La regolamentazione e la tutela amministrativa

Elia Cremona

Abstract: This chapter analyses the public bodies entrusted with regulating, monitoring and enforcing data protection and data governance rules. In particular, it illustrates the sanctioning and non-sanctioning measures that can be taken by the supervisory authority.

Keywords: Data protection bodies, data governance bodies, penalties, administrative actions

1. Il ruolo dell'autorità garante nazionale

Il Garante per la protezione dei dati personali, anche noto come Garante privacy, è un'autorità amministrativa indipendente. L'autorità è stata istituita con la l. n. 675/96, la quale recepiva la direttiva 95/46/CE, ed è oggi «Autorità di controllo» incaricata di controllare la corretta applicazione del Regolamento in materia di protezione dei dati personali ai sensi dell'art. 51 GDPR e dell'art. 153 del d.lgs. 196/2003 (d'ora in avanti: cod. privacy).

L'istituzione del Garante per la Privacy nasce dall'esigenza di proteggere le persone fisiche riguardo al trattamento dei loro dati personali, garantendo che tale trattamento avvenga nel rispetto dei diritti e delle libertà fondamentali, senza che – allo stesso tempo – sia pregiudicata la libera circolazione dei dati personali all'interno dell'Unione.

Il Garante, dunque, si configura oggi come una autorità amministrativa con una *mission* supplementare rispetto ad altre autorità: non è chiamato a svolgere una attività meramente tecnica di regolazione del mercato in un'ottica di efficienza economica, ma ha il compito di presidiare la tutela di diritti e libertà fondamentali.

Per questa ragione, è particolarmente importante che sia assicurata l'indipendenza dei suoi componenti nell'adempimento dei propri compiti e nell'esercizio dei propri poteri, ai sensi dell'art. 52 GDPR. I componenti del collegio, infatti, debbono astenersi da qualunque attività incompatibile con le loro funzioni per tutta la durata del mandato.

Elia Cremona, University of Siena, Italy, elia.cremona@unisi.it, 0000-0001-9336-218X

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Ai sensi dell'art. 153 cod. privacy, il collegio è composto da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato (i parlamentari possono cioè esprimere un numero di preferenze inferiore rispetto al totale dei candidati, in modo da assicurare l'elezione di almeno un candidato espresso dai gruppi di minoranza).

Dal 2018 si prevede poi che i componenti siano eletti tra coloro che presentano la propria candidatura nell'ambito di una procedura di selezione il cui avviso deve essere pubblicato nei siti internet della Camera, del Senato e del Garante. Le candidature possono essere avanzate da persone che assicurino, come accennato, indipendenza e che risultino di comprovata esperienza nel settore della protezione dei dati personali, con particolare riferimento alle discipline giuridiche o dell'informatica.

I componenti eleggono tra loro un presidente, il cui voto prevale in caso di parità, e un vicepresidente, che assume le funzioni del presidente in caso di sua assenza o impedimento. L'incarico di presidente e quello di componente hanno durata settennale e non sono rinnovabili.

L'autorità opera in piena autonomia, sia amministrativa che finanziaria, e le sue decisioni possono essere impugnate solo davanti al giudice ordinario.

Il ruolo del Garante è variegato e comprende diversi «compiti» (*ex* art. 57 GDPR e 154 cod. privacy) e «poteri» (*ex* art. 58 GDPR e 154-*bis* cod. privacy).

Tra i «compiti» vi è naturalmente quello di assicurare e sorvegliare l'applicazione del GDPR da parte di soggetti pubblici e privati, controllando altresì l'applicazione delle norme nazionali in materia di protezione dei dati. Questo include, ad esempio, la verifica che i dati siano raccolti e trattati solo per finalità legittime, che il trattamento sia proporzionato e trasparente, o che siano adottate tutte le misure necessarie per garantire la sicurezza dei dati, evitando accessi non autorizzati, perdite o distruzioni accidentali.

A questa competenza principale si affiancano ulteriori compiti di carattere informativo, finalizzati alla promozione della consapevolezza pubblica su questi temi, e l'attività consultiva, principalmente rivolta nei confronti del Parlamento, del Governo e di altri organismi istituzionali. Il Garante è altresì titolare di specifiche competenze regolatorie di integrazione contrattuale consistenti ad esempio nella adozione di «clausole contrattuali tipo» o nella approvazione delle «norme vincolanti d'impresa», v. cap. Le fonti della disciplina in materia di dati personali).

