Adeguatezza nel GDPR

Il termine “adeguatezza” e gli altri vocaboli con la medesima radice sono presenti 113 volte nel testo italiano del GDPR.

L’adeguatezza è sinonimo di “proporzionalità” cioè, essere in giusta relazione con l’elemento di raffronto.

L’adeguatezza del GDPR non è una caratteristica presente nel mondo materiale ma è una circostanza desumibile da una valutazione obiettiva di proporzionalità calata nello specifico contesto, tenendo in considerazione determinati criteri [v. considerando (76)]. Questa valutazione va rivisitata periodicamente e ogni volta che mutano gli elementi che sono stati a fondamento del giudizio (art. 24, ult. frase, GDPR).

Il principio di adeguatezza, nel GDPR, è prevalentemente riferito a:

* Le **misure** di sicurezza tecnico-organizzative
* Le **garanzie** per la difesa dei diritti e delle libertà fondamentali degli interessati.



# Adeguatezza delle misure

In linea di principio l’adeguatezza incorpora un obiettivo che il legislatore intende raggiungere: ad esempio, le misure di sicurezza tecnico-organizzative sono adeguate (proporzionate) al rischio, per conseguire una sicurezza adeguata (idonea). Il legislatore del GDPR esprime questo concetto nella formulazione dell’articolo 32 quando prescrive: «*(…) il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (…)*».

A prima vista, la formulazione sembrerebbe ripetitiva (i.e. “misure adeguate per una sicurezza adeguata”); al contrario, essa intende esprimere un preciso concetto: le misure di sicurezza devono essere adeguate di per sé, cioè, essere intrinsecamente idonee a soddisfare determinate esigenze tecnico-organizzative **e, inoltre,** devono anche assicurare, nel contesto di riferimento, un livello di sicurezza proporzionato al rischio.

Ad esempio, l’adozione di un sistema di autenticazione deve essere adeguato (idoneo), di per sé, ad accertare l’identità dell’utente che richiede l’accesso a un sistema informatico oppure a una piattaforma software ma esso deve anche essere in grado di assicurare (obiettivo) un livello di sicurezza adeguato (proporzionato) al rischio presente nelle specifiche circostanze del caso. Questo secondo profilo, obbliga titolare e responsabile a individuare il livello di robustezza della misura tecnico-organizzativa, che sia confacente con lo scopo di ottenere un livello di sicurezza proporzionato al rischio. La stretta correlazione tra

* le misure di sicurezza idonee e
* il livello di rischio individuato

comporta che, aumentando il rischio, automaticamente deve corrispondere l’innalzamento del tasso di robustezza delle misure di sicurezza che si intende adottare. Misure astrattamente idonee ma non proporzionate all’effettivo rischio non sono conformi al principio di adeguatezza.

# Adeguatezza delle garanzie

Il GDPR non definisce cosa debba intendersi per “garanzia” ma applica il principio di adeguatezza, oltre che alle misure di sicurezza anche alle “garanzie”.

Dall’analisi complessiva del testo del regolamento emerge che il termine “garanzia” è utilizzato dal legislatore secondo un’accezione elastica. Talvolta, esso si riferisce genericamente a qualsiasi forma di tutela per l’interessato comprensiva, pertanto, delle misure di sicurezza tecnico-organizzative. È questo il caso della formulazione del Considerando (39) secondo cui «*[è] opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento.*». Analogamente, il Considerando (42) riporta che «*nel contesto di una dichiarazione scritta relativa a un'altra questione dovrebbero esistere garanzie che assicurino che l'interessato sia consapevole del fatto di esprimere un consenso e della misura in cui ciò avviene*», laddove per “garanzia” si intende la modalità atta a raccogliere un consenso consapevole suscettibile di dimostrazione. Oppure, ancora, nel Considerando (50) quando, trattando della compatibilità della finalità ulteriore, si chiede al titolare di tener conto, tra l’altro, «*dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto*».

Il significato ampio di “garanzia”, di cui ai richiamati esempi, si consolida in quei casi in cui il legislatore ha come riferimento una legge o un regime di protezione presente in un ordinamento extra UE-SEE. Come nel caso della flessibilità riconosciuta agli Stati membri di ammettere nuove ipotesi di deroghe al divieto di trattamento di particolari categorie di dati («*fatte salve adeguate garanzie*») e soprattutto riguardo alla condizione per il riconoscimento dell’equivalenza del livello di protezione del paese terzo oppure con riferimento agli strumenti a garanzia adeguata per i trasferimenti esteri di dati.

L’ampia portata della nozione viene precisata dal Considerando (108) che, con riferimento alle adeguate garanzie che gli strumenti per il trasferimento estero dei dati devono contenere, precisa: «*[t]ali garanzie dovrebbero assicurare un rispetto dei requisiti in materia di protezione dei dati e dei diritti degli interessati adeguato ai trattamenti all'interno dell'Unione, compresa la disponibilità di diritti azionabili degli interessati e di mezzi di ricorso effettivi, fra cui il ricorso effettivo in sede amministrativa o giudiziale e la richiesta di risarcimento, nell'Unione o in un paese terzo. Esse dovrebbero riguardare, in particolare, la conformità rispetto ai principi generali in materia di trattamento dei dati personali e ai principi di protezione dei dati fin dalla progettazione e di protezione dei dati di default.*».

