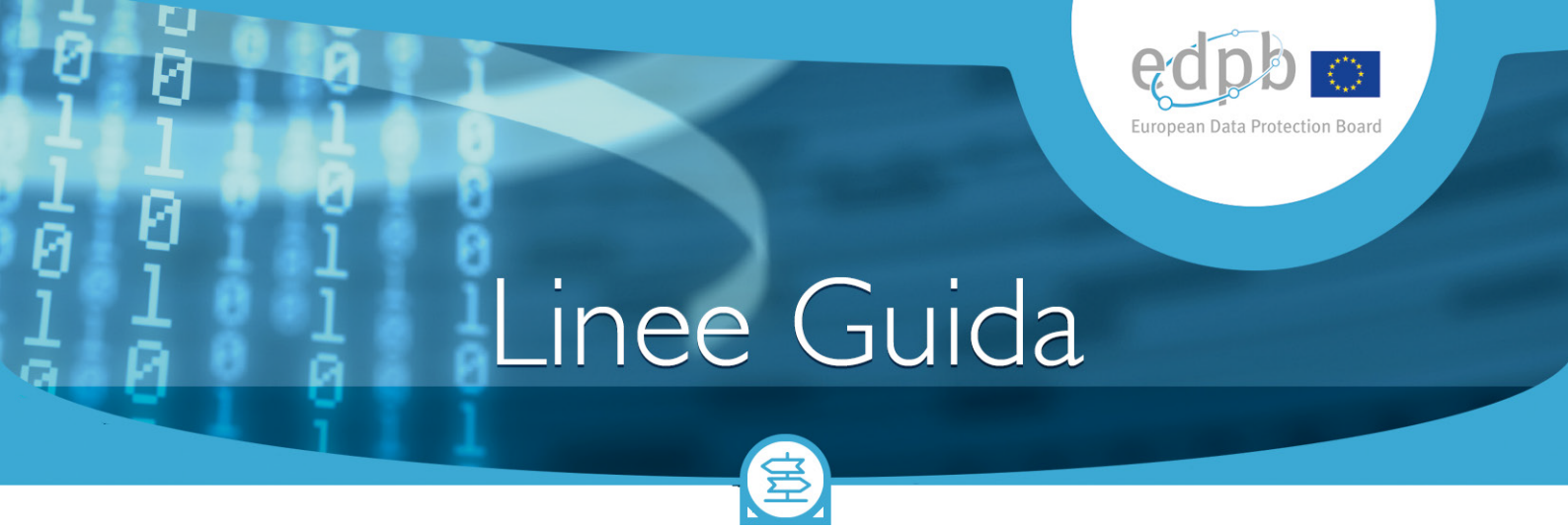


Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR

Versione 2.1

Adottate il 24 maggio 2023

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Adottato

Cronologia delle versioni

Versione 1.0	12 maggio 2022	Adozione delle linee guida per la consultazione pubblica
Versione 2.0	24 maggio 2023	Adozione delle linee guida dopo la consultazione pubblica
Versione 2.1	29 giugno 2023	Lieve modifica

SINTESI

Il Comitato europeo per la protezione dei dati (EDPB) ha adottato le presenti linee guida al fine di armonizzare la metodologia utilizzata dalle autorità di controllo per il calcolo dell'importo delle sanzioni pecuniarie. Le presenti linee guida integrano le linee guida precedentemente adottate riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679 (WP 253), che si concentrano sulle circostanze in cui infliggere una sanzione pecuniaria.

Il calcolo dell'importo di una sanzione pecuniaria rientra nella discrezionalità dell'autorità di controllo, fatte salve le norme previste dal regolamento generale sulla protezione dei dati (GDPR). In tale contesto, il GDPR impone che l'importo della sanzione pecuniaria sia in ogni singolo caso effettivo, proporzionato e dissuasivo (articolo 83, paragrafo 1, GDPR). Inoltre, nel fissare l'importo della sanzione pecuniaria, le autorità di controllo devono tenere debito conto di un elenco di elementi che fanno riferimento alle caratteristiche della violazione (la sua gravità) o al carattere del suo autore (articolo 83, paragrafo 2, GDPR). Infine l'importo della sanzione pecuniaria non deve superare i massimali previsti dall'articolo 83, paragrafi 4, 5 e 6, GDPR. La quantificazione dell'importo della sanzione pecuniaria si basa quindi su una valutazione specifica effettuata in ogni singola fattispecie, all'interno dei parametri previsti dal GDPR.

Tenendo conto di quanto sopra, l'EDPB ha elaborato la seguente metodologia, articolata in cinque fasi, per il calcolo delle sanzioni amministrative pecuniarie per le violazioni del GDPR.

In primo luogo devono essere individuati i trattamenti nel caso in questione e deve essere valutata l'applicazione dell'articolo 83, paragrafo 3, GDPR (**capitolo 3**). In secondo luogo occorre individuare il punto di partenza per l'ulteriore calcolo dell'importo della sanzione pecuniaria (**capitolo 4**); a tal fine si valuta la classificazione della violazione del GDPR, analizzandone la gravità alla luce delle circostanze del caso, e il fatturato dell'impresa. In terzo luogo si valutano le circostanze aggravanti e attenuanti legate al comportamento passato o presente del titolare/responsabile del trattamento e si aumenta o riduce conseguentemente la sanzione pecuniaria (**capitolo 5**). In terzo luogo si individuano gli importi massimi di legge previsti per le diverse violazioni. Gli aumenti applicati nelle fasi precedenti o successive non possono superare tali importi massimi (**capitolo 6**). Infine si deve analizzare se l'importo finale calcolato risponde ai requisiti di effettività, dissuasività e proporzionalità. La sanzione pecuniaria può essere ulteriormente adeguata di conseguenza (**capitolo 7**), ma senza superare il pertinente limite massimo di legge.

In tutte le fasi sopra descritte occorre tenere presente che il calcolo della sanzione pecuniaria non è un mero esercizio matematico. Al contrario, le circostanze del caso specifico sono i fattori determinanti che portano all'importo finale, che può - in tutti i casi - essere qualsiasi importo non superiore al limite massimo di legge.

Le presenti linee guida e la relativa metodologia saranno oggetto di costante revisione da parte dell'EDPB.