Per quanto riguarda invece i «poteri», si distinguono i) i poteri di indagine, ii) i poteri correttivi e sanzionatori e iii) i poteri autorizzativi e consultivi.

Quanto ai primi, essi consentono all'autorità di condurre accertamenti e raccogliere informazioni. Ad esempio, può richiedere informazioni al titolare del trattamento e al responsabile del trattamento, può effettuare ispezioni e audit dei trattamenti di dati, può accedere a qualsiasi locale in cui sono trattati i dati.

Quanto ai poteri correttivi e sanzionatori, essi includono il potere di emettere ammonimenti o avvertimenti al titolare o al responsabile del trattamento, di imporre limiti o divieti sul trattamento dei dati, di disporre la rettifica o la

cancellazione di dati personali o la limitazione del trattamento e, infine, come si vedrà, di comminare sanzioni amministrative, comprese le multe.

Infine, per quanto attiene ai poteri autorizzativi e consultivi, essi consentono all'autorità di controllo di intervenire in alcune situazioni su richiesta di soggetti pubblici e privati, potendo rilasciare pareri – quando richiesto – in materia di trattamenti o autorizzare clausole contrattuali standard o meccanismi di trasferimento di dati verso paesi terzi. Il Garante ha anche il potere di esprimere pareri su atti normativi e regolamenti che possono influire sulla protezione dei dati personali, assicurando che ogni nuova normativa rispetti i principi fondamentali della materia. Inoltre, gestisce i reclami presentati dai cittadini riguardanti presunte violazioni dei loro diritti relativi alla privacy.

Oltre alle sue attività a livello nazionale, il Garante per la Privacy collabora strettamente con altre autorità nazionali per la protezione dei dati all'interno dell'Unione Europea e a livello internazionale. Questo lavoro di collaborazione è fondamentale per affrontare le sfide globali legate alla protezione dei dati, come l'armonizzazione delle normative tra diversi paesi e la gestione delle problematiche legate ai trasferimenti internazionali di dati personali.

2. Il ruolo dell'European Data Protection Board e il meccanismo di coerenza

L'European Data Protection Board (EDPB) è un organismo indipendente dell'UE istituito dal GDPR, con il compito di garantire un'applicazione coerente del regolamento in tutta l'Unione Europea. Esso è composto dai rappresentanti delle autorità di controllo di ciascun Stato membro e dal Garante europeo per la protezione dei dati. Il Board raccoglie l'eredità del Working Party 29, gruppo di lavoro istituito ai sensi dell'art. 29 della previgente direttiva 95/46/CE che aveva avviato un'importante opera di interpretazione e indirizzo volta ad armonizzare l'applicazione del diritto europeo in materia di protezione dei dati personali.

Le funzioni dell'EDPB sono disciplinate dagli articoli 68-76 del GDPR e si caratterizzano per una doppia natura, in parte consultiva e in parte decisoria. In particolare, come previsto dall'art. 70 GDPR, il Board ha il compito di monitorare l'attuazione del Regolamento e di assicurare la corretta applicazione del regolamento attraverso la pubblicazione di linee guida, raccomandazioni e buone prassi.

Il Board fornisce inoltre pareri e consulenze alla Commissione, relativamente agli adempimenti connessi all'applicazione del GDPR, e alle autorità di controllo nazionali. In particolare, coordina e supervisiona il funzionamento del «meccanismo di coerenza», uno degli strumenti fondamentali per garantire l'uniformità nell'applicazione del GDPR (*ex* artt. 63-66 del Regolamento).

Ai sensi dell'art. 64 GDPR, infatti, viene richiesto da parte delle autorità nazionali il parere dell'EDPB quando queste redigono una lista dei tipi di trattamenti che richiedono una valutazione di impatto (DPIA), o quando approvano clausole contrattuali standard per il trasferimento di dati verso paesi terzi o organizzazioni internazionali, o ancora codici di condotta che riguardano il trattamento di dati personali transfrontaliero o internazionale.

