Achille D, 'I «Registri delle attività di trattamento» tra responsabilizzazione e presupposto di liceità del trattamento dei dati personali' (2024) 2 EJPLT, 102 – 114.
DOI: https://doi.org/10.57230/EJPLT242DA

EJPLT
ISSN 2704-8012



I «Registri delle attività di trattamento» tra responsabilizzazione e presupposto di liceità del trattamento dei dati personali

«Records of processing activities» between accountability and the prerequisite of lawfulness of personal data processing

DAVIDE ACHILLE
Professore Associato di Diritto Privato
Università del Piemonte Orientale

Abstract

Il GDPR ha previsto l'obbligo di tenuta dei registri delle attività di trattamento quale strumento di concretizzazione del principio di responsabilizzazione (c.d. accountability) cui è improntata la normativa europea sulla protezione dei dati. Attraverso l'analisi della normativa di riferimento e mediante l'individuazione della disciplina applicabile ai registri delle attività di trattamento, si rileva come questi svolgano altresì la funzione di consentire la valutazione e la documentazione della conformità del trattamento al GDPR esplicitando quel necessario bilanciamento tra diritto all'informazione e diritto alla riservatezza che sottende alla normativa sulla tutela dei dati personali.

The GDPR has provided for the obligation to keep records of processing activities as a tool for implementing the principle of responsibility (so-called accountability) to which the European data protection legislation is guided. Through the analysis of the relevant legislation and through the identification of the discipline applicable to the records of processing activities, it is noted how they also perform the function of enabling the evaluation and documentation of the compliance of processing with the GDPR by making explicit that necessary balance between the right to information and the right to confidentiality that underlies the legislation on the protection of personal data.

* Il presente contributo è destinato allo special issue in memoria del Prof. Cesare Massimo Bianca e del Commentario al D. Lgs. 30 giugno 2003, n. 196 «Codice della privacy» da lui curato con il Prof. Francesco Donato Busnelli nel 2007 (Cedam).

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: dati personali; trattamento; registro delle attività; accountability

Summary: 1. I registri dell'attività di trattamento e la responsabilizzazione. – 2. Il registro del titolare del trattamento. – 3. Il registro del responsabile del trattamento. – 4. Le regole di tenuta e di gestione dei registri. – 5. L'obbligo di mettere a disposizione del Garante il registro. – 6. Le esenzioni. – 7. I registri come strumenti di valutazione e documentazione della conformità del trattamento al GDPR.

1. I registri dell'attività di trattamento e la responsabilizzazione.

Nell'insieme delle varie novità apportate dalla normativa europea in tema di protezioni dei dati personali (Regolamento (UE) 2016/679 [1]) si inserisce senz'altro la previsione dell'obbligo di tenuta del registro dell'attività di trattamento[2] che, secondo l'art. 30 *GDPR*, costituisce un incombente a carico del titolare del trattamento, del responsabile del trattamento e, ove presente, del loro rappresentante[3], siano questi soggetti pubblici o privati. In particolare, viene prevista la tenuta di due differenti registri dell'attività di trattamento, quello del titolare del trattamento[4] e quello del responsabile del trattamento[5], comminando per la relativa omissione specifiche sanzioni[6].

[1] Per una visione d'insieme sul GDPR, oltre alle opere citate nel prosieguo, v. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, 2016; S. Sica-V. D'Antonio-G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, 2016; G. Busia-L. Liguori-O. Pollicino (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali*, Roma, 2016; L. Califano-C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/ 679*, Napoli, 2017; V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice privacy)*, Milano, 2019; E. Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019; N. Zorzi Galgano (a cura di), *Persona e mercato dei dati: riflessioni sul GDPR*, Padova, 2019.

[2] Sul tema, per una prima informazione, v. L. Bolognini, *Obbligo di documentazione*, in L. Bolognini-E. Pelino-C. Bistolfi, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 413 ss.

[3] Con riferimento al concetto di rappresentante rilevante ai fini del discorso che ci occupa, v. S. Melchionna, *Art. 30*, in *GDPR e normativa privacy* a cura di G.M. Riccio-G. Scorza-E. Belisario, Vicenza, 2018, p. 284, la quale ritiene «utile riferirsi alla copiosa giurisprudenza del GPDP sul tema e ad alcune disposizioni già presenti nel CPDP che richiamano espressamente le attività sulle quali il titolare esercita un potere decisionale su finalità e mezzi con conseguente responsabilità».

[4] Il titolare del trattamento è definito dall'art. 4, n. 7, *GDPR*, come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri».

[5] Il responsabile del trattamento è definito dall'art. 4, n. 8, *GDPR*, come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

[6] La mancata tenuta dei registri viene sanzionata, ai sensi dell'art. 83, par. 4, lett. a), *GDPR*, con una pena pecuniaria fino a 10.000.000 di euro o, per le imprese, fino al 2% del fatturato dell'esercizio precedente, se superiore. Rileva inoltre S. Melchionna, *op. cit.*, p. 291, che l'inadempimento all'obbligo di tenuta dei registri «può essere considerato dal GPDP come elemento valutativo nell'ambito dell'esercizio dei propri poteri di intervento e controllo».

