ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

# La PSD2, il GDPR e l'evoluzione del sistema dei pagamenti

# PERCHE' IL GDPR E' IMPORTANTE PER L'INDUSTRIA DEI PAGAMENTI

**MASSIMILIANO FORTE**

12 novembre 2019

# GDPR

Come è noto, il Regolamento UE 679/2016 sulla protezione dei dati personali ("**GDPR**") bilancia due esigenze potenzialmente in conflitto: favorire la libera circolazione dei dati e assicurare la protezione di tali dati.

La nuova disciplina **assicura che il trattamento dei dati sia effettuato in maniera trasparente**, garantendo all'interessato il diritto di essere sempre informato sull'esistenza di un trattamento avente ad oggetto propri dati personali, nonché sulle modalità di svolgimento di tale trattamento.

# GDPR e banche

Il **settore bancario** è uno dei settori su cui l'impatto del GDPR è maggiore: le banche, nello svolgimento della propria attività, acquisiscono per ogni cliente un numero elevato di dati personali.

Questi dati, permettono alla banca di effettuare una costante attività di profilazione dei propri clienti (cd. **KYC rule**).

# La profilazione

La profilazione, quando eseguita con un trattamento automatizzato rientra più precisamente tra quelle forme che il GDPR definisce "***qualsiasi forma di trattamento automatizzato*** *di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*" (**pensate alla profilatura MIFID o allo scoring credizio**).

# La profilazione

La profilazione del cliente assume caratteri inscindibili nel corso dello svolgimento dell'attività del cliente nella misura in cui le banche, ad esempio **nella prestazione di servizi di pagamento** acquisiscono e archiviano tutti i dati relativi alle operazioni di pagamento del cliente, ottenendo in tal modo una conoscenza potenzialmente dettagliata delle spese, delle operazioni di pagamento, degli acquisti effettuati.

# La profilazione

In questo modo la banca «alimenta» il profilo personale del cliente al fine di inserirlo all'interno di determinate categorie o classi commerciali di clientela.

Tale profilazione può essere utilizzata in primo luogo per indirizzare al cliente offerte mirate di servizi bancari e finanziari (cd. cross selling).

# La profilazione

**L'attività di profilazione pertanto non solo è intrinseca e imprescindibile** all'attività finanziaria, ma talvolta è **addirittura imposta *ex lege*** allo scopo di adempiere specifici obblighi a carico delle banche.

La scelta del legislatore europeo, in linea con la visione generale del GDPR, è quella di ammettere la profilazione, richiedendo tuttavia alcuni **accorgimenti** volti ad assicurare una adeguata tutela delle persone coinvolte.

# Obblighi GDPR per le banche

**Gli obblighi che le banche devono assolvere** per continuare a condurre lecitamente tale attività sono, infatti, i seguenti:

- fare espressa menzione nell'**informativa agli interessati** ai sensi degli artt. 13 e 14 GDPR dell'esistenza di un processo di profilazione, fornendo tutte le informazioni significative sulla logica utilizzata, nonché sull'importanza e le conseguenze previste di tale trattamento per l'interessato;

# Obblighi GDPR per le banche

- svolgere una valutazione d'impatto sulla protezione dei dati (***Data Protection Impact Assessment*** **– DPIA**), obbligatoria quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, considerati la natura, l'oggetto, il contesto e le finalità del trattamento stesso (tale valutazione è richiesta specificamente dall'art. 35 GDPR in presenza di un'attività di profilazione);

# Obblighi GDPR per le banche

- designare un responsabile della protezione dei dati (***Data Protection Officer – DPO***) previsto dall'art. 37 GDPR con il compito di assistere e consigliare il titolare del trattamento (in questo caso la banca) con riferimento a tutte le questioni relative alla protezione dei dati personali.

# La GDPR e la PSD2

Il 13 gennaio 2018 è stato pubblicato in Gazzetta Ufficiale il D.lgs. 15 dicembre 2017, n. 218 di recepimento della Direttiva UE 2015/2366 (cosiddetta **"PSD2"**) relativa ai servizi di pagamento nel mercato interno.