In tutti questi casi, l'EDPB è tenuto ad intervenire secondo una procedura dettagliata, che prevede: 1) *Richiesta di parere*: l'autorità di controllo che intende adottare una misura, che può avere un impatto su trattamenti transfrontalieri o può richiedere un'armonizzazione a livello europeo, invia una richiesta formale di parere all'EDPB; 2) *Termine per il parere dell'EDPB*: l'EDPB deve emettere il suo parere entro un termine massimo di otto settimane dalla ricezione della richiesta. Tale termine può essere prorogato di altre sei settimane per questioni particolarmente complesse. L'autorità di controllo che ha richiesto il parere deve necessariamente attendere la decisione dell'EDPB prima di adottare la propria misura; 3) *Efficacia del parere*: Sebbene i pareri dell'EDPB non siano sempre vincolanti, l'autorità di controllo, ricevuta la notifica, è tenuta a dare seguito a essi e a giustificare ogni eventuale decisione contraria.

In casi di disaccordo, può essere attivato il «meccanismo di composizione delle controversie» dell'art. 65. Il meccanismo si applica in situazioni in cui, ad esempio, vi sia disaccordo tra un'autorità di controllo competente e l'EDPB o tra l'autorità di controllo capofila e le altre autorità interessate in un trattamento transfrontaliero.

La procedura inizia con la richiesta di una delle autorità coinvolte all'EDPB di intervenire per risolvere la controversia. Il Board emette quindi una decisione vincolante entro un mese (prorogabile di altre due settimane per casi particolarmente complessi). Questa decisione può confermare il parere dell'autorità principale, accogliere i punti sollevati dalle altre autorità o risolvere questioni specifiche di disaccordo. Una volta adottata, la decisione vincolante viene notificata a tutte le autorità coinvolte, le quali devono poi applicarla nei rispettivi ordinamenti nazionali.

L'articolo 65 si collega strettamente al meccanismo dello sportello unico (c.d. *one-stop-shop*) previsto dall'art. 60 GDPR. In caso di trattamenti transfrontalieri, infatti, l'autorità capofila adotta la decisione notificandola presso lo stabilimento principale del titolare o responsabile del trattamento, ma il meccanismo di risoluzione delle controversie garantisce che, anche in caso di disaccordi tra le autorità, vi sia un intervento dell'EDPB volto ad assicurare coerenza.

3. Il ruolo dell'European Data Protection Supervisor

L'European Data Protection Supervisor (EDPS), o Garante europeo per la protezione dei dati, è un organismo dell'Unione istituito per garantire che le istituzioni e gli organismi dell'Unione Europea rispettino le norme sulla protezione dei dati personali. Il suo mandato è disciplinato dal Regolamento UE 2018/1725, che stabilisce le regole per il trattamento dei dati personali da parte delle istituzioni europee, riflettendo principi simili a quelli del GDPR.

Il Parlamento europeo e il Consiglio nominano di comune accordo il Garante europeo della protezione dei dati, per un periodo di cinque anni, in base a un elenco predisposto dalla Commissione dopo un invito pubblico a presentare candidature. L'elenco di candidati deve essere composto da personalità che offrano ogni garanzia di indipendenza e che possiedano una conoscenza specialistica in materia di protezione dei dati.

A differenza delle autorità di controllo nazionali, che vigilano sull'applicazione del GDPR nei singoli Stati membri, l'EDPS ha la responsabilità esclusiva di monitorare il rispetto delle norme in materia di protezione dei dati personali da parte del Parlamento Europeo, della Commissione Europea e del Consiglio dell'Unione Europea. Nell'ambito dell'assetto istituzionale dell'Unione, riveste un duplice ruolo: da un lato, assicura la conformità del trattamento dei dati delle istituzioni europee, dall'altro fornisce pareri consultivi in materia di protezione dei dati, in particolare quando nuove normative o politiche UE impattano sui diritti dei cittadini.

Tra i poteri dell'EDPS rientrano quelli di condurre indagini e prendere misure correttive in caso di violazioni delle norme sulla protezione dei dati. Può altresì emettere ammonimenti, ordini di rettifica o cancellazione dei dati trattati in modo illegittimo, e imporre limitazioni o divieti sul trattamento. Come accennato, si tratta di poteri che riflettono quelli delle autorità di controllo nazionali, ma sono focalizzati esclusivamente sulle istituzioni dell'UE.