Indice

Il Comitato europeo per la protezione dei dati

visto l'articolo 70, paragrafo 1, lettere k), j) ed e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito "GDPR"),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

visti gli articoli 12 e 22 del proprio regolamento interno,

viste le linee guida del Gruppo di lavoro articolo 29 riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento 2016/679 (WP 253), approvate dal Comitato europeo per la protezione dei dati (di seguito "EDPB") nella sua prima riunione plenaria,

HA ADOTTATO LE SEGUENTI LINEE GUIDA

CAPITOLO 1 – INTRODUZIONE

1.1 – Contesto normativo

1. Con il regolamento generale sulla protezione dei dati (di seguito "GDPR"), applicabile dal 25 maggio 2018, l'UE ha attuato una riforma globale della normativa sulla protezione dei dati in Europa. La protezione delle persone fisiche in relazione al trattamento dei dati di carattere personale è un diritto fondamentale. Il regolamento si basa su diverse componenti fondamentali, una delle quali è il rafforzamento dei poteri di esecuzione delle autorità di controllo. Il regolamento impone un nuovo livello di sanzioni pecuniarie sostanzialmente più elevato, oltre a prevedere l'armonizzazione delle sanzioni pecuniarie tra gli Stati membri.

2. Ai titolari del trattamento e ai responsabili del trattamento dei dati sono attribuite maggiori responsabilità nel garantire che i dati personali degli interessati siano protetti in modo efficace. Le autorità di controllo sono dotate di poteri volti a garantire che i principi del GDPR e i diritti delle persone interessate siano rispettati conformemente all'enunciato e alla ratio del regolamento.

3. L'EDPB ha quindi elaborato orientamenti al fine di fornire una base chiara e trasparente per la previsione delle sanzioni pecuniarie da parte delle autorità di controllo. Le linee guida sull'applicazione e la previsione delle sanzioni amministrative pubblicate in precedenza esaminano le circostanze in cui una sanzione amministrativa pecuniaria sarebbe uno strumento adeguato, e forniscono un'interpretazione dei criteri dell'articolo 83, GDPR a tal riguardo[2]. Le presenti linee guida riguardano la metodologia per il calcolo delle sanzioni amministrative pecuniarie. I due insiemi di linee guida sono applicabili contestualmente e devono essere considerati complementari.

[1] Nel presente documento con il termine "Stati membri" si intendono gli "Stati membri del SEE".
[2] Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento 2016/679 (WP 253) (di seguito "linee guida WP 253"). L'EDPB ha approvato le linee guida WP 253 nel corso della sua prima riunione plenaria, il 25 maggio 2018. Cfr. l'approvazione 1/2018, disponibile online qui.

1.2 - Obiettivo

4. Le presenti linee guida sono destinate a essere utilizzate dalle autorità di controllo per garantire un'applicazione e un'attuazione coerenti del GDPR ed esprimono l'interpretazione comune dell'EDPB delle disposizioni di cui all'articolo 83, GDPR.

5. L'obiettivo delle presenti linee guida è quello di creare, come orientamento comune, dei punti di partenza armonizzati sulla base dei quali effettuare il calcolo delle sanzioni amministrative pecuniarie nei singoli casi. Tuttavia, secondo giurisprudenza consolidata, tali indicazioni non devono essere specifiche al punto da consentire a un titolare del trattamento o un responsabile del trattamento di effettuare un calcolo matematico preciso della sanzione pecuniaria prevista[3]. Nelle presenti linee guida si sottolinea che l'importo finale della sanzione pecuniaria dipende da tutte le circostanze del caso. L'EDPB prevede quindi, piuttosto che un'armonizzazione sul risultato, un'armonizzazione sui punti di partenza e sulla metodologia utilizzata per calcolare la sanzione pecuniaria.

6. Le presenti linee guida possono essere considerate come un approccio da seguire fase per fase, sebbene le autorità di controllo non siano tenute a seguire tutte le fasi se queste non sono applicabili in un determinato caso, né a fornire una motivazione sugli aspetti delle linee guida che non sono applicabili. Tuttavia la motivazione dovrebbe almeno includere i fattori che hanno portato a determinare il livello di gravità, il fatturato applicato e i fattori aggravanti e attenuanti applicati.

7. Nonostante le presenti linee guida, le autorità di controllo rimangono soggette a tutti gli obblighi procedurali previsti dall'ordinamento nazionale e dalla normativa dell'UE, compresi il dovere di motivare le proprie decisioni e gli obblighi previsti dal meccanismo dello sportello unico. In quest'ottica, sebbene le autorità di controllo siano tenute a fornire una motivazione sufficiente per le loro conclusioni in conformità del diritto nazionale e dell'UE, le presenti linee guida non devono essere interpretate come intese a imporre all'autorità di controllo di indicare l'importo iniziale preciso o di quantificare l'impatto esatto di ciascuna circostanza aggravante o attenuante. Inoltre il semplice riferimento alle presenti linee guida non può sostituire la motivazione che deve essere fornita nel caso specifico.

8. Le linee guida saranno sottoposte a una revisione costante, in base all'evolversi delle prassi nell'UE e nel SEE. Occorre rilevare che, fatta eccezione per la Danimarca e l'Estonia[4], le autorità di controllo sono autorizzate a irrogare sanzioni amministrative pecuniarie, che, se non impugnate, sono vincolanti. Nel tempo, quindi, la prassi amministrativa e giudiziaria è destinata a evolversi ulteriormente.

1.3 - Ambito di applicazione

9. Le presenti linee guida intendono disciplinare e porre le basi per la previsione delle sanzioni pecuniarie da parte delle autorità di controllo a livello generale. Gli orientamenti forniti si applicano a tutti i tipi di titolari del trattamento e responsabili del trattamento ai sensi dell'articolo 4, punti 7 e 8, GDPR, a eccezione delle persone fisiche quando non agiscono come imprese. Ciò non toglie che le autorità nazionali abbiano la facoltà di irrogare sanzioni pecuniarie alle persone fisiche.