Al di là delle non trascurabili implicazioni che tale adempimento comporta a livello di *compliance* aziendale rispetto alla normativa di riferimento[7], la tenuta del registro in questione costituisce una delle misure in cui si estrinseca con maggiore evidenza il principio di responsabilizzazione (c.d. *accountability*) di cui all'art. 5, par. 2, *GDPR*[8]. Infatti, come si evince dal Considerando n. 82, «per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità».

A tal ultimo riguardo, sulla base del rilievo per cui la responsabilizzazione deve consistere anche in una serie di attività che consentano di comprovare il rispetto delle norme contenute nel *GDPR* e l'adozione di misure efficaci, è stato opportunamente rilevato che la tenuta del registro delle attività di trattamento, piuttosto che costituire un mero adempimento formale, è «parte integrante di un approccio sostanziale alla tutela dei dati e delle persone nell'ambito di un sistema di corretta gestione dei dati personali»[9].

In questo contesto, per quanto la tenuta dei registi delle attività di trattamento si ponga in continuità con l'obbligo di notificazione di cui agli artt. 37 s., d.lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali)[10], oggi abrogato dall'art. 27 del d.lgs. 10 agosto 2018, n. 101, si distingue profondamente dal previgente incombente in quanto non integra il dovere di comunicare all'autorità competente lo svolgimento di determinati trattamenti, costituendo invece uno «strumento di ricognizione delle attività svolte[11], che si colloca in un sistema trasparente di corretta gestione dei dati

[7] È infatti innegabile che l'adempimento dell'obbligo di tenuta dei registri dell'attività di trattamento ha costituito e costituisce un incombente particolarmente gravoso, specialmente per quelle grandi realtà in cui l'ordinaria attività imprenditoriale implica per sua natura il trattamento di una innumerevole quantità di dati personali (si pensi, ad es., alle aziende di telecomunicazione e agli istituti di credito). L'affermazione non deve tuttavia essere enfatizzata, dovendosi riconosce che la predisposizione dei registri in parola risulta in concreto facilitata dagli obblighi previsti dalla normativa previgente, la quale già prevedeva la tenuta del documento programmatico sulla sicurezza (D.P.S.) di cui all'Allegato B (Disciplinare tecnico in materia di misure minime di sicurezza) del d.lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali), oggi abrogato dall'art. 27, co. 1, lett. d), del d. lgs. 10 agosto 2018, n. 101, il cui contenuto era individuato dal punto 19 del citato Disciplinare tecnico in materia di misure minime di sicurezza. Può quindi ritenersi che, pur a fronte della differente logica sottesa ai due adempimenti (CONTI, *La tenuta dei registri: consapevolezza,* accountability, substance over form *e documentazione delle scelte*, in *Foro padano*, 2019, c. 42), la nuova previsione che impone la tenuta del registro delle attività di trattamento non sia totalmente inedita (L. GIACOMINI-C.A. TROVATO-C. ROSSI CHAUVENET, *Il registro delle attività di trattamento previsto dal GDPR: più di uno strumento di mera* compliance, in *MediaLaws*, 2018, p. 461).

[8] Sul ruolo del principio di responsabilizzazione nel quadro del *GDPR,* v. G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Leggi civ. comm.*, 2017, 1 ss.; ID., *Il principio di* accountability, in *Giur. it.*, 2019, p. 2778 ss.

[9] Cfr. MELCHIONNA, *op. cit.*, p. 283.

[10] Al riguardo, v. R. ROSETTI, *Artt. 37-38*, in *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 («Codice della* privacy*»)* a cura di C.M. BIANCA e F.D. BUSNELLI, I, Padova, 2007, p. 732 ss.

[11] Sul punto v. anche la Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali emanata dal Garante per la protezione dei dati personali (doc. web. n. 6807118), disponibile all'indirizzo *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6807118*, dove si rileva che nella nuova prospettiva del *GDPR* l'intervento delle autorità di controllo sarà principalmente *ex post*, ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiegando l'abolizione per effetto del d.lgs. 10 agosto 2018, n. 101 di alcuni istituti previsti dalla Direttiva 95/46/CE e dal d.lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali), come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto *prior-checking* (o verifica preliminare), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare e del responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia con eventuale

personali»[12]. È quindi corretto individuare l'obbligo di tenuta dei registri alla stregua di un adempimento prodromico ad ogni attività di trattamento dei dati personali in quanto funzionale a valutarne i rischi[13], costituendo quindi un prerequisito del trattamento stesso[14].

Ciò consente, inoltre, di ritenere che la tenuta dei registri in questione sia un obbligo per il titolare e per il responsabile, non potendo lo stesso essere demandato ad altro e diverso soggetto e, in particolare, al *data protection officer* (*DPO*)[15], posto che quest'ultimo è piuttosto tenuto a sorvegliare l'osservanza della normativa di riferimento da parte del titolare e del responsabile del trattamento (art. 39, par. 1 lett. b), *GDPR*), compito questo che riguarda quindi anche l'obbligo di tenuta dei registri in questione, con la conseguenza che onerando tale soggetto della tenuta dei registri in esame si realizzerebbe una inammissibile commistione tra controllore e controllato in evidente contrasto con i principi sottesi alla normativa europea in tema di protezione dei dati personali.