Un altro aspetto rilevante del mandato dell'EDPS è la sua partecipazione in seno all'European Data Protection Board (EDPB), nell'ambito del quale collabora, ad esempio, nella risoluzione di eventuali questioni transfrontaliere riguardanti il trattamento di dati personali da parte delle istituzioni UE.

L'EDPS gioca anche un ruolo di primo piano nella promozione della consapevolezza sui diritti alla protezione dei dati. Secondo l'art. 57(1)(b) del Regolamento 2018/1725, il Garante ha il compito di informare e sensibilizzare il pubblico e le istituzioni dell'UE sui rischi, le norme e i diritti relativi alla protezione dei dati personali.

4. Le autorità per i servizi di intermediazione dei dati e per l'altruismo dei dati

Come si è visto nel Capitolo precedente, il fenomeno della circolazione dei dati è regolato da norme ulteriori e complementari rispetto al GDPR, che si limita a disciplinare le forme e i modi del trattamento dei dati personali. Tra queste, il *Data Governance Act* (Regolamento UE 2022/868), delinea le responsabilità di ulteriori autorità con l'obiettivo di promuovere un utilizzo responsabile e sicuro dei dati sia a livello commerciale sia a fini altruistici.

In particolare, gli Stati membri sono obbligati a designare le «autorità competenti per i servizi di intermediazione dei dati» e quelle «per la registrazione delle organizzazioni per l'altruismo dei dati».

Con riferimento alle prime, ai sensi dell'art. 13 del *Data Governance Act*, la designazione di una o più autorità competenti è funzionale a gestire la procedura di notifica e monitoraggio dei fornitori di servizi di intermediazione dei dati. Queste autorità sono cioè incaricate di verificare la conformità dei fornitori ai requisiti stabiliti dal Regolamento, nonché di intervenire in caso di violazioni. Tra i loro poteri, figurano la richiesta di informazioni necessarie per il controllo e la possibilità di imporre sanzioni o di sospendere i servizi in caso di mancato rispetto delle norme.

Queste autorità devono cooperare strettamente con altre entità nazionali, come le autorità per la protezione dei dati, le autorità di concorrenza e quelle

responsabili della sicurezza informatica, per garantire una regolamentazione armonizzata e coerente a livello nazionale e sovranazionale.

Le autorità competenti per la registrazione delle organizzazioni per l'altruismo dei dati hanno invece il compito, ai sensi dell'art. 23 del Data Governance Act, di mantenere un registro pubblico delle organizzazioni riconosciute che operano a fini di altruismo dei dati. Queste organizzazioni, che raccolgono dati messi a disposizione volontariamente dai cittadini per finalità di interesse generale, devono rispettare criteri rigorosi di trasparenza e sicurezza. Le autorità competenti monitorano il rispetto di tali criteri e collaborano con altre entità per garantire, anche in questo caso, la corretta gestione dei dati, in particolare quando tali dati comprendono informazioni personali.

Ogni Stato membro deve notificare alla Commissione Europea le autorità competenti individuate e tali registrazioni sono rese pubbliche per garantire trasparenza e fiducia nel sistema.

Infine, sia le autorità di intermediazione dei dati che quelle per l'altruismo dei dati debbono essere giuridicamente indipendenti e garantire l'imparzialità delle loro decisioni, al fine di promuovere un ambiente di scambio dei dati sicuro e trasparente per cittadini e aziende.

5. Il Comitato europeo per l'innovazione in materia di dati

Il Comitato europeo per l'innovazione in materia di dati, istituito dalla Commissione Europea, è un gruppo di esperti volto a promuovere una governance efficace dei dati nell'Unione Europea. Questo comitato è composto da rappresentanti delle autorità competenti per i servizi di intermediazione dei dati, per la registrazione delle organizzazioni per l'altruismo dei dati, del Comitato europeo per la protezione dei dati, del Garante europeo della protezione dei dati, dell'European Union Agency for Cybersecurity (ENISA), della Commissione e da altri rappresentanti rilevanti, inclusi quelli per le PMI e altri settori specifici.