10. Ai sensi dell'articolo 83, paragrafo 7, GDPR, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro. Purché le autorità di controllo abbiano tale facoltà sulla base del diritto

[3] Cfr., ad esempio, le cause C-189/02 P, C-202/02 P, da C-205/02 P a C-208/02 P e C-213/02 P, *Dansk Rørindustri A/S e altri contro Commissione*, punto 172 e la causa T-91/11, *InnoLux Corp. contro Commissione*, punto 88.
[4] Cfr. il considerando 151, GDPR.

nazionale, le presenti linee guida si applicano al calcolo delle sanzioni pecuniarie da infliggere ad autorità pubbliche e organismi pubblici, a eccezione della sezione 4.3. Le autorità di controllo rimangono comunque libere di applicare una metodologia simile a quella descritta in tale sezione. Inoltre il capitolo 6 non è applicabile al calcolo delle sanzioni pecuniarie da infliggere ad autorità pubbliche e organismi pubblici nel caso in cui l'ordinamento nazionale preveda limiti massimi di legge diversi e l'autorità pubblica o l'organismo pubblico non agisca come impresa, come definito nella sezione 6.2.1.

11. Le linee guida riguardano sia i casi transfrontalieri sia quelli non transfrontalieri.

12. Le linee guida non sono esaustive, né forniscono spiegazioni sulle differenze tra i sistemi nazionali di diritto amministrativo, civile o penale nell'irrogazione di sanzioni amministrative in generale.

1.4 - Applicabilità

13. Ai sensi dell'articolo 70, paragrafo 1, lettera e), GDPR, l'EDPB ha la facoltà di pubblicare linee guida, raccomandazioni e migliori pratiche al fine di promuovere l'applicazione coerente del GDPR. L'articolo 70, paragrafo 1, lettera k), GDPR specifica che il Consiglio garantisce l'applicazione coerente del GDPR e, di propria iniziativa o, se del caso, su richiesta della Commissione Europea, in particolare, elabora per le autorità di controllo linee guida riguardanti l'applicazione delle misure di cui all'articolo 58 e la previsione delle sanzioni amministrative pecuniarie ai sensi dell'articolo 83.

14. Al fine di ottenere un approccio coerente all'irrogazione di sanzioni amministrative pecuniarie che rifletta adeguatamente tutti i principi del GDPR, l'EDPB ha concordato un'interpretazione comune dei criteri di valutazione di cui all'articolo 83, GDPR. Le singole autorità di controllo terranno conto di tale approccio comune, in conformità delle leggi amministrative e giudiziarie locali ad esse applicabili.

CAPITOLO 2 – METODOLOGIA PER IL CALCOLO DELL'IMPORTO DELLA SANZIONE PECUNIARIA

2.1 – Osservazioni generali

15. Nonostante gli obblighi di cooperazione e coerenza, il calcolo dell'importo della sanzione pecuniaria è a discrezione dell'autorità di controllo. Il GDPR dispone che l'importo della sanzione pecuniaria sia in ogni singolo caso effettivo, proporzionato e dissuasivo (articolo 83, paragrafo 1, GDPR). Inoltre, nel fissare l'importo della sanzione pecuniaria, le autorità di controllo tengono debito conto di una serie di circostanze che si riferiscono alle caratteristiche della violazione (la sua gravità) o al carattere del suo autore (articolo 83, paragrafo 2, GDPR). La quantificazione dell'importo della sanzione pecuniaria si basa quindi su una valutazione specifica effettuata per ciascun caso, tenendo conto dei parametri di cui al GDPR.

16. Per le condotte che violano le norme sulla protezione dei dati il GDPR non prevede una sanzione pecuniaria minima. All'articolo 83, paragrafi da 4 a 6, GDPR, sono invece previsti soltanto importi massimi e sono raggruppati diversi tipi di condotta. In definitiva una sanzione pecuniaria può essere calcolata solo valutando tutti i fattori espressamente identificati all'articolo 83, paragrafo 2, lettere da a) a j), GDPR pertinenti per il caso in questione e qualsiasi altro elemento pertinente, anche se non esplicitamente elencato in tali disposizioni (in quanto l'articolo 83, paragrafo 2, lettera k), GDPR dispone di tenere debito conto di eventuali altri fattori applicabili). Infine l'importo finale della sanzione pecuniaria risultante da tale valutazione deve essere in ogni singolo caso effettivo, proporzionato e dissuasivo (articolo 83, paragrafo 1, GDPR). Le sanzioni

pecuniarie irrogate devono tenere adeguatamente conto di tutti questi parametri, senza superare il limite massimo legale previsto all'articolo 83, paragrafi da 4 a 6, GDPR.

2.2 - Panoramica della metodologia

17. Tenendo conto tali parametri, l'EDPB ha elaborato la presente metodologia per il calcolo delle sanzioni amministrative pecuniarie da infliggere in caso di violazioni del GDPR.

Fase 1	Individuare le operazioni di trattamento nel caso in questione e valutare l'applicazione dell'articolo 83, paragrafo 3, GDPR. **(Capitolo 3)**
Fase 2	Trovare il punto di partenza per l'ulteriore calcolo basato sulla valutazione degli elementi seguenti **(Capitolo 4):** a) la classificazione di cui all'articolo 83, paragrafi da 4 a 6, GDPR; b) la gravità della violazione ai sensi dell'articolo 83, paragrafo 2, lettere a), b) e g), GDPR; c) il fatturato dell'impresa come elemento pertinente da prendere in considerazione al fine di infliggere una sanzione pecuniaria effettiva, dissuasiva e proporzionata, ai sensi dell'articolo 83, paragrafo 1, GDPR.
Fase 3	Valutare le circostanze aggravanti e attenuanti legate al comportamento passato o presente del titolare/responsabile del trattamento e aumentare o ridurre di conseguenza la sanzione pecuniaria. **(Capitolo 5)**
Fase 4	Individuare i pertinenti limiti massimi di legge per le diverse operazioni di trattamento. Gli aumenti applicati nelle fasi precedenti o successive non possono superare tale importo massimo. **(Capitolo 6)**
Fase 5	Analizzare se l'importo finale della sanzione pecuniaria calcolata risponde ai requisiti di effettività, dissuasività e proporzionalità, come disposto dall'articolo 83, paragrafo 1, GDPR, e aumentare o diminuire la sanzione pecuniaria di conseguenza. **(Capitolo 7)**

2.3 - Violazioni con importi fissi

18. In determinate circostanze l'autorità di controllo può ritenere che alcune violazioni possano essere punite con una sanzione pecuniaria di importo fisso e predeterminato. L'applicazione di un importo fisso a determinati tipi di violazioni non può impedire l'applicazione del GDPR, in particolare l'articolo 83. Inoltre l'applicazione di importi fissi non esonera le autorità di controllo dal rispetto della cooperazione e della coerenza (capo VII, GDPR).