2. Il registro del titolare del trattamento.

Nel prevedere l'obbligo di tenuta del registro dell'attività di trattamento da parte del titolare[16], il par. 1 dell'art. 30 *GDPR* individua il contenuto, minimo ed essenziale, dello stesso. In particolare, si prevede che questo debba contenere: a) le indicazioni per l'individuazione del titolare, o contitolare, del rappresentante del titolare e del responsabile della protezione dei dati, comprensive dei relativi dati di contatto; b) l'indicazione delle finalità del trattamento; c) le categorie di interessati e di dati personali che vengono trattati; d) l'indicazione delle categorie di destinatari a cui i dati personali trattati possono essere comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; e) i trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali, compresa l'identificazione del paese terzo o dell'organizzazione e, per i trasferimenti *ex* art. 49, par. 2, *GDPR*, la documentazione delle garanzie adeguate; f) i termini ultimi previsti per la cancellazione delle diverse categorie di dati; g) la descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 31, par. 1, *GDPR* che

successiva consultazione dell'Autorità, tranne che per alcune specifiche situazioni di trattamento (v. art. 36, par. 5, *GDPR*).

[12] M. SOFFIENTINI, *Registro dei trattamenti e dei data breaches*, in *Dir. e prat. lav.*, 2019, p. 1733.

[13] S. MELCHIONNA, *op. cit.*, p. 283 s., la quale rileva altresì il ruolo, riteniamo anche promozionale, di «un nuovo approccio culturale e organizzativo al trattamento».

[14] V. W. KOTSCHY, *Article 30. Records of processing activities*, in *The EU General Data Protection Regulation (GDPR). A Commentary* edited by C. Kuner-L.A. Bygrave-C. Docksey, Oxford, 2020, p. 618, dove si afferma che «Knowing which data are processed about what kind of data subjects and for what purpose is a prerequisite for being able to be held accountable».

[15] In questo senso, invece, A. AVITABILE, *Il* data protection officer, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* opera diretta da G. Finocchiaro, Bologna, 2017, p. 364, secondo il quale ciò sarebbe possibile in quanto il legislatore ha previsto una «elencazione non esaustiva dei compiti attribuibili al DPO», potendosi al riguardo rilevare che ciò non esclude che le competenze di tale soggetto siano determinate coerentemente con il ruolo allo stesso attribuito dal legislatore.

[16] Si è peraltro ritenuto che «laddove l'attività sia effettuata da più titolari in contitolarità, non solo la stessa sia censita nei registri di tutti i titolari, ma anche che ogni contitolare indichi con riferimento a quali trattamenti sussiste la contitolarità e con quali soggetti» (così S. MELCHIONNA, *op. cit.*, p. 285).

sono adottate con riferimento alle attività di trattamento.

Il contenuto eterogeneo cui fa riferimento la norma può essere suddiviso in due distinte categorie di informazioni che il registro deve avere, consentendo di distinguere tra profili prettamente afferenti al titolare del trattamento (contenuto formale) e aspetti riferibili ai dati che sono trattati (contenuto sostanziale).

Quanto al contenuto formale, oltre al riferimento al titolare, contitolare e responsabile, comprensivo delle relative informazioni per consentire una più agevole contatto con tali soggetti[17], devono essere indicate le categorie di destinatari a cui i dati possono essere comunicati [18] e, secondo quanto suggerito dal Garante per la protezione dei dati personali, anche gli eventuali altri soggetti ai quali – in qualità di responsabili e sub-responsabili del trattamento – siano trasmessi i dati da parte del titolare, al fine di consentire al titolare medesimo di avere effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate le operazioni di trattamento dei dati personali[19]. Quanto alle informazioni circa i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale andrà riportata l'informazione relativa ai suddetti trasferimenti unitamente all'indicazione relativa al Paese terzo cui i dati sono trasferiti e alle adeguate garanzie adottate ai sensi degli artt. 44 ss. *GDPR*[20]. Infine, per quanto attiene la descrizione generale delle misure di sicurezza andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell'art. 32 *GDPR*[21], che si è ritenuto possano «essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale»[22].

Il contenuto sostanziale riguarda invece una serie di indicazioni direttamente riconducibili ai dati trattati. In primo luogo, occorre indicare il contenuto delle finalità del trattamento, con ciò intendendosi la base giuridica del trattamento[23], con la precisazione che in caso di trattamenti di categorie

[17] Cogliendo il parallelismo con il contenuto essenziale dell'informativa ai sensi dell'art. 13, par. 1, lett. a), *GDPR*, si è ritenuto che debbano essere indicati l'indirizzo, anche di posta elettronica certificata, il numero di telefono e di *fax* (S. MELCHIONNA, *op. cit.*, p. 280).

[18] Il destinatario, secondo quanto previsto dall'art. 4, n. 9, *GDPR* è «la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento».

[19] In questo senso le FAQ sul registro delle attività di trattamento del Garante per la protezione dei dati personali (consultabili all'indirizzo *www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento*).

[20] Con riguardo all'indicazione delle «garanzie adeguate», ci si è chiesti se debbano essere allegati i documenti a supporto della legittimità del trattamento o sia sufficiente la mera indicazione delle garanzie adottate, ritenendo condivisibilmente che «la norma si riferisca esclusivamente alle informazione atte a provare tale adeguatezza e non specificatamente alla documentazione richiesta a tal fine» (L. GIACOMINI-C.A. TROVATO-C. ROSSI CHAUVENET, *op. cit.*, p. 456).