La PSD2 e il GDPR presentano **alcuni aspetti che evidenziano profili di complessità applicativa** frutto di una mancanza di coordinamento delle norme.

# I TPP

La PSD2 ha introdotto e disciplinato nuovi servizi che consentiranno agli utenti dei servizi bancari e di pagamento di rivolgersi a operatori di derivazione non bancaria, definiti "terze parti" (o ***Third Parties Provider*** **– TPP**), per chiedere l'esecuzione di operazioni di pagamento e altre attività connesse ai servizi di pagamento.

I TPP operano frapponendosi tra il cliente e i servizi di pagamento erogati dalle banche.

# I TPP

I TPP sono, a seconda della tipologia di servizio erogato:

- **PISP** (*Payment Initiation Service Provider*);
- **AISP** (*Account Information Service Provide*);
- **CISP** (*Card Issuer Credit Provider*).

# I TPP

Il flusso di dati derivante da tutte le operazioni di pagamento effettuate si "**sposta**", in tal modo, **dalle banche ai TPP**, i quali si frappongono tra cliente e banca e acquisiscono tutte le informazioni relative ad una transazione (ad esempio il bene/servizio acquistato, l'identità del "professionista" che vende il bene o il servizio on-line, ecc.).

# I TPP

L'ingresso dei TPP nel sistema dei pagamenti genera l'esigenza di inquadrare e, ove possibile, **regolare i rapporti tra questi e gli operatori del sistema bancario tradizionale**.

# I TPP

Un primo aspetto da considerare riguarda l'accesso ai dati dell'interessato (il cliente).

I nuovi servizi disciplinati dalla PSD2 necessitano, per poter funzionare, di una più **rapida interazione** tra i dati a disposizione delle banche e i TPP i quali, per poter eseguire i propri servizi, necessitano di **poter accedere tempestivamente** ai dati del cliente trattati dalla banca.

# PSD2

La tendenza in ambito PSD2 è, pertanto, quella di **rendere i dati dei clienti maggiormente accessibili ai soggetti terzi**.

# Banche e TPP

In base alla PSD2, le banche sono, infatti, tenute a fornire ai TPP alcuni dati dei propri clienti allo scopo di permettere ai TPP di erogare i propri servizi, a meno che tali dati non siano qualificabili come **dati sensibili relativi ai pagamenti**.

# Dato sensibile relativo ai pagamenti

Ma il legislatore comunitario non ha fornito una nozione oggettiva e univoca di **dato sensibile relativo ai pagamenti** e, all'atto pratico, tale concetto è affidato alla sensibilità delle banche.

# Obbligo di informativa

A loro volta gli artt. 13 e 14 del GDPR impongono al titolare del trattamento l'obbligo di fornire all'interessato una serie di informazioni specifiche in merito al trattamento dei dati personali che lo riguardano.

Qualora più soggetti siano coinvolti nel trattamento, come avviene nel caso di "concorso" tra banche e TPP, si pone il **problema di stabilire chi sia tenuto a fornire all'interessato l'informativa** nonché ad acquisire e conservare il relativo consenso, ove questo sia necessario.

# Banca, TPP e cliente

E’ pertanto opportuno, nell’interesse sia della banca sia del TPP, che i reciproci rapporti, con riferimento al trattamento dei dati personali dei clienti, siano **disciplinati in via negoziale.**

# TPP titolare o responsabile?

**L'inquadramento sul piano della protezione dei dati personali** del TPP è uno degli aspetti a maggiori criticità e controversie, a partire dalla questione se il TPP debba essere considerato ***titolare*** o ***responsabile*** del trattamento.

Ciascuna delle due ipotesi appare realizzabile, almeno in astratto. Non sembra possibile fornire, a priori, una risposta univoca e standardizzata per tutti i TPP e i nuovi servizi PSD2; appare invece opportuna **una valutazione caso per caso** che tenga conto in concreto delle funzioni, delle attività svolte e delle effettive relazioni tra le parti.

