Gdpr ed enti ecclesiastici: prime indicazioni operative della Cei per le diocesi

A partire dal 25 maggio 2018 è entrato in applicazione il Regolamento 679/2016 UE in materia di trattamento dei dati personali. Ai sensi dell'art. 91 di tale Regolamento è stato predisposto un aggiornamento del Decreto generale della CEI del 1999 in materia, che è stato promulgato mediante la pubblicazione nel **sito web della Conferenza Episcopale Italiana**.

Finalità del decreto è in primo luogo quella di garantire in modo adeguato la protezione dei dati personali trattati, in risposta alle crescenti esigenze di tutela determinate dagli sviluppi della "società dell'informazione" e alla rinnovata sensibilità verso tali temi, rispetto ai quali anche la Chiesa non può non mostrare una rinnovata sollecitudine.

Inoltre l'adeguamento del testo – volto a renderlo "conforme" al Regolamento così come previsto dall'art. 91 del Regolamento – consente alla Chiesa di continuare ad applicare, per i soggetti e le finalità istituzionali, un proprio corpus completo di norme, nell'esercizio della propria autonomia e indipendenza e a tutela delle esigenze di libertà connesse all'esercizio della sua missione. Ecco una sintesi per punti delle indicazioni che maggiormente possono interessare diocesi e parrocchie:

– In primo luogo, occorre considerare che la nozione di "trattamento" dei dati personali accolta nel Regolamento e nell'aggiornamento del Decreto CEI è piuttosto ampia e che essa in sostanza riguarda qualsiasi operazione riferibile ai dati personali, compiuta con o senza l'ausilio di processi automatizzati e applicata a dati personali o insiemi di dati personali, come la raccolta, la registrazione, la conservazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, indipendentemente dal fatto che tali operazioni siano compiute in via automatizzata. Quindi, tutte o quasi le attività abitualmente compiute nell'ambito di parrocchie e/o diocesi (registri dei sacramenti, elenchi per il catechismo…) devono considerarsi trattamento dei dati personali (art. 1, § 2 e art. 2, Decreto; art. 2, par. 2 e art. 4 Regolamento).

- Perché il trattamento sia lecito deve essere presente almeno una delle condizioni elencate dall'art. 4, § 1, del Decreto. La condizione più frequente è il consenso informato del soggetto interessato, cioè del soggetto dei cui dati si tratta (art. 2; art. 4; art. 5 Decreto; art. 4; art. 6; art. 7 Regolamento). Tale consenso deve essere espresso e inequivocabile e deve essere preceduto da una adeguata informativa (v. allegato) (art. 6 Decreto; art. 13; art. 14 Regolamento). L'interessato può sempre revocare il consenso al trattamento (art. 5, § 3 Decreto; art. 17; art. 21 Regolamento).

Alcuni trattamenti, tuttavia, non trovano la loro base giuridica nel consenso, che pertanto non deve essere acquisito (cfr. in tal senso art. 4, § 1, lett. b), c), d), e), f), g) del Decreto). In questo quadro si può ritenere, in particolare, che non deve essere chiesto il consenso in caso di amministrazione di sacramenti o qualora il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria. Dovrebbe essere invece acquisito il consenso in caso di iscrizione a catechismo, di partecipazione a gite, a grest (per i minori serve il consenso di entrambi genitori).

– È necessario nominare un "titolare del trattamento", cioè il soggetto che determina le finalità e i mezzi del trattamento (art. 2 Decreto; art. 4 Regolamento). Tale soggetto dovrebbe essere di regola il soggetto apicale dell'ente (Vescovo, parroco,…), ma potrebbe anche essere un soggetto diverso, persona fisica o giuridica (Diocesi, parrocchia). Data la "mutevolezza" del soggetto al vertice dell'ente, potrebbe essere preferibile nominare titolare l'ente stesso (nella persona del suo legale rappresentante pro tempore, senza necessità di dichiararlo espressamente).

Il titolare del trattamento può nominare, con contratto o altro valido atto giuridico, un "responsabile del trattamento", ossia colui che tratta dati personali per conto del titolare del trattamento (art. 2; art. 15 Decreto; art. 4; art. 28 Regolamento). Tale nomina, tuttavia, non comporta l'esonero del titolare da eventuali responsabilità.

– Ai sensi dell'art. 8, § 5, del Decreto generale "Chiunque ha diritto di chiedere e ottenere, personalmente o mediante un procuratore legittimamente nominato, certificati, estratti, attestati, ovvero copie fotostatiche o autentiche dei documenti contenenti dati che lo riguardano (20), alle condizioni previste dal regolamento di cui al § 2.