[21] S. MELCHIONNA, *op. cit.*, p. 288, secondo la quale, tramite la descrizione delle misure di sicurezza e l'analisi che vi sottende, «il registro si pone […] anche come strumento di pianificazione e controllo della politica di sicurezza».

[22] V. le FAQ sul registro delle attività di trattamento del Garante per la protezione dei dati personali cui si è già fatto riferimento.

[23] Rileva S. MELCHIONNA, *op. cit.*, p. 286, che con riguardo ai soggetti pubblici «l'indicazione della finalità di trattamento implica una ricognizione delle disposizioni normative di settore, che attribuiscono al soggetto

particolari di dati occorre individuare la specifica condizione di cui all'art. 9, par. 2, *GDPR* e in caso di trattamenti di dati relativi a condanne penali e reati si deve indicare la specifica normativa che ne autorizza il trattamento ai sensi dell'art. 10 *GDPR*[24]. In merito alla descrizione delle categorie di interessati e di dati personali trattati, andranno specificate sia le tipologie di interessati, evidenziando se il trattamento riguarda particolari categorie di soggetti[25], sia le tipologie di dati personali oggetto di trattamento. Circa i termini ultimi previsti per la cancellazione delle diverse categorie di dati dovranno essere individuati i tempi di cancellazione per tipologia e finalità di trattamento e, dove non sia possibile stabilire a priori un termine massimo[26], i tempi di conservazione dovranno essere specificati mediante il riferimento a criteri indicativi degli stessi, tenendo in ogni caso presente che tale profilo deve essere necessariamente coordinato con il principio di limitazione della conservazione di cui all'art. 5, par. 1, lett. e), *GDPR*, il quale impone che i dati siano conservati per un tempo non superiore a quello necessario per il conseguimento delle finalità per le quali sono trattati.

A fronte delle indicazioni circa il contenuto del registro del titolare che fornisce l'art. 30 *GDPR*, che – come detto – costituisce il contenuto minimo e essenziale del registro, è stato correttamente rilevata l'opportunità di un contenuto ulteriore del documento in parola, da implementare con ogni ulteriore informazione che si rendesse necessaria in base ad una valutazione complessiva di impatto della normativa applicabile rispetto ai trattamenti di dati in concreto effettuati[27]. La precisazione si giustifica, ed in ciò deve trovare conferma, sul rilievo che la tenuta del registro è funzionale al corretto e puntuale rispetto della regolamentazione in tema di protezione dei dati personali, in ottemperanza al principio di responsabilizzazione, il quale nella variabilità e nelle eterogeneità del caso concreto impone di adoperarsi per la miglior tutela dell'interessato e del sistema di protezione dei dati.

---

pubblico la specifica finalità per il raggiungimento della quale diviene indispensabile trattare i dati personali».

[24] Il chiarimento si trova nelle FAQ sul registro delle attività di trattamento del Garante per la protezione dei dati personali cui si è già richiamato.

[25] V. S. MELCHIONNA, *op. loc. cit.*, la quale, in particolare, si riferisce a «minori, lavoratori, sottoposti a misure di privazione della libertà, rifugiati, beneficiari di provvidenze, disabili, pazienti, ovvero individui distinguibili per credo, convinzioni politiche o etnie».

[26] Si tengano presenti al riguardo le determinazioni specifiche di conservazione massima delle informazioni personali, come ad esempio previsto per la videosorveglianza comunale dall'art. 6, co. 8, d. l. n. 11 del 23 febbraio 2009, convertito in legge con modificazioni, dall'art. 1, co. 1, l. n. 39 del 23 aprile 2009, ai sensi del quale «La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione».

[27] V. S. MELCHIONNA, *op. cit.*, p. 288, che con riferimento al contenuto ulteriore indica la data di inizio del trattamento, la necessità di acquisire il consenso dell'interessato con riferimento ad una specifica attività di trattamento, l'indicazione di un accordo con il contitolare in ordine alle responsabilità sugli obblighi e sull'esercizio dei diritti, le informazioni circa il luogo dove risiedono i dati, le categorie di persone autorizzare al trattamento, l'adesione/adozione di codici di condotta, l'applicazione di meccanismi di certificazione, la sussistenza di una valutazione di impatto *privacy*, l'eventuale consultazione preventiva del Garante per la protezione dei dati personali, il verificarsi di un *data breach*.

3. Il registro del responsabile del trattamento.

Il contenuto del registro delle attività del responsabile del trattamento è individuato dal par. 2 dell'art. 30 *GDPR*, il quale riproduce in gran parte, con una tecnica normativa quantomeno discutibile, l'elencazione del contenuto del registro delle attività di trattamento del titolare previsto dal precedente par. 1 della medesima disposizione[28]. In particolare – oltre alle indicazioni necessarie per l'individuazione dei soggetti coinvolti nel trattamento (responsabile, titolare, rappresentante del titolare o responsabile del trattamento e responsabile della protezione dei dati), i trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali, compresa l'identificazione del paese terzo o dell'organizzazione e, per i trasferimenti *ex* art. 49, par. 2, *GDPR*, la documentazione delle garanzie adeguate e la descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 31, par. 1, *GDPR* che sono adottate con riferimento alle attività di trattamento – il contenuto peculiare che caratterizza il registro in parola è unicamente quello delle «categorie di trattamenti effettuati per conto di ogni titolare del trattamento». A differenza del registro tenuto dal titolare del trattamento, quello del responsabile non contiene invece l'indicazione del termine di cancellazione dei dati personali e l'indicazione delle finalità del trattamento, il che si spiega in ragione del diverso ruolo attribuito al responsabile rispetto al titolare del trattamento.