# TPP titolare o responsabile?

Se si imponesse di inquadrare la banca come titolare del trattamento e il TPP come **responsabile del trattamento**, sarebbe necessario stipulare un contratto che, in conformità all'art. 28 del GDPR, disciplini il trattamento effettuato dal TPP.

# TPP titolare o responsabile?

La banca, in quanto titolare del trattamento, dovrebbe fornire al TPP, in quanto responsabile del trattamento, una serie di istruzioni per la realizzazione del trattamento stesso (es. le misure di sicurezza da mettere in atto, eventuali tecniche di criptazione e/o pseudonimizzazione da adottare, elaborazione di procedure da seguire in caso di *data breach* ecc.).

# TPP titolare o responsabile?

La banca dovrebbe esercitare uno stretto controllo sull'operato del TPP in quanto, come titolare, sarebbe la banca stessa ad essere responsabile ultimo di tutte le violazioni del GDPR, anche quelle derivanti da comportamenti del responsabile del trattamento, salvo che dimostri di non essere in alcun modo responsabile.

# Il mancato coordinamento tra GDPR e PSD2.

Mentre l'art. 28 del GDPR richiede che i rapporti tra titolare e responsabile del trattamento siano disciplinati da un contratto o altro atto giuridico, gli articoli 66(5) e 67(4) della PSD2 stabiliscono che non può essere richiesto al TPP alcun contratto per accedere e usufruire dei dati personali del cliente della banca che ha scelto di avvalersi dei servizi del TPP.

# Il mancato coordinamento tra GDPR e PSD2.

Allo scopo di agevolare l'operatività dei TPP facilitando la diffusione dei loro servizi, il TPP ha diritto di accedere direttamente ai dati bancari (*i.e.* quelli necessari per l'erogazione del servizio del TPP) del cliente.

La banca non potrebbe, dunque, rifiutarsi di concedere al TPP l'accesso ai dati del cliente che, volendo usufruire dei nuovi servizi previsti dalla PSD2, avesse deciso di avvalersi di un TTP.

# Il mancato coordinamento tra GDPR e PSD2.

**Un eventuale rifiuto della banca a fornire i dati del cliente al TPP costituirebbe una violazione della PSD2** e, almeno astrattamente, un inadempimento nei confronti del cliente che ha deciso di avvalersi dei servizi TPP.

# Il mancato coordinamento tra GDPR e PSD2.

Viceversa, se la banca decidesse di conformarsi alla PSD2 e fornire i dati del cliente al TPP, in caso di *data breach* e violazione delle norme a tutela della riservatezza del cliente da parte del TPP, la banca potrebbe essere responsabile in base al GDPR

# Banca e TPP titolari autonomi?

La banca e il TPP potrebbero essere inquadrati come **due titolari autonomi** del trattamento.

# Banca e TPP titolari autonomi?

In tal caso si porrebbe comunque il problema di **regolare il trasferimento dei dati dalla banca al TPP**. Infatti, il cliente instaura un rapporto in primo luogo con la banca: nel momento in cui il cliente richiede al TPP l'erogazione del nuovo servizio PSD2, il TPP non raccoglie i dati direttamente dal cliente, ma li acquisisce attraverso l'accesso ai dati della banca.

# Il mancato coordinamento tra GDPR e PSD2.

E', in via generale, con riferimento ai centrali aspetti delle condizioni di "**liceità**" e "**correttezza**" del trattamento dei "**dati personali**", della necessità o no a tal fine quale relativa "**base giuridica**" del consenso dell'interessato, nonché delle possibili "**finalità**" del trattamento stesso, che le norme della PSD2 e quelle della GDPR non risultano, almeno *prima facie*, perfettamente coordinate, dovendo quindi essere ricondotte a coerenza in via interpretativa

# Il mancato coordinamento tra GDPR e PSD2.

Un'operazione questa che, tra l'altro, a livello di ordinamento italiano è resa ancora più complessa dal fatto che il quadro normativo applicabile in materia si compone, oltre che delle norme di attuazione della PSD 2 (cfr. il citato d.lgs. 15 dicembre 2017, n. 218), anche di quelle specificamente introdotte al fine di adeguare la normativa nazionale allo stesso GDPR (cfr. d.lgs. 10 agosto 2018 , n. 101)71.

