li istruisca e li autorizzi al trattamento dei dati personali e alle categorie di dati personali. L'autorizzazione può essere effettuata mediante una lettera d'incarico scritta comunicata ad personam, ma non necessariamente, infatti il GDPR, ma anche il nuovo codice concedono al titolare la possibilità di individuare le modalità più adeguate per autorizzare tali soggetti al trattamento dei dati. La cosa importante è che la modalità scelta sia tale da permettere al titolare del trattamento di provare nel caso di ispezione, ma anche nel caso di complicazioni, violazioni, contenziosi in relazione ai dati trattati, che tali soggetti sono stati autorizzati, ma soprattutto formati, istruiti e impegnati alla riservatezza. Senza dimenticare che tali soggetti dovranno avere dei permessi limitati, circoscritti unicamente a quei dati necessari per permettere loro di svolgere le proprie mansioni; questo significa che ad esempio il/la segretario/a che si occupa solo della parte amministrativa e che gestisce l'agenda del medico, non dovrebbe venire a conoscenza (o avere l'accesso) dei dati sanitari dei pazienti, in quanto non è a ciò abilitata, innanzitutto non essendo un professionista medico e, poi perché tale accesso non risulta necessario ai fini dell'esercizio delle sue funzioni.

Ma quindi la segretaria del medico non può consegnare al paziente la documentazione contenente dati sanitari, né

la ricetta medica?

Il personale di segreteria può consegnare al paziente o a chi da lui delegato la documentazione sanitaria o le ricette mediche, ma tali documenti devono essere custoditi in una busta preventivamente sigillata dal medico al quale il paziente ha conferito l'incarico di eseguire una prestazione sanitaria, il personale di segreteria infatti non può entrare nel merito dei dati sanitari del paziente. Quindi, situazioni del tipo: segretaria che per velocizzare prende nota delle richieste dai pazienti, entra nella stanza del medico e riporta le ricette compilate o addirittura riporta brevemente risposte del medico al paziente, mentre la sala d'attesa è gremita di persone, sono da evitare nella maniera più assoluta. E se un paziente delega il figlio a ritirare i documenti contenenti dati sanitari? Un paziente può certamente delegare il figlio o altri a ricevere i documenti contenenti dati sanitari che lo riguardano con apposita delega sottoscritta dal delegante e copia del documento di identità dello stesso. In tal caso, i documenti possono essere consegnati in busta chiusa al delegato. Ma se un datore di lavoro chiede al medico del lavoro da lui incaricato i dati sanitari di un suo dipendente per conferirgli dei permessi speciali? Ciò è ammesso unicamente dietro il consenso espresso del paziente che deve essere scritto, e specifico; è consigliabile trattenere sempre anche copia del documento di identità del paziente, anch'essa firmata. Come comportarsi per gestire correttamente la sala d'attesa? Ad esempio è fondamentale, evitare di lasciare nella sala d'attesa documenti che riportino dati personali o peggio ancora dati sanitari, evitare di inserire armadietti non ben custoditi o lasciati aperti in cui sono conservati dati o informazioni personali o sanitarie; tali armadi dovrebbero essere sempre chusi con cura e posti in una zona diversa dalla sala d'attesa e comunque tenuta sotto controllo; è fondamentale bloccare con password eventuali computer presenti, quando ci si allontana dalla propria postazione. Si tiene a precisare che tali indicazioni, restano accorgimenti di base.

6.6 Soggetti autorizzati al trattamento, infermieri, colleghi collaboratori dello studio medico

Eventuali collaboratori medici o personale infermieristico di cui il titolare si avvale nello studio potranno essere autorizzati al trattamento anche dei dati sanitari dei pazienti, di questo va resa nota nelle informazioni rese in sede di raccolta dei dati. Il medico, titolare del trattamento dovrà poi individuare i soggetti esterni cui comunica i dati trattati, si pensi ad esempio al commercialista, a chi eventualmente gestisce il suo sito internet, che potrebbe accedere a dati personali per finalità di manutenzione del sito, alla società di consulenza che si occupa di effettuare interventi sui sistemi informatici dello studio, alla società che fornisce il gestionale per lo studio o, nel caso ad esempio, di un dentista, all'odontotecnico che fornisce al professionista un supporto una tantum, nel caso di ortopedico al fisioterapista con cui il medico stabilmente collabora. Sebbene, in tali ultimi casi, occorre comunque analizzare in dettaglio il rapporto per comprendere se ci si trova in una situazione di contitolarità del trattamento, titolarità autonoma o rapporto titolare/responsabile. In ogni caso, il rapporto tra professionisti in merito al trattamento dei dati deve essere debitamente contrattualizzato e l'informazione va riportata nell'informativa.

