Le centrali di committenza e il GDPR

L’esperienza nella definitiva applicazione del Reg. UE 2016/679 (GDPR) ci ha portato ad affrontare molti casi concreti, superandoli anche con l’aiuto delle linee guida dell’European Data Protection Board (EDPB)[1] e del Garante per la Protezione dei Dati Personali[2]. Tra i documenti più recenti dell’EDPB, ancora nella fase di consultazione, ci sono le *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*[3] che chiariscono la dinamica del rapporto tra titolare e responsabile del trattamento, con particolare attenzione alle previsioni dell’art. 28 del GDPR. Purtroppo, le linee guida n. 7 non hanno aiutato a chiarire alcuni aspetti che caratterizzano tale dinamica quando, in ambito di scelta del contraente nella pubblica amministrazione, interviene un soggetto terzo che funge da centrale di committenza secondo la definizione contenuta nell’art. 3, comma 1, lett. i) del D.Lgs. 50/2016 (Codice dei contratti pubblici)[4].

Cercheremo, dunque, di approfondire gli aspetti problematici di questa fattispecie e di esprimere alcuni elementi che possono aiutare a superarli.

Le “garanzie sufficienti”

L’art. 28 del GDPR prevede che:

“Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest’ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell’interessato”.

Questo vuol dire che, quando una pubblica amministrazione vuole scegliere un partner esterno al quale affidare una parte o l'intero processo di trattamento di dati personali, deve:

- attenersi alle previsioni del Codice dei contratti pubblici e, quindi, avviare una procedura pubblica di scelta del contraente per l'affidamento;
- definire, fin dall'avvio della procedura di scelta del contraente, quali garanzie richiedere al contraente per proteggere i dati personali; questo vale sia quando si tratta di una vera e propria "gara" (così come comunemente sono chiamate le procedure che prevedono la candidatura di più soggetti) sia quando si procede all'affidamento diretto.

Il combinato disposto di questi due obblighi deve indurre l'amministrazione aggiudicatrice a:

1. predisporre una **valutazione dei rischi** (se è necessario nelle forme e nei contenuti della valutazione d'impatto sulla protezione dei dati personali prevista dall'art. 35 del GDPR);
2. formalizzare preventivamente, in un apposito documento, **misure di garanzia** adeguate a minimizzare il rischio precedentemente valutato, che il contraente deve assicurare durante il trattamento effettuato per conto del titolare (cioè della stessa amministrazione aggiudicatrice); il documento può assumere la forma di requisiti specifici obbligatori o di criteri di valutazione dell'offerta tecnica nell'ambito di un capitolato oppure di un apposito allegato ad una richiesta di preventivo; in ogni caso, le misure di garanzia devono essere portate a conoscenza del "candidato contraente" (potenziale responsabile del trattamento) *prima* di giungere alla conclusione del contratto affinché tali misure siano parte integrante del contratto stesso e, quindi, figurino tra le obbligazioni del contraente;

3. definire, nell’ambito del contratto, apposite **penali** in caso di inadempimento rispetto alle misure di garanzia previste oltre che, nei casi più gravi, clausole risolutive.

Le linee guida dell’EDPB

Le linee guida n. 7/2020 dell’EDPB dedicano un apposito paragrafo alla scelta del responsabile del trattamento e alle **garanzie sufficienti.**
L’elemento chiave sul quale punta l’EDPB è la definizione *caso-per-caso* delle garanzie che l’amministrazione deve effettuare tenendo conto della natura, del perimetro, del contesto e degli scopi del trattamento (in pratica effettuando una preventiva valutazione dei rischi) pur suggerendo alcuni elementi che possono essere impiegati per caratterizzare i candidati contraenti, cioè:

- privacy policy;
- adeguati termini del servizio;
- registrazione delle operazioni di trattamento;
- sistema di gestione della sicurezza delle informazioni (p.e., ISO-IEC 27001);
- resoconti periodici di audit esterni;
- precedenti esperienze di trattamento in ambiti analoghi;
- risorse disponibili per il trattamento;
- adesione a codici di condotta;
- meccanismi di certificazione.

Tuttavia, questi costituiscono elementi generali che, sebbene ragionevoli, non tengono conto della specificità del singolo trattamento adottato dall’amministrazione aggiudicatrice.