19. Stabilire quali tipi di violazioni possano essere punite con un importo fisso predeterminato, in base alla loro natura, gravità e durata, è a discrezione dell'autorità di controllo. L'autorità di controllo non può decidere in tal senso se ciò è vietato o sarebbe in altro modo in conflitto con l'ordinamento nazionale dello Stato membro.

20. Gli importi fissi possono essere stabiliti a discrezione dell'autorità di controllo, tenendo conto - tra l'altro - delle circostanze sociali ed economiche dello Stato membro in questione, in relazione alla gravità della violazione secondo l'interpretazione di cui all'articolo 83, paragrafo 2, lettere a), b) e g), GDPR. Si raccomanda all'autorità di controllo di comunicare preventivamente gli importi e le circostanze di applicazione.

CAPITOLO 3 – CONCORSO DI VIOLAZIONI E APPLICAZIONE DELL'ARTICOLO 83, PARAGRAFO 3, GDPR

21. Prima di poter calcolare una sanzione pecuniaria secondo la metodologia esposta nelle presenti linee guida, è importante considerare innanzitutto su quali condotte (circostanze di fatto relative al comportamento) e violazioni (qualificazione giuridica astratta di ciò che è sanzionabile) si basa la sanzione pecuniaria. Un caso particolare potrebbe infatti includere circostanze che potrebbero essere considerate come un'unica e medesima condotta o come distinte condotte sanzionabili. Inoltre è possibile che da un'unica e medesima condotta scaturisca una serie di violazioni diverse: in questo caso l'imputazione di una violazione preclude l'imputazione di un'altra oppure le diverse violazioni possono essere imputate congiuntamente. In altre parole, possono verificarsi casi di concorso di violazioni. A seconda delle norme in materia di concorso, il calcolo delle sanzioni pecuniarie può variare.

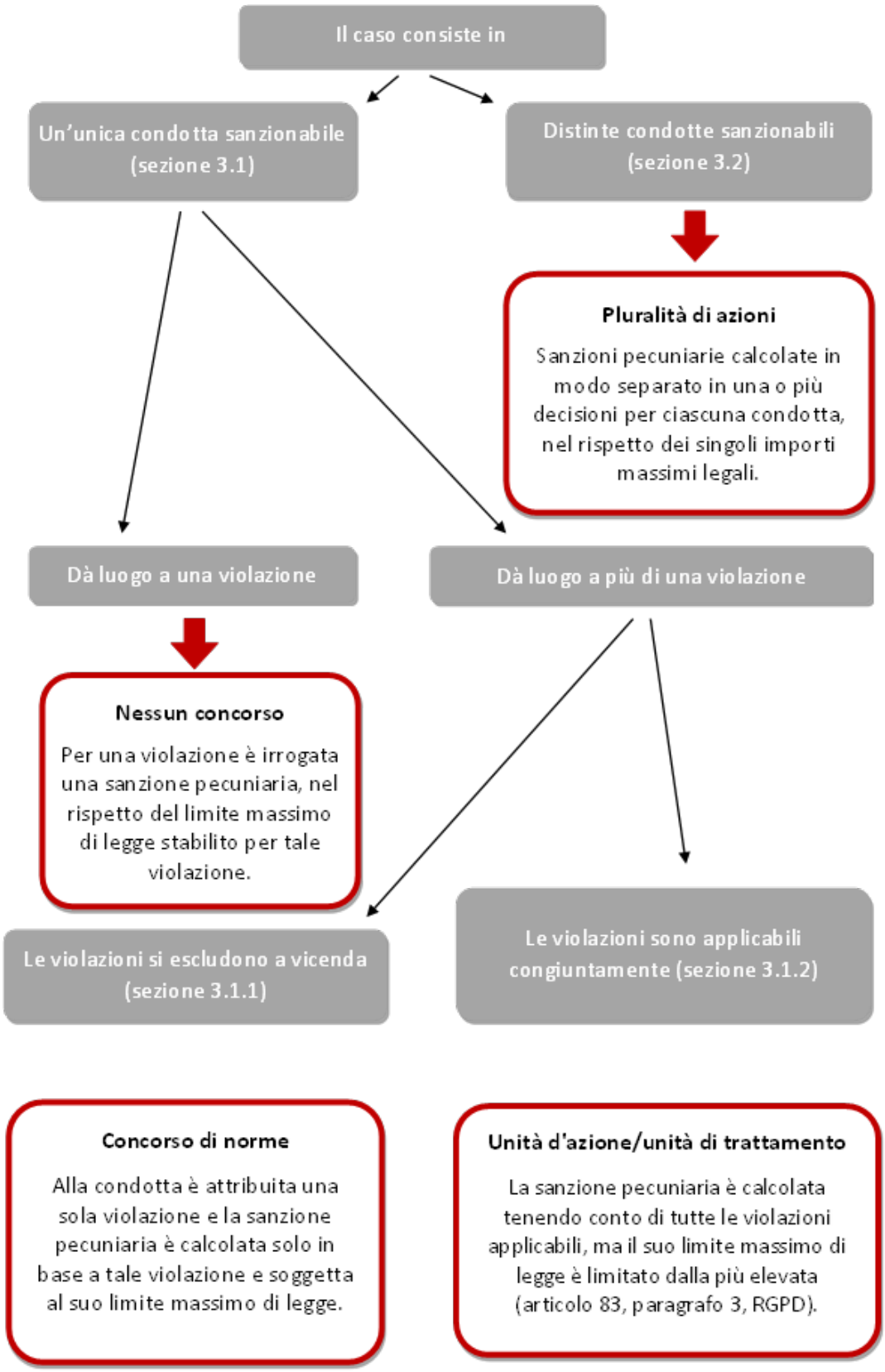
22. Esaminando l'analisi delle tradizioni degli Stati membri per quanto riguarda le norme in materia di concorso, secondo quanto delineato nella giurisprudenza della Corte di giustizia dell'UE (di seguito CGUE)[5], e considerando i diversi ambiti di applicazione e le conseguenze giuridiche, questi principi possono essere raggruppati approssimativamente nelle **tre categorie** seguenti:
    - **concorso di illeciti (sezione 3.1.1)**,
    - **unità d'azione (sezione 3.1.2),**
    - **pluralità di azioni (sezione 3.2).**

23. Queste diverse categorie di concorso non sono in conflitto tra loro, ma hanno ambiti di applicazione diversi e si inseriscono in un sistema complessivo coerente che fornisce un metodo di prova logico.