Ciò posto, anche per il registro del responsabile del trattamento come per quello del titolare, si deve ammettere la possibilità di implementare il contenuto del registro delle attività di trattamento prevedendo ulteriori indicazioni rispetto a quelle cui si riferisce la disposizione normativa[29].

---

[28] È peraltro opportuno rilevare che la previsione di uno specifico obbligo di tenuta da parte del responsabile del Registro delle attività di trattamento, in aggiunta a quello del titolare del trattamento, ha costituito uno degli argomenti utilizzati per affermare che la disciplina contenuta nel *GDPR* non consentirebbe la nomina di un responsabile del trattamento "interno", potendo rivestire tale posizione solamente soggetti "esterni" al titolare, mentre eventuali soggetti collocati nella struttura organizzativa o aziendale del titolare sarebbero da qualificare quali designati e autorizzati ai sensi degli artt. 29 GDPR e 2-*quaterdecies* cod. prot. dati pers. (L. GRECO, *L'organigramma privacy: i soggetti del trattamento*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101* a cura di Finocchiaro, Bologna, 2019, p. 343 ss.). per quanto l'opinione in parola non sia stata condivisa da una parte della dottrina, prospettando la possibilità di differenziare la disciplina applicabile al responsabile "esterno" rispetto a quella riferibile al responsabile "interno", che sarebbe assoggettato a quella del responsabile "esterno" «nei soli limiti di quanto risulti eventualmente possibile e con gli adeguamenti che si rendono necessari in via interpretativa» (F. BRAVO, *Sulla figura del responsabile "interno" del trattamento di dati personali*, in *Dir. inf. e informatica*, 2019, p. 973, il quale – nello specifico e per quanto in questa sede rileva – afferma che «l'art. 30, par. 2, GDPR […] potrà essere applicato al responsabile interno affidando a questi la gestione della porzione di registro prevista per il titolare del trattamento ai sensi del par. 1 del medesimo articolo»), non pare che si possa convenire con tale ultima impostazione, non fosse altro che diversamente si legittimerebbe un porzionamento delle competenze relativamente ai contenuti del registro che sono considerati unitariamente dal legislatore. D'altronde, neppure sembra possibile affermare che il responsabile, qualora "interno", debba tenere il relativo registro, posto che ciò si tradurrebbe in una inutile duplicazione (v. L. GIACOMINI-C.A. TROVATO-C. ROSSI CHAUVENET, *op. cit.*, p. 457), che esporrebbe in definitiva il medesimo soggetto al rischio di essere sanzionato in quanto titolare e in quanto responsabile, ragione questa che nella realtà ha indotto le grandi realtà aziendali a non nominare responsabili "interni", preferendo qualificarli come designati al trattamento dei dati personali (su tale ultima figura, anche in relazione a quella di persona autorizzata, v. D. FARACE, *Le persone autorizzate al trattamento dei dati personali*, in *Riv. trim. dir. e proc. civ.*, 2021, p. 423 ss.).

[29] In questo senso S. MELCHIONNA, *op. cit.* p. 289, che individua il contenuto eventuale del registro del responsabile negli elementi considerati come requisiti minimi del registro del titolare non previsti dalla norma per quello del responsabile e nel contenuto ulteriore del registro del titolare (v., *retro*, nota n. 26), considerando di particolare utilità l'indicazione dell'applicazione di un codice di condotta o di un

Infine, può senz'altro convenirsi sul rilievo per cui il responsabile del trattamento sarà altresì tenuto, in ragione della contemporanea pluralità dei ruoli ricoperti, a tenere, salvo che ne resulti esentato, anche il registro delle attività di trattamento per i dati di cui è titolare, non potendosi invece condividere l'ulteriore assunto secondo cui il responsabile dovrebbe tenere tanti registri quanti sono i soggetti per i quali viene effettuato il trattamento[30]. In senso contrario a quest'ultima interpretazione depone lo stesso dato normativo, il quale parla di «un registro» e indica che questo deve contenere i riferimenti legislativi ad «ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento», con ciò suggerendo di escludere una moltiplicazione del registro anche in ossequio ad un principio di semplificazione che sembra dover ispirare un adempimento così peculiare e complesso. D'altronde, deve considerarsi che la tenuta del registro in questione è strettamente connesso all'attività svolta dal soggetto responsabile e non anche dal titolare del dato, sicché non pare avere fondamento la tesi che richiede un numero di registri pari a quello dei titolari dei dati di cui si è responsabili.

Peraltro, quanto ai rapporti tra titolare e responsabile, si è ritenuto che non sia possibile escludere un obbligo di vigilanza del primo sulla tenuta del registro da parte del secondo[31]. L'affermazione, pur da condividere, nella sua genericità potrebbe essere fuorviante, non potendosi intendere che il suddetto obbligo di vigilanza da parte del titolare sia limitato alla verifica dell'esistenza di tale registro, estendendosi piuttosto anche all'accertamento della sua regolarità formale e finanche alla corretta tenuta dei dati riguardanti l'attività di trattamento[32].