Secondo l'articolo 29 del *Data Governance Act*, il Comitato ha – tra gli altri – il compito di consigliare e assistere la Commissione nello sviluppo di una prassi coerente per il riutilizzo dei dati e per l'altruismo dei dati nell'Unione. Il Comitato opera anche attraverso la costituzione di sottogruppi che si occupano di specifici temi, come le questioni tecniche legate alla portabilità e interoperabilità dei dati, oltre che al coinvolgimento dei portatori di interessi, incluse le imprese e la società civile.

6. Le sanzioni amministrative e gli altri provvedimenti dell'autorità

Il rispetto del Regolamento è garantito attraverso un complesso sistema sanzionatorio, di natura amministrativa e penale, a seconda della gravità dell'infrazione commessa. In particolare, l'articolo 83 GDPR stabilisce un sistema di sanzioni amministrative pecuniarie. Per espressa previsione della norma, tali sanzioni devono essere «effettive, proporzionate e dissuasive», e il loro ammontare varia a seconda della gravità della violazione e delle circostanze del

caso specifico. Le sanzioni pecuniarie possono arrivare fino a 20 milioni di euro o al 4% del fatturato mondiale annuo dell'impresa, a seconda di quale delle due sia la cifra maggiore.

Il GDPR distingue due livelli di gravità delle violazioni, con sanzioni differenti. Il primo livello, disciplinato dal paragrafo 4 dell'articolo 83, prevede multe fino a 10 milioni di euro o al 2% del fatturato annuo globale, per violazioni legate agli obblighi di natura tecnica e organizzativa. Ad esempio, rientrano in questa categoria le violazioni degli articoli 8 (condizioni applicabili al consenso dei minori), 11 (trattamento che non richiede identificazione), e 25-39, che riguardano i principi di «privacy by design» e «privacy by default», la nomina e i compiti del responsabile della protezione dei dati (DPO), e altre misure tecniche e organizzative atte a garantire la sicurezza dei dati personali.

Il secondo livello di gravità, disciplinato dai paragrafi 5 e 6 dell'articolo 83, prevede sanzioni più severe, fino a 20 milioni di euro o al 4% del fatturato mondiale annuo, per violazioni dei principi fondamentali del GDPR. In questa categoria rientrano le violazioni degli articoli 5, 6, 7 e 9, che trattano i principi di base per il trattamento dei dati, le condizioni di liceità del trattamento, le condizioni per il consenso e il trattamento di categorie particolari di dati personali, come quelli relativi alla salute o all'orientamento sessuale. Anche le violazioni riguardanti i diritti degli interessati, previsti negli articoli 12-22, come il diritto di accesso, rettifica, cancellazione (diritto all'oblio), portabilità e opposizione, sono soggette a tale trattamento sanzionatorio.

Le autorità di controllo, che hanno il compito di monitorare la conformità al GDPR, sono i soggetti deputati alla irrogazione delle sanzioni in caso di violazione. Nel decidere se infliggere una sanzione amministrativa pecuniaria e nel determinare il suo importo, l'autorità di controllo deve tenere in considerazione una serie di fattori elencati nel paragrafo 2 dell'articolo 83, che include undici criteri specifici. Tra questi figurano: la natura, la gravità e la durata della violazione, avuto riguardo al tipo di trattamento e al numero di soggetti coinvolti; il carattere doloso o colposo della violazione; le misure adottate per attenuare i danni subiti dagli interessati; il grado di responsabilità del titolare o del responsabile del trattamento, considerando le misure tecniche e organizzative adottate in conformità con gli articoli 25 e 32; le eventuali precedenti violazioni pertinenti; il grado di cooperazione con l'autorità di controllo; le categorie di dati personali interessate dalla violazione, come dati particolari ai sensi dell'articolo 9; le modalità con cui l'autorità di controllo ha preso conoscenza della violazione, ad esempio, se la violazione è stata notificata dal titolare come previsto dall'articolo 33; l'adesione a codici di condotta o meccanismi di certificazione.

Tutti questi criteri devono essere contemporaneamente presi in considerazione dall'autorità di controllo nella commisurazione della sanzione da infliggere, che deve quindi essere sempre proporzionalmente gradata.

