BACCIARDI PARTNERS legal tax finance | POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT | osservatori.net digital innovation | punto impresa digitale | CAMERA DI COMMERCIO DELLA ROMAGNA FORLÌ-CESENA E RIMINI

INNOVARE IL SETTORE AGROALIMENTARE
Export – digitalizzazione – sostenibilità

L'INNOVAZIONE DIGITALE NEL SETTORE AGROALIMENTARE

20 OTTOBRE 2022

RELATORI

AVV. ENZO BACCIARDI
DOTT. CLAUDIO RORATO
ING. FEDERICO IANNELLA
DOTT.SSA CHIARA CORBO, PhD
PROF. FABRIZIO CORONA

INQUADRAMENTO GENERALE

Il progressivo sviluppo delle tecnologie nel settore agroalimentare, ha determinato la crescita esponenziale di nuovi servizi e tecnologie. Se ciò ha comportato, da un lato, indiscutibili vantaggi in termini di semplificazione e rapidità nel reperimento e nello scambio di informazioni, dall'altro, ha provocato un enorme incremento del numero e delle tipologie di dati personali trasmessi e scambiati, nonché dei pericoli connessi al loro illecito utilizzo da parte di terzi non autorizzati.

DATO PERSONALE

qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

ESEMPI DI TECNOLOGIE

Nestlé – La collaborazione di Nestlé con OpenSc (società co-fondata da WWF e BCG Digital Ventures) è scaturita in una piattaforma blockchain in grado di tracciare il latte delle fattorie e dei produttori dalla Nuova Zelanda fino alle fabbriche e ai magazzini Nestlé in Medio Oriente;

Carrefour – Nel 2018 Carrefour è stato primo rivenditore europeo a introdurre blockchain per i prodotti alimentari, in particolare per i polli allevati all'aperto. Successivamente la tecnologia è stata estesa a uova, formaggio, latte, bistecca di manzo macinata, salmone, arance e pomodori.

ESEMPI DI TECNOLOGIE

Barilla – Il produttore di pasta e food italiano ha collaborato con IBM per affrontare la trasparenza e la tracciabilità nel suo ciclo di produzione del pesto: dalla coltivazione, al trattamento, alla raccolta, fino al trasporto, allo stoccaggio, al controllo di qualità e infine alla distribuzione, tutti i dettagli sono tracciati e resi disponibili su un sistema di blockchain che il cliente può verificare scansionando il codice QR del pesto.

DPIA

Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), l'art. 35 del GDPR obbliga i titolari a svolgere una valutazione di impatto (Data Protection Impact Assessment – DPIA) prima di darvi inizio, consultando l'autorità di controllo (art. 36 del GDPR) in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.

DPIA

QUANDO LA DPIA E' OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche.
Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:
- trattamenti valutativi o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

QUANDO LA DPIA NON E' OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON è necessaria** per i trattamenti che:
- non presentano rischio elevato per diritti e libertà delle persone fisiche
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

PROCEDURA DATA BREACH

L'art. 4 del GDPR definisce la violazione dei dati personali (data breach) come «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati».

Quindi, un data breach non è solo un evento doloso come un attacco informatico, ma può essere anche un evento accidentale come un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali (furto di un notebook di un dipendente).

PROCEDURA DATA BREACH

Il GDPR prescrive specifici adempimenti per il caso in cui una violazione di dati personali si realizzi (art. 33- 34).

Il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.) senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.

Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.

PROCEDURA DI BUSINESS CONTINUITY E DISASTER RECOVERY

Piano di Business Continuity: processi e procedure nell'ambito di un'organizzazione volte ad assicurare l'operatività delle funzioni base durante e a seguito di un evento disastroso.

Piano di Disaster Recovery: parte del processo di Business Continuity che specifica, a livello tecnico, le precauzioni da prendere e le attività da svolgere per mettere al sicuro i dati e le funzioni aziendali da attacchi o eventi disastrosi.

INNOVARE IL SETTORE AGROALIMENTARE:
Export – digitalizzazione – sostenibilità

L'INNOVAZIONE DIGITALE NEL SETTORE AGROALIMENTARE

GRAZIE PER L'ATTENZIONE

CONTATTI
segreteria@bacciardistudiolegale.it