Le centrali di committenza

A questa circostanza si aggiunge un ulteriore elemento problematico. In alcuni casi, non infrequenti, le procedure di scelta del contraente si sviluppano con l’aiuto di un

intermediario: la centrale di committenza. Il Codice dei contratti pubblici, infatti, all'art. 37, comma 1 prevede che:

"Le stazioni appaltanti, fermi restando gli obblighi di utilizzo di strumenti di acquisto e di negoziazione, anche telematici, previsti dalle vigenti disposizioni in materia di contenimento della spesa, possono procedere direttamente e autonomamente all'acquisizione di forniture e servizi di importo inferiore a 40.000 euro e di lavori di importo inferiore a 150.000 euro, ***nonché attraverso l'effettuazione di ordini a valere su strumenti di acquisto messi a disposizione dalle centrali di committenza e dai soggetti aggregatori".***

Con la seguente specificazione, al successivo comma 7:
"*Le centrali di committenza possono:*
a) aggiudicare appalti, stipulare ed eseguire i contratti per conto delle amministrazioni aggiudicatrici e degli enti aggiudicatori;
b) stipulare accordi quadro ai quali le stazioni appaltanti qualificate possono ricorrere per l'aggiudicazione dei propri appalti;
c) gestire sistemi dinamici di acquisizione e mercati".

Accade, quindi, che le centrali di committenza (o qualsiasi altro soggetto aggregatore) fungano da intermediari per una pluralità di singole amministrazioni. Questo accade molto spesso per piccoli comuni, carenti di professionalità adeguate a gestire le gare, o anche per aziende sanitarie pubbliche, obbligate dalla normativa regionale, e significa che la centrale di committenza arriva a definire in modo completo il quadro delle obbligazioni al quale è vincolato il contraente. Quando l'oggetto del contratto coinvolge, in tutto o in parte, il trattamento dei dati personali, il contraente assume il ruolo di responsabile del trattamento per la singola amministrazione che, quindi, si trova:

- ad assumere il ruolo di titolare senza essere il soggetto che ha effettuato la scelta e, quindi, senza

aver avuto la possibilità concreta di definire le “garanzie sufficienti” adeguate al proprio contesto;
- a non poter integrare gli obblighi contrattuali per il contraente-responsabile che, ovviamente, non sarebbe disposto a sopportare eventuali costi aggiuntivi non preventivati.

Qualche ipotesi risolutiva

Per superare questo aspetto problematico, con riferimento all’ipotesi in cui il contraente assumerà il ruolo di responsabile del trattamento per conto delle singole amministrazioni, possono essere utili le seguenti indicazioni pratiche.

Indagare preventivamente le esigenze delle singole amministrazioni: la centrale di committenza, nel raccogliere le esigenze funzionali delle singole amministrazioni aggiudicatrici, deve porre particolare attenzione alla valutazione dei rischi nel trattamento dei dati personali; la valutazione dei rischi e la conseguente griglia delle misure di garanzia da chiedere ai candidati dovrebbero essere sottoposte alle singole amministrazioni aggregate affinché possano preventivamente condividerle.

Lasciare un margine di *libertà* nell’ambito delle singole dinamiche contrattuali: la centrale di committenza, ferma restando la necessità di obbligare il contraente ad offrire garanzie minime legate allo specifico trattamento di dati personali connesso all’oggetto del contratto, potrebbe prevedere, nell’ambito degli accordi con lo stesso contraente, un margine decisionale alle singole amministrazioni affinché possano autonomamente completare il quadro di protezione che sono obbligate ad offrire agendo quali titolari del trattamento.

Note

[1] https://edpb.europa.eu/edpb_it

[2] https://www.garanteprivacy.it/

[3] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

[4] «Centrale di committenza»: un’amministrazione aggiudicatrice o un ente aggiudicatore che forniscono attività di centralizzazione delle committenze e, se del caso, attività di committenza ausiliarie.

Articolo a cura di **Francesco Maldera**

Francesco Maldera è Data Protection Officer e Data Scientist.

Il suo percorso professionale lo ha chiamato a responsabilità direzionali nell’ambito dei sistemi informativi, della safety&security, della privacy e dell’auditing svolgendo diversi incarichi dirigenziali nella Pubblica Amministrazione e in aziende private.

Attualmente, accompagna l’attività consulenziale a quella di sensibilizzazione delle persone tramite il sito www.prontoprivacy.it

https://www.ictsecuritymagazine.com/articoli/le-centrali-di-committenza-e-il-gdpr/