24. È quindi importante stabilire prima
    a. se le circostanze debbano essere considerate come un'unica condotta (**sezione 3.1**) o come molteplici condotte sanzionabili **(sezione 3.2**);
    b. nel caso si tratti di un'unica condotta **(sezione 3.1**), se questa condotta dia origine a una o a più violazioni; e
    c. nel caso di una condotta che dà origine a più violazioni, se l'imputazione di una violazione precluda l'imputazione di un'altra violazione **(sezione 3.1.1**) o se debbano essere attribuite congiuntamente (**sezione 3.1.2**).

[5] In particolare, si veda l'analisi approfondita contenuta nel parere dell'avvocato generale Tanchev nella causa C-10/18 P, *Marine Harvest*.

SCHEMA


Il caso consiste in
Un'unica condotta sanzionabile (sezione 3.1)
Distinte condotte sanzionabili (sezione 3.2)
Pluralità di azioni
Sanzioni pecuniarie calcolate in modo separato in una o più decisioni per ciascuna condotta, nel rispetto dei singoli importi massimi legali.
Dà luogo a una violazione
Dà luogo a più di una violazione
Nessun concorso
Per una violazione è irrogata una sanzione pecuniaria, nel rispetto del limite massimo di legge stabilito per tale violazione.
Le violazioni si escludono a vicenda (sezione 3.1.1)
Le violazioni sono applicabili congiuntamente (sezione 3.1.2)
Concorso di norme
Alla condotta è attribuita una sola violazione e la sanzione pecuniaria è calcolata solo in base a tale violazione e soggetta al suo limite massimo di legge.
Unità d'azione/unità di trattamento
La sanzione pecuniaria è calcolata tenendo conto di tutte le violazioni applicabili, ma il suo limite massimo di legge è limitato dalla più elevata (articolo 83, paragrafo 3, RGPD).

3.1 - Un'unica condotta sanzionabile

25. In primo luogo è essenziale stabilire se si tratta di un'unica e medesima condotta sanzionabile ("idem") o di una pluralità di condotte, al fine di individuare il comportamento pertinente da sanzionare. È quindi importante comprendere quali circostanze sono considerate come un'unica e medesima condotta rispetto a molteplici condotte. Il comportamento sanzionabile pertinente deve essere valutato e identificato caso per caso. Ad esempio, in certi casi, "lo stesso trattamento o trattamenti collegati" potrebbero costituire un'unica e medesima condotta.

26. Il termine "trattamento" figura all'articolo 4, punto 2, GDPR, nel quale "trattamento" è definito come "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione."

27. Nella valutazione in merito allo "stesso trattamento o trattamenti collegati" si dovrebbe tenere presente che le autorità di controllo, ai fini della valutazione delle violazioni, possono prendere in considerazione tutti gli obblighi giuridicamente necessari affinché le operazioni di trattamento siano svolte in modo lecito, compresi ad esempio gli obblighi di trasparenza (ad esempio, l'articolo 13, GDPR). Ciò è sottolineato anche dalla frase "per lo stesso trattamento o per trattamenti collegati", che indica che l'ambito di applicazione di questa disposizione comprende qualsiasi violazione che si riferisce e può avere un impatto sullo stesso trattamento o su trattamenti collegati.

28. Il termine "collegati" si riferisce al principio secondo cui una condotta unitaria può consistere in più azioni che sono poste in essere sulla base di una volontà unitaria e sono contestualmente (in particolare, per quanto riguarda l'identità in termini di interessato, finalità e natura), spazialmente e temporalmente correlate in modo così stretto da potere essere considerate, da un punto di vista oggettivo, come un'unica condotta coerente. L'esistenza di un collegamento sufficiente non dovrebbe essere presunta con facilità, al fine di evitare che l'autorità di controllo violi i principi di dissuasività e di effettiva applicazione della normativa europea. Pertanto gli aspetti delle relazioni che determinano un collegamento sufficiente devono essere valutati caso per caso.

Esempio 1a - Lo stesso trattamento o trattamenti collegati
Un istituto finanziario richiede una verifica del credito a un'agenzia di informazioni sul credito (CRA). L'istituto finanziario riceve tali informazioni e le conserva nel suo sistema.

Sebbene la raccolta e la conservazione dei dati sull'affidabilità creditizia da parte dell'istituto finanziario siano di per sé operazioni di trattamento, esse formano un insieme di operazioni di trattamento poste in essere sulla base di una volontà unitaria e sono contestualmente, spazialmente e temporalmente correlate in modo così stretto da essere considerati, da un punto di vista oggettivo, come un'unica condotta coerente. Pertanto i trattamenti compiuti dall'istituto finanziario sono da considerarsi "collegati" e costituiscono la medesima condotta.

Esempio 1b - Lo stesso trattamento o trattamenti collegati
Un intermediario di dati decide di attuare una nuova attività di trattamento nel modo seguente: decide di raccogliere - in qualità di terzo e senza disporre di una base giuridica - la cronologia delle transazioni dei consumatori da decine di dettaglianti, per eseguire analisi psicometriche e prevedere il comportamento

futuro delle persone, tra cui il comportamento di voto politico, l'intenzione di lasciare il proprio lavoro e altro ancora. Nell'ambito della stessa decisione, l'intermediario di dati decide di non includere tale procedura nei registri delle attività di trattamento, di non informare gli interessati e di ignorare le richieste di accesso degli interessati relative alle nuove operazioni di trattamento. Le operazioni di trattamento coinvolte in questa attività di trattamento formano un insieme di operazioni di trattamento poste in essere sulla base di una volontà unitaria e sono contestualmente, spazialmente e temporalmente correlate. Devono essere considerate come "collegate" e costitutive della medesima condotta. Lo stesso vale anche per quanto riguarda la mancata registrazione dell'attività di trattamento nei registri, la mancata informazione degli interessati e la mancata definizione di procedure per l'attuazione del diritto di accesso in relazione alle nuove operazioni di trattamento. Tali obblighi sono stati violati per trattamenti collegati.