4. Le regole di tenuta e di gestione dei registri.

I registri delle attività di trattamento, secondo l'unica prescrizione circa la tenuta e la gestione dei registri in parola fornita dall'art. 30 *GDPR*, devono essere «tenuti in forma scritta, anche in formato elettronico», il che implica la possibilità di compilare il registro sia in formato cartaceo che in formato elettronico. In tale ultimo ipotesi, che, come intuibile, costituisce la stragrande maggioranza dei casi, il registro – secondo quanto indicato del Garante per la protezione dei dati personali [33] – deve in ogni caso recare, in maniera verificabile, la data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella dell'ultimo aggiornamento.

---

meccanismo di certificazione da parte del responsabile «in quanto tale elemento può essere utilizzato dal titolare come parametro per verificare il rispetto degli obblighi da parte del responsabile».

[30] S. MELCHIONNA, *op. cit.*, p. 285.

[31] S. MELCHIONNA, *op. loc. cit.*

[32] Si tenga al riguardo presente che nella contrattualistica che coinvolge il titolare del trattamento e il responsabile del trattamento è frequente la previsione di specifiche clausole contrattuali che attribuiscono al primo delle facoltà ispettive sulla corretta tenuta del registro da parte del responsabile del trattamento. In argomento vd. A. CHIAPPINI, *Riflessioni sul contratto tra titolare e responsabile del trattamento*, in *Contratto e impresa*, 2021, p. 317 ss.

[33] Si tratta delle già richiamate FAQ sul registro delle attività di trattamento del Garante per la protezione dei dati personali.

Oltre alla prescrizione sulla forma, che – come detto – è l'unica espressamente prevista dal dato normativo, può tuttavia ritenersi che s'impongano ulteriori regole risultanti dal sistema.

In primo luogo, le informazioni contenute nei registri devono necessariamente essere aggiornate[34], dovendo quindi essere caratterizzate dal requisito dell'attualità. In tal senso, in base alle richiamate indicazioni del Garante per la protezione dei dati personali[35], si è evidenziato che il registro dei trattamenti, in quanto documento di censimento e analisi dei trattamenti effettuati dal titolare o responsabile, deve essere mantenuto costantemente aggiornato dovendo il suo contenuto corrispondere all'effettività dei trattamenti posti in essere, da ciò derivando che qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel registro, dando conto delle modifiche sopravvenute.

Infine, deve ritenersi che ulteriori specifiche regole di tenuta e gestione dei registri sull'attività di trattamento siano costituite dalla completezza, che si collega al contenuto dei registi sia come individuati dalla normative che come necessario in base alla particolarità del caso, dalla veridicità, dovendo corrispondere quanto indicato nei registri alle reali ed effettive modalità di trattamento, e dalla intellegibilità dei dati riportati, dovendo questi avere un sufficiente grado di chiarezza di ordine interpretativo o percettivo.

5. L'obbligo di mettere a disposizione del Garante il registro.

Come accennato in precedenza, una delle funzioni principale del registro sull'attività di trattamento è quella di dare concretezza alla cooperazione dei soggetti che effettuano il trattamento con l'autorità Garante della protezione dei dati personali. Proprio in questa prospettiva, l'art. 30, par. 4, *GDPR* prevede che il titolare o il responsabile debbano mettere a disposizione delle autorità di controllo il registro delle attività di trattamento. Occorre al riguardo tenere presente che siffatto obbligo, a differenza di quanto avveniva nella previgente disciplina con riguardo alle notificazioni[36], deve essere fornito alle autorità unicamente a fronte di una specifica richiesta in tal senso. In tale contesto, peraltro, si deve rilevare che le autorità di controllo avranno in ogni caso la possibilità di richiedere, nell'ambito dei propri poteri ispettivi e di controllo, ogni ulteriore documento necessario per lo svolgimento delle proprie funzioni, non potendosi certamente ipotizzare che le richieste siano limitate al registro delle attività di trattamento.

Ciò che certamente si può rilevare è che la tenuta dei registri in parola, oltre a correlarsi al principio di responsabilizzazione, rivestono altresì un ruolo non secondario nelle attività ispettive, di monitoraggio e di vigilanza svolte dall'autorità.

---

[34] Sul punto si è ritenuto che «l'aggiornamento […] debba avvenire in tempo reale […], tanto da divenire una sorta di obbligo dinamico» (così S. MELCHIONNA, *op. cit.*, p. 289).

[35] V. le FAQ sul registro delle attività di trattamento cui si è in precedenza fatto riferimento.

[36] Il rilievo si trova in S. MELCHIONNA, *op. cit.*, p. 291.

6. Le esenzioni.

A fronte del generico obbligo di tenuta dei registri del trattamento, l'art. 30, par. 5, *GDPR* prevede una serie di esenzioni che escludono l'obbligatorietà di tale adempimento per terminati soggetti, vale a dire le imprese o le organizzazioni con meno di 250 dipendenti, salvo il caso che il trattamento effettuato possa presentare un rischio per i diritti e le libertà dell'interessato, non sia occasionale o includa il trattamento di categorie particolari di dati personali (art. 9, par. 1, *GDPR*) o di dati personali relativi a condanne penali e a reati (art. 10 GDPR). In altri termini, a fronte dell'esenzione per i soggetti con caratteristiche dimensionali inferiori a 250 dipendenti[37], la norma individua tre ipotesi che consentono di escludere l'operatività dell'esenzione facendo quindi riemergere l'obbligatorietà della tenuta del registro delle attività di trattamento per imprese o organizzazioni[38], vale a dire: a) il rischio per i diritti e le libertà dell'interessato; b) la non occasionalità del trattamento [39]; c) l'utilizzo di particolari categorie di dati personali.