6.7 Misure di sicurezza e data breach

Per quanto concerne le misure di sicurezza in merito ai dati personali e sanitari trattati da uno studio medico, il riferimento è l'art. 32 del GDPR che, nel rispetto del principio dell'accountability (responsabilizzazione di chi tratta dati personali), non individua nel dettaglio le misure minime, come diversamente faceva l'abrogato Allegato B del vecchio Codice Privacy, ma offre delle linee guida sulle misure di sicurezza, stabilendo che esse devono essere adottate tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e

delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche; si tratta dunque di misure di sicurezza che ciascun titolare e responsabile del trattamento devono individuare in base al modo in cui svolgono il trattamento dei dati, misure di sicurezza che devono essere adatte alla specifica situazione di trattamento al fine di garantire un livello di sicurezza adeguato al rischio. Tali misure devono comprendere, tra le altre, dice l'articolo 32 del GDPR:a. la pseudonimizzazione e la cifratura dei dati personali; b. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza si deve tener conto dei rischi che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Quando si parla di data breach si intende una violazione sui dati personali riferita dunque a perdita, modifica, divulgazione illecita o non autorizzata, distruzione, accesso non autorizzato a dati personali. Il GDPR impone ai titolari del trattamento di predisporre una procedura che sia in grado di individuare tempestivamente una violazione sui dati trattati e permettere così di intervenire immediatamente per evitare che tale violazione possa provocare danni sui diritti e le libertà degli interessati, tale individuazione tempestiva della violazione deve permettere di soddisfare un altro obbligo posto a carico dei titolari del trattamento, quello di comunicare al Garante la violazione subita entro 72 ore decorrenti dal momento in cui il titolare ne ha preso conoscenza, tenendo presente che non tutte le violazioni vanno comunicate al Garante, ma solo quelle potrebbero incidere negativamente sulle persone fisiche, sui loro diritti e sulle loro libertà, provocando danni fisici, morali o immateriali (vanno notificate al Garante dunque solo le violazioni in relazione alle quali il titolare ritenga probabile che dalle stesse derivino rischi per i diritti e le libertà degli interessati); le violazioni che potrebbero provocare danni sui diritti degli interessati devono essere comunicate anche agli stessi. In ogni caso le violazioni di dati personali subite, anche se non notificate all´autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33, paragrafo 5) devono essere inserite in un registro delle violazioni. La procedura per individuare le violazioni sui dati deve essere predisposta prima che una violazione si verifichi, in modo che nel caso in cui l'evento potenzialmente individuato come rischioso dovesse verificarsi nel concreto, si conoscano già le procedure da eseguire. Occorrerà pertanto anche in tal caso effettuare un'analisi dell'organizzazione per individuare quali azioni meglio si confanno al contesto specifico e indicare a priori eventualmente un soggetto interno cui demandare l'incarico di procedere in tal senso. La procedura deve essere dimostrabile così come l'eventuale incarico attribuito al soggetto che dovrà effettuare le operazioni in caso di data breach, pertanto si consiglia di inserire un capitolo specifico dedicato a tale procedura in un regolamento più ampio da comunicare a tutti coloro che a vari livelli collaborano o lavorano nello studio.

6.8 Registro dei trattamenti

Nel registro dei trattamenti il titolare del trattamento (ma anche il responsabile) deve inserire una serie di informazioni indicate all'art. 30 del GDPR:

a. il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b. le finalità del trattamento;

c. una descrizione delle categorie di interessati e delle categorie di dati personali;

d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati (i soggetti terzi cui i dati vengono eventualmente comunicati, ad esempio ASL, Agenzia Entrate, INPS, commercialista, eventualmente cloud service provider), compresi i destinatari di paesi terzi od organizzazioni internazionali;

e. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati (10 anni);

g. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 o rimandare ad un manuale che le contenga in dettaglio;

h. l'indicazione degli assett utilizzati dallo studio;

i. la base giuridica del trattamento (assistenza sanitaria, quindi esecuzione contrattuale, obbligo di legge o legittimo interesse del titolare). Il registro dei trattamenti dovrà essere fornito al Garante o all'autorità ispettiva qualora ne facciano richiesta.

Non tutti sono tenuti a redigere il registro, sebbene il Garante ne raccomandi comunque l'adozione, in particolare a chi tratta dati sanitari, come appunto i medici, ritenendo che il registro costituisca in uno strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso. Per facilitare tale onere il Garante ha individuato delle modalità semplificate di tenuta e predisposizione del registro in favore di piccoli studi professionali e PMI, così ha stabilito ad esempio che i piccoli studi medici e le PMI possono circoscrivere la redazione del registro alle sole attività di trattamento riferite alle categorie particolari di dati e/o dati relativi a condanne penali o reati.

Queste sono le operazioni di base che uno studio medico è tenuto ad approntare per approcciarsi in maniera conforme al trattamento dei dati personali trattati, resta inteso che, quanto indicato non deve essere inteso come una consulenza, in quanto ogni contesto organizzativo deve essere analizzato nel dettaglio per consentire di procedere in maniera adeguata nel rispetto del principio di responsabilizzazione.

15

Un'ultima raccomandazione prima di chiudere: meglio evitare di fornire assistenza medica o informazioni sullo stato di salute di pazienti in chat o peggio ancora in messaggi privati sui social network, se non si tratta di sistemi appositamente ideati e sviluppati per gestire e quindi proteggere anche dati sanitari mediante ad esempio sistemi di crittografia che garantiscono livelli di sicurezza realmente elevati.