Altre volte, il legislatore pur preservando il senso ampio del termine “garanzia”, lo utilizza riferendosi alternativamente a:

* **strumenti di protezione** (misure di sicurezza tecnico-organizzativa), come nel caso dell’articolo 6.4.e), per la valutazione della compatibilità della finalità ulteriore, si chiede al titolare di tener conto «*dell’esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione*», laddove il Considerando (50) precisa che tale valutazione deve tener conto anche, «*dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto*», oppure
* **oggetto della tutela** (diritti e libertà fondamentali dell’interessato), come in occasione della deroga per i trattamenti di dati sensibili nel contesto lavorativo «*in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato*» [art. 9.2.b), GDPR].

In conclusione, sulla base degli esempi richiamati, l’adeguatezza – sia essa riferita a misure di sicurezza o garanzie – intende esprimere il medesimo concetto dell’obbligo di un approccio proporzionato al rischio specificamente individuato, con l’obiettivo di assicurare una elevata protezione di diritti e libertà fondamentali dell’interessato.

# Elevato livello di protezione

In linea generale, l’adeguatezza nel GDPR mira a conseguire un **elevato livello di protezione** per i diritti e le libertà fondamentali degli interessati, in quanto «*il legislatore dell’Unione ha inteso rafforzare sia i diritti di tali persone sia gli obblighi dei titolari del trattamento, rispetto alle disposizioni anteriori a tale regolamento, come indicato dal considerando 11 di quest’ultimo*» ([CGUE, c-340/21](https://curia.europa.eu/juris/document/document.jsf?text=&docid=280623&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=4213110), par. 56, [c-300/21](https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=4231553), par. 48, con richiami).

Si è conformi al GDPR se si è in grado di operare attività di trattamento di dati personali con modalità che siano proporzionate al rischio che esse generano, assicurando un elevato livello di protezione degli interessati; tale livello di protezione «*dipende dalle misure di sicurezza adottate dai titolari del trattamento di dati personali*» ([CGUE, c-340/21](https://curia.europa.eu/juris/document/document.jsf?text=&docid=280623&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=4213110), par. 55).

# Approccio basato sul rischio

L’adeguatezza è il precipitato dell’approccio normativo basato sul rischio.

La prescrizione scaturente dal principio di adeguatezza è un obbligo che ha natura relativa, determinato sulla base delle specifiche circostanze, in modo obiettivo.

La **natura relativa dell’adeguatezza** del GDPR agisce sotto due profili:

* in quanto essa si rapporta e acquista contenuto **in base alle circostanze specifiche** (caratteristiche del trattamento e contesto). Il giudizio deve essere valutato «*in concreto, in particolare tenendo conto dei rischi connessi al trattamento di cui trattasi*», valutando la natura e il contenuto delle misure che sono attuate, il modo in cui sono state applicate e i «*loro effetti pratici sul livello di sicurezza che (il titolare) era tenuto a garantire*»; questa valutazione va riesaminata e aggiornata qualora necessario ([CGUE, c-340/21](https://curia.europa.eu/juris/document/document.jsf?text=&docid=280623&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=4213110), parr. 40, 45 e 25)
* perché l’adeguatezza delle misure di sicurezza ha come **obiettivo la limitazione dei rischi** anziché la loro eliminazione (CGUE, c-340/21, par. 29). La Corte di giustizia ha deciso nel senso che una violazione di dati personali (data breach), ai sensi dell’art. 4, 12) del GDPR, non è sufficiente «*di per sé, per ritenere che le misure tecniche e organizzative attuate dal titolare del trattamento in questione non fossero “adeguate”, ai sensi degli articoli 24 e 32*» (CGUE, c-340, punto 1 conclusioni).

La valutazione deve essere **obiettiva** «*prendendo in considerazione il grado di probabilità dei rischi individuati e il loro grado di gravità» passando poi a verificare se misure e garanzie siano adeguate a tali rischi, tenuto conto dello stato dell’arte, dei costi di attuazione nonché della natura, della portata, del contesto e delle finalità di tale trattamento*» ([CGUE, c-340/21](https://curia.europa.eu/juris/document/document.jsf?text=&docid=280623&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=4213110), par. 42).

## Obbligo di dimostrare l’efficacia

In ultima analisi, il principio di adeguatezza è espressione dell’accountability, in quanto esso è oggetto della conformità al regolamento ed è elemento dell’obbligo di dimostrazione, come è sancito dall’articolo 5, paragrafo 2, e concretizzato all’articolo 24 del GDPR ([CGUE, c-340/21](https://curia.europa.eu/juris/document/document.jsf?text=&docid=280623&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=4213110), parr. 48, 49, 52, 53).