Con specifico riferimento al rischio per i diritti e le libertà dell'interessato come anche alle particolari categorie di dati personali, a fronte dell'indeterminatezza dei concetti, un utile parametro di riferimento per le valutazioni del caso è costituito dal Considerando n. 75, il quale si riferisce a «i rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;

[37] Si tenga presente che il Considerando n. 13 afferma che «Per tener conto della specifica situazione delle micro, piccole e medie imprese, il presente regolamento prevede una deroga per le organizzazioni che hanno meno di 250 dipendenti per quanto riguarda la conservazione delle registrazioni».

[38] Il riferimento alle imprese e alle organizzazioni induce ad escludere dall'ambito di applicazione dell'esenzione i soggetti pubblici (in questo senso v. S. MELCHIONNA, *op. cit.*, p. 285, che giunge a tale conclusione anche in ragione dell'ambito oggettivo dell'esenzione che non consentirebbe di includervi i soggetti pubblici).

[39] Segnala S. MELCHIONNA, *op. cit.*, p. 286, che «l'Autorità di controllo belga (*Commission de la protection de la vie privée* – CPVP), al fine di fornire utili elementi interpretativi, ha richiamato la definizione inglese del termine occasionale, arrivando a suggerire di considerare occasionali quei trattamenti che si verificano a intervalli irregolare o sporadici, ovvero di tanto in tanto o per caso [Raccomandazione n. 6 del 14 giugno 2017 della CPVP, punto 18]».

se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati». Si tratta, com'è facile intuire, di una elencazione non tassativa, ben potendosi far riferimento ad ulteriori ipotesi che consentono di neutralizzare l'esonero dall'obbligo di tenuta del registro delle attività di trattamento, dovendosi più in generale ritenere che la deroga non possa operare tutte le volte in cui sussiste un potenziale pregiudizio ai diritti e alle libertà personali dei soggetti cui i dati personali si riferiscono.

Certamente di più difficile determinabilità è il riferimento alla non occasionalità del trattamento, con riguardo al quale nella valutazione di non saltuarietà e, quindi, di ricorrenza del trattamento, si dovrà pur sempre tenere in considerazione che si tratterà di un'analisi prognostica da compiere sulla ragionevole previsione della ricorrenza del trattamento, senza che possano assumere rilevanza le contingenze del caso concreto che non siano preventivamente correlabili al trattamento realmente effettuato.

La maggiore difficoltà interpretativa che si è riscontrata nell'individuazione dell'ambito di applicazione dell'esenzione in parola ha riguardato la portata delle tre richiamate condizioni di esclusione dell'esenzione, con riferimento alle quali si sono prospettate due opzioni ermeneutiche, da un lato ritenere che le condizioni in parola siano tra loro alternative e, pertanto, anche solo una di esse renda inoperante l'esenzione dall'obbligo di tenuta dei registri, dall'altro lato ritenere che le tre condizioni operino in maniera composita, ipotizzando che oltre al rischio per diritti e libertà dell'interessato l'esclusione della esenzione richiede che sussistano o la non occasionalità del trattamento o l'utilizzo di particolari categorie di dati[40].

Sul punto, la formulazione letterale della norma e le preposizioni che la compongono inducono a ritenere che il requisito primario di esenzione, costituito dalla struttura dimensionale dell'impresa o dell'organizzazione, che non deve avere più di 250 dipendenti, sia irrilevante e quindi il soggetto sarà comunque obbligato alla tenuta del registro dell'attività di trattamento, nel caso in cui sussista anche una delle tre condizioni di esclusione dell'esenzione (rischiosità del trattamento, trattamento non occasionale o trattamento di dati particolari), come conferma l'uso della congiunzione "o" tra il secondo ed il terzo caso previsi dalla norma[41]. Tale interpretazione, pur rendendo di fatto applicabile l'esenzione ad un ristretto e limitato numero di ipotesi, con la conseguenza che la tenuta dei registri dell'attività di trattamento risulta obbligatoria nella quasi totalità dei casi, è l'unica che risulta conforme al dato letterale e sistematico, non potendosi ammettere differenti letture, quale, in

[40] Rileva S. MELCHIONNA, *op. cit.*, p. 285, che inizialmente la lettura composita è stata prospettata dall'Autorità di controllo tedesca (*Unabhängige Landeszentrum für Datenschutz (ULD), Kurzpapier Nr. 1 – Verzeichnis von Verarbertunstätigkeiten* – Art. 30 DS-GVO, del 29 settembre 2017).