# Il mancato coordinamento tra GDPR e PSD2.

Ad esempio, come noto, le regole generali in materia di protezione dei dati personali (fatte quindi salve le disposizioni speciali relative alle "**categorie particolari di dati personali**" di cui all'art. 9 del GDPR) prevedono che il relativo trattamento «***è lecito solo se e nella misura in cui ricorre almeno una***» delle condizioni di liceità elencate all'art. 6 del GDPR, tra le quali rileva in primis – ma non solo quindi – proprio quella in cui l'interessato abbia prestato il «**consenso**» al trattamento «**per una o più specifiche finalità**» (cfr. par. 1, lett. a).

# Il mancato coordinamento tra GDPR e PSD2.

Ad un "**consenso**" fa riferimento anche l'art. 94, par. 2, della PSD 2 laddove si prevede, per l'appunto, il «**consenso esplicito**» dell'utente all'accesso, al trattamento e alla conservazione da parte dei PSPs dei propri «**dati personali necessari alla prestazione dei rispettivi servizi di pagamento**».

# Il mancato coordinamento tra GDPR e PSD2.

Natura, funzione e finalità di tali due manifestazioni di "adesione" non sono tuttavia del tutto omogenei e sovrapponibili nella dinamica dei rispettivi plessi disciplinari, ciò considerato ad esempio anche che, come noto, mentre **il GDPR** reca un corpus di norme relativo alla protezione delle "persone fisiche" (identificate o identificabili – c.d. **"interessati"**) con riguardo al trattamento dei loro "dati personali", nonché alla libera circolazione dei dati stessi, in quest'ambito **il focus della PSD2** è piuttosto sulla protezione dei dati degli "**utenti**" in genere di servizi di pagamento.

# Il mancato coordinamento tra GDPR e PSD2.

In particolare, uno dei principali aspetti distintivi sembra essere il fatto che il «**consenso esplicito**» dell'utente di cui all'art. 94, par. 2, della PSD2 va qualificato essenzialmente come un consenso di tipo "**contrattuale**", ovvero quale (ulteriore e specifico) elemento necessario dei contratti relativi alla prestazione di servizi di pagamento richiesto dalla disciplina speciale di settore.

Ne consegue che, in pratica, tale «**consenso esplicito**» dell'utente di servizi di "**informazione sui conti**" all'accesso, al trattamento e alla conservazione da parte degli AISPs dei propri «**dati personali**» deve essere dato nell'ambito del contratto tra l'utente medesimo e il relativo AISP necessario per la prestazione stessa del servizio in parola (cfr. art. 67, par. 2, lett. a), della PSD2).

# Il mancato coordinamento tra GDPR e PSD2.

Nell'ottica e ai fini del GDPR il "**consenso**" è invece innanzitutto «*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*» (cfr. art. 4, punto 11), del GDPR).

# Il mancato coordinamento tra GDPR e PSD2.

Inoltre ai sensi del GDPR, in linea di principio, il trattamento di "**dati personali**" da parte degli AISP potrebbe trovare la sua base giuridica nel relativo art. 6, par. 1, lett. b), ai sensi del quale il trattamento stesso è lecito *ipso iure* se e nella misura in cui questo «*è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso*», senza bisogno di norma che siano soddisfatte ulteriori condizioni (salvo quindi che il trattamento non riguardi, ad esempio, le suddette "categorie particolari di dati personali" di cui all'art. 9 del GDPR).

# Il mancato coordinamento tra GDPR e PSD2.

Appare quindi così delinearsi **una disciplina differenziata**, segnatamente nel senso della previsione di una protezione extra o rafforzata, **per il trattamento di "dati personali"** nell'ambito della prestazione dei servizi di "informazione sui conti", in quanto ai sensi dell'art. 94, par. 2, della PSD2 un "**consenso esplicito**" e specifico dei relativi "utenti" sembra invece essere sempre necessario, sicché è lasciato all'interprete il compito di stabilire se anche in tale contesto casi trovi applicazione oppure no, e in che misura, l'autonoma e generale condizione di liceità del trattamento dei dati personali di cui all'art. 6, par. 1, lett. b), del GDPR.