Esempio 1c - Il trattamento non è lo stesso o i trattamenti non sono collegati
i) Un ente edilizio esegue un controllo dei precedenti personali di un candidato a un posto di lavoro. Il controllo dei precedenti personali include anche l'affinità politica, l'appartenenza a un sindacato e l'orientamento sessuale. ii) Cinque giorni dopo, l'ente edilizio rivolge ai propri fornitori (imprese individuali) una richiesta di divulgazione volontaria eccessiva di informazioni in merito ai loro rapporti commerciali con altri soggetti, indipendentemente dalla rilevanza per il contratto o dagli obblighi di conformità dell'ente edilizio autorità del settore edilizio. iii) Dopo un'altra settimana, l'ente edilizio subisce una violazione dei dati personali. Nonostante la presenza di misure tecniche e organizzative adeguate, la rete dell'ente edilizio viene violata e l'hacker ottiene l'accesso a un sistema di trattamento dei dati personali dei cittadini che hanno presentato richieste all'ente edilizio. Nonostante i dati fossero adeguatamente crittografati in linea con le norme applicabili, l'hacker è in grado di violarli con una tecnologia di decodifica militare e vende i dati nella rete oscura. L'ente edilizio si astiene dal notificare il fatto all'autorità di controllo, malgrado sia tenuto a farlo. Le operazioni di trattamento interessate in questo caso, vale a dire il controllo dei precedenti personali, le richieste di divulgazione volontaria da parte dei fornitori e la mancata notifica di una violazione dei dati personali, non sono contestualmente collegate. I trattamenti non devono essere quindi considerati "collegati" in quanto si configurano come condotte diverse.

29. Se si stabilisce che le circostanze del caso costituiscono un'unica e medesima condotta e danno origine a un'unica violazione, la sanzione pecuniaria può essere calcolata in base a tale violazione e al suo limite massimo di legge. Tuttavia se le circostanze del caso costituiscono un'unica e medesima condotta che però dà origine a più violazioni, occorre stabilire se l'imputazione di una violazione preclude l'imputazione di un'altra (sezione 3.1.1) o se le violazioni possono essere imputate congiuntamente (sezione 3.1.2). Se le circostanze del caso configurano molteplici condotte, queste devono essere considerate come una pluralità di azioni e gestite conformemente alla sezione 3.2.

3.1.1 - Concorso di illeciti

30. Il principio del concorso di illeciti (definito anche "concorso apparente" o "falso concorso"[6]) si applica ogniqualvolta l'applicazione di una disposizione preclude o sostituisce l'applicabilità dell'altra. In altre parole, il concorso si verifica già al livello astratto di disposizioni di legge. Tale situazione potrebbe configurarsi in base ai principi di specialità[7], sussidiarietà o consunzione, che spesso si applicano nel caso di norme che

[6] Cfr., ad esempio, il *Verwaltungsgerichtshof (tribunale amministrativo) austriaco, Ra* 2018/02/0123, punto 9.
[7] Come valutato nella causa C-10/18 P, *Marine Harvest contro Commissione*.

tutelano lo stesso interesse giuridico. In questi casi, sarebbe illegittimo sanzionare due volte il trasgressore per lo stesso illecito[8].

31. In questa fattispecie di concorso di illeciti, l'importo della sanzione pecuniaria dovrebbe essere calcolato solo sulla base della violazione selezionata conformemente ai principi di cui sopra ("violazione prevalente")[9].

Principio di specialità[10]

32. Il principio di specialità (*specialia generalibus derogant*) è un principio giuridico in base al quale una disposizione più specifica (derivata dallo stesso atto giuridico o da atti giuridici diversi aventi la stessa forza) prevale su una disposizione più generale, sebbene entrambe perseguano lo stesso scopo. La violazione più specifica è quindi talvolta considerata di "tipo qualificato" rispetto a quella meno specifica. Una fattispecie di violazione qualificata potrebbe essere soggetta a una sanzione pecuniaria di livello superiore, a un limite massimo di legge più elevato o a un termine di prescrizione più lungo.

33. Talvolta tuttavia, per via interpretativa, il principio di specialità è applicabile anche laddove, in ragione della sua natura e della sua sistematicità, una violazione è considerata una categoria di una violazione apparentemente più specifica, sebbene la sua formulazione in sé non menzioni esplicitamente un elemento aggiuntivo.

34. Il fatto invece che due disposizioni perseguono obiettivi autonomi costituisce un fattore di differenziazione che giustifica l'irrogazione di sanzioni pecuniarie distinte. Ad esempio, se la violazione di una disposizione comporta automaticamente la violazione di un'altra disposizione, ma non è vero il contrario, queste violazioni perseguono obiettivi autonomi.

35. Tali principi di specialità possono essere applicati solo se e nella misura in cui gli obiettivi perseguiti dalle violazioni in questione sono effettivamente congruenti nel singolo caso. Poiché i principi della protezione dei dati di cui all'articolo 5, GDPR sono definiti come concetti di carattere generale e trasversale, possono verificarsi situazioni in cui altre disposizioni siano una concretizzazione di tale principio, ma non lo abbraccino nella sua interezza. In altre parole, una disposizione non sempre definisce l'intera portata del principio[11]. Pertanto, a seconda delle circostanze[12], in alcuni casi esse si sovrappongono in modo congruente e una violazione potrebbe sostituire l'altra, mentre in altri casi la sovrapposizione è solo parziale e quindi non interamente congruente. Nella misura in cui le disposizioni non sono congruenti non vi è concorso di illeciti. Possono invece essere applicate congiuntamente nel calcolo della sanzione pecuniaria.