[41] In tal senso si è espresso anche il *Position Paper on the dergations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR* del Gruppo di lavoro Articolo 29 del 19 aprile 2018, il quale ha ritenuto che «the wording of Article 30(5) is clear in providing that the three types of processing to which the derogation does not apply are alternative ("or") and the occurrence of any one of them alone triggers the obligation to maintain the record of processing activities». In questo senso si è peraltro orientato il Garante per la protezione dei dati personali nel provvedimento n. 278 del 17 dicembre 2020 (doc. web n. 9529527), dove si è affermato che «la deroga alla tenuta del registro prevista dal Regolamento non opera in presenza anche di uno solo degli elementi indicati dall'art. 30, par. 5 (trattamento che presenta un rischio per i diritti e le libertà dell'interessato, trattamento non occasionale, trattamento che includa categorie particolari di dati di cui all'art. 9 o dati relativi a condanne penali e a reati)».

particolare, quella che al fine di escludere l'operatività dell'esenzione richiede contemporaneamente che il trattamento presenti un rischio per i diritti e le libertà dell'interessato e che il trattamento sia o non occasionale o riguardante dati particolari/giudiziali[42]. D'altronde, non può essere nascosto il *favor* verso i registri delle attività di trattamento manifestato dal Garante per la protezione dei dati personali, il quale ha auspicato che i titolari del trattamento e i responsabili del trattamento si adoperino per la tenuta dei registi indipendentemente dai propri requisiti dimensionali[43].

7. I registri come strumenti di valutazione e documentazione della conformità del trattamento al GDPR.

Quanto sinora detto consente di confermare che la tenuta dei registri della attività di trattamento risulta complementare all'attuazione del principio di responsabilizzazione, costituendo altresì un indispensabile strumento di cooperazione con il Garante per la protezione dei dati personali, dovendosi peraltro attribuire ai registri in questione una ulteriore e non marginale funzione laddove gli stessi consentono di determinare la conformità del trattamento alla normativa in tema di protezione dei dati personali.

Una chiara indicazione in tal senso sembra desumibile dai primi provvedimenti di ingiunzione del Garante per la protezione dei dati personali relativi all'art. 30 *GDPR,* dove si è affermato che i «registri […] sono indispensabili per consentire di valutare e documentare la conformità dei trattamenti alla disciplina in materia di protezione dei dati personali e dunque sono preliminari rispetto all'avvio degli stessi»[44].

Per quanto tale rilevanza attribuita ai registri sembra andare oltre quanto indicato dall'art. 6 *GDPR* laddove si individuano le condizioni di liceità del trattamento con una formulazione che difficilmente consente di riferirsi all'adempimento di cui all'art. 30 *GDPR,* una differente conclusione si giustifica ricordando che l'obbligo di tenuta del registro dei trattamenti costituisce un prerequisito dell'attività di trattamento laddove consente di soddisfare la responsabilizzazione della stessa, risultando finanche funzionale all'obbligo di garantire l'adeguatezza delle misure di sicurezza e protezione dei dati personali[45], con ciò dando concretezza al nesso inscindibile che il legislatore europeo ha voluto costituire tra il processo di gestione dei dati personali e la liceità del loro trattamento.

---

[42] Così, ad esempio, G. ARCELLA, *GDPR: il registro delle attività di trattamento e le misure di* accountability, in *Notariato*, 2018, p. 393.

[43] In tal senso si esprime la già citata Guida per l'applicazione del Regolamento europeo in materia di protezione dei dati personali emanata dal Garante per la protezione dei dati personali, dove «si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro» (p. 26).

[44] Il riferimento è al provvedimento n. 268 del 21 luglio 2022 (doc. web n. 9811271), ma in senso non dissimile, ancorché senza riferirsi alla idoneità a «documentare la conformità al trattamento», i provvedimenti nn. 292 e 293 del 22 luglio 2021 (doc. web nn. 9698558 e 9698597), n. 134 del 7 aprile 2022 (doc. web n. 9768363).

[45] Su questo punto si rivela particolarmente interessante la recente pronuncia della Corte di Giustizia UE 14 dicembre 2023, C-340/21, *VB* c. *Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986, in *Foro it.*, 2024, IV, c., 58 ss. Sul tema vd. A. MONTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Leggi civ. comm.*, 2017, p. 144 ss.; ID., *La gestione del rischio*, in *La protezione dei dati personali in Italia*, cit., p. 473 ss.

A tale riguardo sembra imprescindibile riscoprire una prospettiva non sempre adeguatamente considerata dagli interpreti, vale a dire quella che muovendo dal nesso intercorrente tra riservatezza e diritto alla tutela dei dati personali chiarisce che quest'ultimo costituisce «una distinta figura di diritto della personalità, in quanto l'interesse a non subire un abusivo trattamento dei dati personali è esso stesso un distinto interesse della persona»[46].

In questo contesto, l'obbligo di tenuta del registro dell'attività di trattamento esplicita quel necessario bilanciamento tra diritto all'informazione e diritto alla riservatezza che, oggi come ieri, sottende alla normativa sulla tutela dei dati personali e che deve essere assunto quale «punto fermo di orientamento per l'interprete»[47], rivelando in definitiva la sua centralità nel vigente quadro normativo e regolamentare della protezione dei dati personali.

[46] C.M. Bianca, *I. Note introduttive*, in *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 («Codice della* privacy*»)*, cit., p. XXII, e in termini non dissimili anche Id., *Il diritto alla riservatezza*, già in *Valore della persona e giustizia contrattuale. Scritti in onore di Adriano de Cupis*, Milano, 2005, p. 37 ss., e più di recente in Id., *Realtà sociale ed effettività della norma*, Torino, 2023, p. 89 ss. e spec. p. 96.
[47] C.M. Bianca, *I. Note introduttive*, cit., p. XXXI.