Sono esclusi i dati che, non provenendo dal richiedente, sono coperti da segreto stabilito per legge o per regolamento ovvero non sono separabili da quelli che concernono terzi e la cui riservatezza esige tutela. L'interessato in ogni caso non ha diritto di ispezione dei dati del registro e dei dati sottratti alla sua conoscenza". Certificati, estratti, attestati dovrebbero essere quindi richiesti o dal diretto interessato (o dai suoi legali rappresentanti, se minore), o da un suo delegato.

Non sembra si possa dare seguito a richieste provenienti da altri soggetti privi di delega (ad esempio, i nonni che chiedano certificati riguardanti il minore, privi di una delega dei genitori).

– Sembra si possa ritenere ammissibile la comunicazione di dati Diocesi-Diocesi, Diocesi-parrocchia, parrocchia-Diocesi e parrocchia-parrocchia, in quanto declinazione della libertà di organizzazione del culto, nonché di comunicazione sancita dall'accordo del 194. Anche altri indici normativi inseriti nel Regolamento UE (cfr. Considerando 47 e 48; art. 6,

c. 1, lett. f) e c. 4, spec. lett. a), Considerando 51; art. 9, c. 2, lett. d) sembrano avallare tale interpretazione.

– Se il trattamento si svolge su "larga scala" (il Decreto non definisce la nozione di "larga scala", che deve essere quindi valutata nel caso concreto. Il Regolamento fornisce un orientamento al considerando 91. Comunque, il WP29, organo consultivo dell'UE per la materia della Privacy, raccomanda di tenere conto, in particolare, dei seguenti elementi, per stabilire se un trattamento sia effettuato su larga scala: a_ il numero di soggetti interessati dal trattamento in termini assoluti, ovvero espressi in percentuale della popolazione di riferimento; b_ il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; c_ la durata, ovvero la persistenza, dell'attività di trattamento; d_ la portata geografica dell'attività di trattamento) o appare di particolare delicatezza (questo criterio, secondo il WP29, include categorie particolari di dati personali, definite all'articolo 9 del Regolamento, ad esempio informazioni sulle opinioni politiche delle persone) deve essere nominato un "responsabile della protezione dei dati" (art. 18 Decreto; art. 37; art. 38; art. 39 Regolamento). Il responsabile della protezione dei dati può essere alle dipendenze del titolare del trattamento o del responsabile del trattamento o essere un professionista esterno.

Tra i compiti del responsabile per la protezione dei dati (specificamente indicati nel decreto) vi è quello di informare e fornire consulenza al titolare del trattamento e al responsabile del trattamento e ai dipendenti che effettuano il trattamento dei dati personali in merito ai loro obblighi in materia di protezione dei dati, sorvegliare l'osservanza del decreto e delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali.

– Deve essere tenuto un "registro delle attività di trattamento", anche in formato elettronico, che contiene le seguenti informazioni: a) il nome e i dati di contatto del titolare del trattamento e, ove presenti, 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, compresi i destinatari di paesi terzi diversi od organizzazioni internazionali; e) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative (art. 19 Decreto; art. 30 Regolamento).

– Una particolare attenzione deve essere prestata per assicurare l'inviolabilità degli archivi, specie qualora si tratti di archivi informatici. L'archivio deve essere dotato di un sistema di chiusura che garantisca una sufficiente sicurezza da tentativi di furto e di scasso. Le chiavi dell'archivio devono essere custodite personalmente e accuratamente dal titolare del trattamento. Spetta al titolare del trattamento autorizzare agli estranei l'accesso ai dati. Il titolare del trattamento deve denunciare quanto prima all'autorità

ecclesiastica competente e, se del caso, anche all'autorità civile, ogni incursione nell'archivio che abbia causato sparizione, sottrazione o danneggiamento di registri, atti, documenti pubblici, elenchi e schedari contenenti dati personali. Il titolare del trattamento deve documentare qualsiasi violazione dei dati personali, comprese le circostanze in cui si è verificata, le sue conseguenze e i provvedimenti adottati per porvi rimedio (art. 2; art. 13; art. 14 Decreto; art. 4; art. 32; art. 33; art. 34 Regolamento).

– Sono previste sanzioni, di non poco rilievo (art. 23 Decreto; art. 82; art. 83, art. 84 Regolamento).

Tenuto conto dell'evoluzione in corso, gli uffici e Servizi competenti della Segreteria Generale della Conferenza Episcopale Italiana forniranno ulteriori indicazioni e documentazione.