# Il mancato coordinamento tra GDPR e PSD2.

Partendo dall'assunto che **in generale le norme** della PSD2 in materia di protezione dei dati personali e quelle del GDPR **sono da interpretare e applicare in modo il quanto più possibile coordinato e coerente**, una possibile lettura del risultante "combinato disposto" potrebbe essere pertanto quella secondo cui **la necessità del «consenso esplicito»** di cui all'art. 94, par. 2, della PSD2 sarebbe invero da intendere nel senso che:

# Il mancato coordinamento tra GDPR e PSD2.

- da un lato, gli AISP hanno l'obbligo di mantenere informato l'utente dei servizi di "informazione sui conti" circa le finalità della raccolta e successivo specifico trattamento dei suoi dati personali «**necessari alla prestazione dei rispettivi servizi**»

# Il mancato coordinamento tra GDPR e PSD2.

- dall'altro, che l'utente stesso debba acconsentire esplicitamente a tali finalità e trattamento e ciò soprattutto ai sensi e per gli specifici effetti delle norme speciali di settore di cui alla PSD2.

# Il mancato coordinamento tra GDPR e PSD2.

Una separata, benché strettamente attinente, questione tecnico giuridica è costituta dalle condizioni di liceità e compatibilità di un eventuale "ulteriore" trattamento e/o utilizzo dei dati personali raccolti e trattati nell'ambito e, soprattutto, per le specifiche finalità della prestazione di detti servizi di "informazione sui conti", ad esempio mediante trasmissione a terzi dei dati stessi per lo svolgimento di **attività e servizi "ulteriori" e/o "attigui"**, quali in ipotesi la valutazione del merito creditizio dell'utente, ovvero il diligente adempimento degli obblighi di "conoscenza del cliente" (c.d. know your customer rule) strumentali allo svolgimento delle prescritte valutazioni di adeguatezza o appropriatezza dei servizi d'investimento e accessori prestati dai soggetti abilitati" ai sensi della MiFID 2

# Il mancato coordinamento tra GDPR e PSD2.

La questione interpretativa deriva dalla formulazione testuale della disposizione di cui all'art. 67, par. 2, lett. f), della PSD2, ai sensi della quale **agli AISP è fatto divieto, come detto, di usare, accedere o conservare dati «per fini diversi da quelli della prestazione del servizio di informazione sui conti esplicitamente richiesto dall'utente dei servizi di pagamento, conformemente alle norme sulla protezione dei dati**».

# Il mancato coordinamento tra GDPR e PSD2.

Una disposizione questa che, nel non brillare per chiarezza lessicale nella parte in cui pone dei divieti di fare «conformemente alle norme sulla protezione dei dati», potrebbe essere infatti letta (anche) nel senso che **raccolta e il trattamento di dati dei conti di pagamento debbano essere strettamente funzionali alla sola prestazione del servizio di "informazione sui conti" in senso proprio**: ossia di sola fornitura al relativo "utente", e ad esso soltanto, di informazioni consolidate relative a uno o più conti di pagamento);

- **con speculare divieto quindi, in ipotesi, di poterne farne "ulteriori"trattamenti e utilizzi.**

# Il mancato coordinamento tra GDPR e PSD2.

Una conseguenza questa che, oltre a sembrare inutilmente **restrittiva** e sproporzionata rispetto alle esigenze di tutela in materia, da un lato appare **disfunzionale** rispetto alla stessa ratio della PSD2 di promuovere lo sviluppo nell'UE dei servizi di "informazione sui conti" e il loro utilizzo, dall'altro risulterebbe anche **eccentrica rispetto ai principi ordinatori** e alle regole stabiliti in via generale nell'UE dal GDPR in materia di liceità e compatibilità degli "ulteriori" trattamenti e utilizzi di "dati personali" già raccolti e trattati

# Grazie per l'attenzione

m.forte@temaconsulenza.eu