Principio di sussidiarietà

36. Un'altra forma con cui spesso si fa riferimento al concorso di illeciti è il principio di sussidiarietà. Tale principio si applica quando una violazione è considerata sussidiaria rispetto a un'altra. Ciò può verificarsi perché la

[8] Cfr., ad esempio, il *Verwaltungsgerichtshof austriaco,* Ra 2018/02/0123, punto 7.
[9] Come valutato nella causa C-10/18 P, *Marine Harvest contro Commissione*.
[10] Come valutato nella causa C-10/18 P, *Marine Harvest contro Commissione*.
[11] Decisione vincolante 1/2021 dell'EDPB relativa alla controversia sorta sul progetto di decisione dell'autorità di controllo irlandese concernente WhatsApp Ireland ai sensi dell'articolo 65, paragrafo 1, lettera a), GDPR (di seguito "decisione vincolante 1/2021 dell'EDPB"), paragrafo 192.
[12] Decisione vincolante 1/2021 dell'EDPB, paragrafo 193.

legge dichiara formalmente la sussidiarietà, o perché la sussidiarietà sussiste per motivi oggettivi [13]. Quest'ultimo caso può verificarsi quando le violazioni hanno lo stesso obiettivo, ma una contiene un'accusa di immoralità o di illecito meno grave (ad esempio, un illecito amministrativo può essere sussidiario rispetto a un illecito penale ecc.).

Principio di consunzione

37. Il principio di consunzione si applica nei casi in cui la violazione di una disposizione porta regolarmente alla violazione dell'altra, spesso perché una violazione costituisce la fase preliminare dell'altra.

3.1.2 - Unità di azione - Articolo 83, paragrafo 3, GDPR

38. Analogamente alla situazione del concorso di illeciti, il principio di unità di azione (definito anche "concorso ideale") riguarda i casi in cui un'unica condotta è contemplata da diverse disposizioni di legge, con la differenza che una disposizione non è né esclusa né assorbita dall'applicabilità dell'altra, in quanto non rientrano nell'ambito di applicazione dei principi di specialità, sussidiarietà o consunzione e perseguono per lo più obiettivi diversi.

39. Il principio di unità di azione è stato ulteriormente specificato a livello di diritto derivato all'articolo 83, paragrafo 3, GDPR, sotto forma di "unità di trattamento". È importante comprendere che l'articolo 83, paragrafo 3, GDPR è limitato nella sua applicazione e non si applicherà a ogni singolo caso in cui siano state accertate molteplici violazioni, ma solo ai casi in cui siano state commesse più violazioni in relazione allo "stesso trattamento o trattamenti collegati", come spiegato sopra[14]. In questi casi, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave[15].

40. In alcuni casi particolari, si potrebbe anche ipotizzare un'unità di azione quando una singola azione viola più volte la stessa disposizione di legge. Questa situazione potrebbe verificarsi, in particolare, quando le circostanze costituiscono una violazione iterativa e congenere della stessa disposizione di legge in una stretta successione spazio-temporale.

---

[13] L'idea di una sussidiarietà formale è inclusa indirettamente anche nell'articolo 35, paragrafo 2, della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 ("direttiva NIS 2"), sebbene il conflitto si risolva a livello procedurale piuttosto che materiale. La disposizione prevede che "qualora le autorità di controllo di cui all'articolo 55 o 56 del regolamento (UE) 2016/679 impongano una sanzione amministrativa pecuniaria a norma dell'articolo 58, paragrafo 2, lettera i), [GDPR], le autorità competenti non impongono una sanzione amministrativa pecuniaria a norma dell'articolo 34 della [direttiva NIS 2] per una violazione di cui al[l'articolo 35], paragrafo 1, della direttiva NIS 2, imputabile al medesimo comportamento punito con l'ammenda amministrativa pecuniaria a norma dell'articolo 58, paragrafo 2, lettera i), [GDPR]". Nella misura in cui la violazione di cui all'articolo 35, paragrafo 1, della direttiva NIS 2 è indirettamente considerata sussidiaria rispetto a una sanzione pecuniaria basata sul GDPR, quando questa riguarda la medesima condotta.

[14] Decisione vincolante 1/2021 dell'EDPB, paragrafo 320.

[15] L'articolo 83, paragrafo 3, GDPR recita per esteso: "Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave".

Esempio 2 - Unità di azione
Un titolare del trattamento invia a più riprese nel corso della giornata pacchetti di e-mail pubblicitarie a gruppi di interessati, senza disporre di un fondamento giuridico e quindi, con un'unica azione, viola più volte l'articolo 6, paragrafo 1, GDPR.

41. La formulazione dell'articolo 83, paragrafo 3, GDPR non sembra riguardare direttamente quest'ultimo caso di unità di azione, poiché non sono violate "varie disposizioni". Tuttavia qualora un trasgressore che, con un'unica azione, viola diverse disposizioni che perseguono obiettivi diversi fosse favorito rispetto a un trasgressore che, con la stessa azione, viola più volte la stessa disposizione che persegue lo stesso obiettivo, saremmo in presenza di una disparità di trattamento oltre che di un trattamento ingiusto. Per evitare l'incoerenza del principio giuridico e al fine di rispettare il diritto fondamentale alla parità di trattamento sancito nella Carta, in questi casi sarà applicato *mutatis mutandis* l'articolo 83, paragrafo 3, GDPR.

42. Nel caso di unità di azione, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. "Per quanto riguarda l'interpretazione dell'articolo 83, paragrafo 3, [GDPR], l'EDPB sottolinea che il principio dell'effetto utile impone a tutte le istituzioni di conferire piena efficacia ed effetto al diritto dell'Unione"[16]. A questo riguardo, l'articolo 83, paragrafo 3, GDPR non deve essere interpretato in modo tale che "non importerebbe se un [trasgressore] abbia commesso una o più violazioni [del GDPR] […] nella valutazione della sanzione pecuniaria"[17].

43. L'espressione "importo totale" implica che tutte le violazioni commesse devono essere prese in considerazione nella determinazione dell'importo della sanzione pecuniaria[18], e la formulazione "importo specificato per la violazione più grave" fa riferimento ai limiti massimi di legge delle sanzioni pecuniarie (ad esempio, l'articolo 83, paragrafi da 4 a 6, GDPR). Pertanto, "anche se la sanzione pecuniaria in sé non può superare il limite massimo di legge, l'autore della violazione deve comunque essere esplicitamente dichiarato colpevole di aver violato diverse disposizioni e tali violazioni devono essere prese in considerazione nella determinazione dell'importo della sanzione pecuniaria finale da irrogare"[19]. Sebbene ciò non pregiudichi il dovere dell'autorità di controllo che impone la sanzione pecuniaria di tenere conto della necessità che la sanzione pecuniaria sia proporzionata, le altre violazioni commesse non possono essere scartate, bensì devono essere prese in considerazione nel calcolo della sanzione pecuniaria.