Inoltre, il paragrafo 3 dell'articolo 83 stabilisce che se un titolare del trattamento o un responsabile viola con dolo o colpa più disposizioni del GDPR in relazione allo stesso trattamento o a trattamenti collegati, l'importo totale della sanzione non deve superare quello previsto per la violazione più grave. Questo al

fine di evitare un cumulo di sanzioni sproporzionato e di garantire che la multa sia ragionevole in base alla gravità complessiva della condotta.

Oltre alla funzione correttiva, le sanzioni del GDPR perseguono un importante scopo dissuasivo. La severità del trattamento sanzionatorio mira a scoraggiare le imprese dal violare le norme, promuovendo al contempo una cultura di *compliance* alla disciplina in materia di protezione dei dati personali. Per esempio, l'articolo 58, paragrafo 2, conferisce alle autorità di controllo ampi poteri correttivi, tra cui l'emissione di ammonimenti, ordini di limitazione o sospensione del trattamento.

In Italia, come si è detto in apertura di questo Capitolo, il Garante per la protezione dei dati personali è l'autorità di controllo designata per l'applicazione delle sanzioni del GDPR. Il d.lgs. 196/2003 ha modificato il Codice Privacy (d.lgs. 196/2003) per allinearlo al GDPR. Tra le modifiche più significative, vi è stata proprio l'introduzione di sanzioni amministrative per le violazioni del Codice italiano che corrispondono a quelle previste dal GDPR. Il Garante ha il potere di avviare procedimenti sanzionatori sia su segnalazione degli interessati sia d'ufficio, e può imporre provvedimenti correttivi in caso di violazioni accertate.

7. Le azioni nei confronti dell'autorità di controllo

Contro i provvedimenti del Garante per la protezione dei dati personali può essere presentato ricorso innanzi al giudice ordinario in virtù del combinato disposto degli artt. 78 GDPR, 152 cod. privacy, e 10 del d.lgs. 150/2011 recante la disciplina dei procedimenti civili semplificati. In particolare, l'art. 78 GDPR garantisce agli interessati il diritto a un ricorso giurisdizionale effettivo contro le decisioni dell'autorità di controllo, mentre l'art. 152 cod. privacy disciplina le modalità di impugnazione dei provvedimenti del Garante, rinviando per quanto attiene ai profili processuali al d.lgs. 150/2011.

Quest'ultimo, all'art. 10, stabilisce che i provvedimenti del Garante possono essere impugnati dinanzi al giudice ordinario, che il ricorso deve essere presentato entro 30 giorni dalla notifica del provvedimento o entro 60 giorni se il ricorrente è residente all'estero. Il ricorrente può altresì dare mandato a un ente del terzo settore che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, che può esercitare l'azione in sua vece.

Durante il procedimento, il ricorrente può chiedere la modifica, la sospensione o l'annullamento del provvedimento del Garante, come nei casi di sanzioni amministrative ritenute sproporzionate o di presunte violazioni procedurali. Il giudice esamina la legittimità del provvedimento e il rispetto delle regole relative al procedimento che ne ha condotto all'adozione: un vizio di legittimità nell'attività procedimentale (ad esempio, l'eccessiva durata della fase istruttoria) può infatti determinare l'annullabilità del provvedimento finale, ancorché sostanzialmente corretto.

La sentenza che definisce il giudizio non è appellabile e può prescrivere tutte le misure ritenute necessarie dal giudice, anche in difformità da quanto previsto dal provvedimento impugnato, oltre a provvedere – quando richiesto – in merito al risarcimento del danno.

Riferimenti bibliografici

Belisario, E., G. M. Riccio e G. Scorza. 2023. *GDPR e normativa privacy*. Alphen aan den Rijn: Wolters Kluwer, pp. 729 ss.

Bolognini, L., E. Pellino e C. Bistolfi (a cura di). 2016. *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*. Milano: Giuffrè.

European Data Protection Board (EDPB). 2022. *Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR*. [s.l.]: EDPB.

Grossi, L. 2023. "Sulla decisione della Data Protection Commission irlandese nel caso Meta: il ruolo delle autorità indipendenti nella protezione dei dati personali." In *Rivista della regolazione dei mercati*, fasc. 2/2023, pp. 474 ss.

Guzzardo, G. 2018. "Accountability e pubbliche Amministrazioni nel regolamento europeo in materia di protezione dei dati personali." In *Amministrazione In Cammino*, 1° aprile 2018.