In questo ambito, l’obbligo di dimostrare la conformità, di cui si compone l’accountability, si traduce nella dimostrazione dell’adeguatezza del proprio comportamento (proporzionato, in termini di misure e garanzie) ai rischi determinati dal trattamento nello specifico contesto.

L’**onere della prova dell’adeguatezza** di misure e garanzie adottate incombe al titolare del trattamento; la CGUE nella sua prima decisione relativa alle misure di sicurezza del GDPR, ha affermato che «*[d]al disposto dell’articolo 5, paragrafo 2, dell’articolo 24, paragrafo 1, e dell’articolo 32, paragrafo 1, del RGPD risulta senza ambiguità che l’onere di provare che i dati personali sono trattati in modo tale da garantire una loro adeguata sicurezza ai sensi dell’articolo 5, paragrafo 1, lettera f), e dell’articolo 32 di detto regolamento incombe al titolare del trattamento in parola*» ([CGUE, c-340/21](https://curia.europa.eu/juris/document/document.jsf?text=&docid=280623&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=4213110), par. 52, con richiami).

Il titolare, per non essere soggetto a responsabilità, deve essere in grado di dimostrare di aver fatto «*tutto il possibile per prevenire operazioni di trattamento non conformi a tale regolamento*» (CGUE, c-340/21, par. 55).

Questo concetto, nell’ambito della sicurezza dei dati personali, è espresso nel considerando (74) del regolamento che sottolinea l’importanza per il titolare del trattamento di attuare misure adeguate ed **efficaci** e di essere in grado di dimostrare la conformità delle attività di trattamento, **compresa l’efficacia delle misure** (CGUE, c-340/21, par. 35).

# Scrutinio dell’adeguatezza

L’adeguatezza delle misure tecniche e organizzative adottate ai sensi dell’articolo 32 del GDPR e, più in generale, delle garanzie per i diritti e le libertà fondamentali dell’interessato è soggetta allo scrutinio dell’autorità di supervisione e del giudice nazionale.

Autorità e giudice non devono «*limitarsi a constatare in che modo il titolare del trattamento interessato abbia inteso adempiere gli obblighi ad esso incombenti in forza di tale articolo, bensì effettuare un esame di tali misure nel merito, alla luce di tutti i criteri menzionati in detto articolo nonché delle circostanze proprie del caso di specie e degli elementi di prova di cui tale giudice dispone al riguardo.*

*Un siffatto esame richiede di procedere a un’analisi concreta sia della natura e del contenuto delle misure che sono state attuate dal titolare del trattamento, del modo in cui tali misure sono state applicate e dei loro effetti pratici sul livello di sicurezza che quest’ultimo era tenuto a garantire, tenuto conto dei rischi inerenti a tale trattamento.*» ([CGUE, c-340/21](https://curia.europa.eu/juris/document/document.jsf?text=&docid=280623&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=4213110), parr. 45, 46).

Sull’(in)adeguatezza delle misure adottate dal titolare, da ultimo, in merito ai trattamenti di dati connessi al fenomeno delle attivazioni non richieste, si veda il provvedimento del Garante del 28 settembre 2023 ([doc. web n. 9940988](https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9940988)).

# Adeguatezza nel ciclo di vita del trattamento

L’adeguatezza di misure e garanzie va assicurata durante tutto il ciclo di vita del trattamento di dati personali: prima della sua realizzazione, durante la realizzazione delle attività operative e all’atto della cessazione.

Ne è testimonianza il combinato degli articoli 24, 25 e 32, la precisazione contenuta al Considerando (39), nonché la disciplina su:

* la **valutazione d’impatto** che deve essere effettuata prima del trattamento e deve «*vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali e dimostrando la conformità al presente regolamento*» [Considerando (90), GDPR]
* la **violazione dei dati personali** (data breach) ai sensi degli articoli 33 e 34 del GDPR, in quanto l’autorità di controllo o il giudice effettuano due distinte valutazioni:
  + quella riguardante l’adeguatezza delle misure tecnico-organizzative attuate dal titolare o dal responsabile prima della realizzazione del data breach, al fine di verificarne l’astratta idoneità a **prevenire** la violazione, secondo un giudizio ex ante
  + l’altra, relativa alle misure adottate successivamente, al fine di **rimediare** le conseguenze nocive della violazione oppure per assicurare che analoghi data breach **non si verifichino in futuro**.

# Difetto di adeguatezza sanzionabile

L’eventuale difetto di proporzionalità è causa di non conformità e di violazione del principio di accountability.

La non conformità genera responsabilità imputabile prevalentemente in capo al titolare del trattamento, giustificando l’irrogazione delle sanzioni previste dagli articoli 83 e 84 del GDPR nonchè l’esercizio dell’azione di risarcimento per danni materiali e immateriali, da parte degli eventuali danneggiati.

Rosario Imperiali d’Afflitto