3.2 - Molteplici condotte sanzionabili

44. Il principio della pluralità di azioni (chiamato anche "*Realkonkurrenz*", "concorso materiale di illeciti" o "concorso coincidente") descrive tutti i casi che non rientrano nei principi del concorso di illeciti (sezione 3.1.1) o nell'articolo 83, paragrafo 3, GDPR (sezione 3.1.2).

45. L'unico motivo per cui tali violazioni sono trattate nell'ambito di un'unica decisione è che sono giunte per caso all'attenzione dell'autorità di controllo nello stesso momento, senza che si tratti dello stesso trattamento o di trattamenti collegati ai sensi dell'articolo 83, paragrafo 3, GDPR. È stato pertanto accertato che l'autore della violazione ha violato diverse disposizioni di legge e, in base alla procedura nazionale, sono state irrogate sanzioni pecuniarie distinte, nell'ambito della stessa decisione di irrogazione di sanzioni pecuniarie o in decisioni distinte. Inoltre poiché l'articolo 83, paragrafo 3, GDPR non è applicabile, l'importo totale della sanzione amministrativa pecuniaria può superare l'importo specificato per la violazione più grave

[16] Decisione vincolante 1/2021 dell'EDPB, paragrafo 322.
[17] Ibidem, paragrafo 323.
[18] Ibidem, paragrafo 325.
[19] Ibidem, paragrafo 326.

(*argumentum a contrario*). I casi di pluralità di azioni non costituiscono motivo di privilegio nei confronti del trasgressore per quanto riguarda il calcolo della sanzione pecuniaria. Tuttavia ciò non pregiudica l'obbligo di rispettare comunque il principio generale di proporzionalità.

Esempio 3 - Pluralità di azioni
Dopo aver condotto un'ispezione sulla protezione dei dati presso i locali di un titolare del trattamento, l'autorità di controllo ha riscontrato che questi non aveva definito una procedura per la revisione e il miglioramento continuo della sicurezza del suo sito web, non aveva fornito le informazioni di cui all'articolo 13 ai dipendenti in merito al trattamento dei dati delle risorse umane e non aveva informato l'autorità di controllo di una recente violazione dei dati relativi ai suoi fornitori. Nessuna delle violazioni è esclusa o assorbita in virtù dei principi di specialità, di sussidiarietà o di consunzione. Inoltre non sono considerate come lo stesso trattamento o trattamenti collegati: non costituiscono un'unità di azione, bensì una pluralità di azioni. L'autorità di controllo riterrà pertanto che il titolare del trattamento abbia violato con condotte diverse gli articoli 13, 32 e 33, GDPR. Nella relativa decisione imporrà singole sanzioni pecuniarie per ciascun comportamento, senza che vi sia un unico limite massimo di legge applicabile al loro importo.

CAPITOLO 4 – PUNTO DI PARTENZA PER IL CALCOLO

46. L'EDPB ritiene che il calcolo delle sanzioni amministrative pecuniarie debba iniziare da un punto di partenza armonizzato[20]. Tale punto di partenza costituisce la base iniziale per l'ulteriore calcolo, in cui sono prese in considerazione e ponderate tutte le circostanze del caso, per giungere all'importo finale della sanzione pecuniaria da irrogare al titolare del trattamento o al responsabile del trattamento.

47. L'individuazione di punti di partenza armonizzati nelle presenti linee guida non pregiudica e non dovrebbe pregiudicare la facoltà delle autorità di controllo di valutare ciascun caso nel merito. La sanzione pecuniaria irrogata a un titolare/responsabile del trattamento può variare da qualsiasi importo fino al limite massimo di legge, purché la sanzione pecuniaria sia effettiva, dissuasiva e proporzionata. L'esistenza di un punto di partenza non impedisce all'autorità di controllo di ridurre o aumentare la sanzione pecuniaria (fino al suo massimo) se le circostanze del caso lo richiedono.

48. L'EDPB ritiene che tre elementi costituiscano il punto di partenza per l'ulteriore calcolo: la classificazione delle violazioni in base alla loro natura ai sensi dell'articolo 83, paragrafi da 4 a 6, GDPR, la gravità della violazione (come esposto nella sezione 4.2) e il fatturato dell'impresa come elemento pertinente da prendere in considerazione affinché la sanzione pecuniaria inflitta sia effettiva, dissuasiva e proporzionata, ai sensi dell'articolo 83, paragrafo 1, GDPR. Tali elementi sono descritti nelle sezioni 4.1, 4.2 e 4.3. di seguito.

[20] A condizione che le linee guida lascino un margine sufficiente per adattare una sanzione amministrativa pecuniaria alle circostanze del caso, la Corte di giustizia dell'UE generalmente accetta che i calcoli partano da una base iniziale astratta. In particolare nelle cause riunite C-189/02 P, C-202/02 P, da C-205/02 P a C-208/02 P e C-213/02 P, *Dansk Rørindustri*, ma anche più recentemente nella causa T-15/02, *BASF AG contro Commissione*, punti 120-121; 134, causa C-227/14 P, *LG Display Co. Ltd contro Commissione*, punto 53 e causa T-26/02, *Daiichi Pharmaceutical Co. Ltd contro Commissione*, punto 50.

4.1 - Classificazione delle violazioni ai sensi dell'articolo 83, paragrafi da 4 a 6, GDPR

49. Quasi tutti gli obblighi dei titolari del trattamento e dei responsabili del trattamento ai sensi del regolamento sono classificati in base alla loro natura nelle disposizioni dell'articolo 83, paragrafi da 4 a 6, GDPR[21]. Il GDPR prevede due categorie di violazioni: violazioni punibili ai sensi dell'articolo 83, paragrafo 4, GDPR, da un lato, e violazioni punibili ai sensi dell'articolo 83, paragrafi 5 e 6, GDPR, dall'altro. La prima categoria di violazioni è punibile con una sanzione pecuniaria massima di 10 milioni di EUR o del 2 % del fatturato annuo dell'impresa, se superiore, mentre la seconda è punibile con una sanzione pecuniaria massima di 20 milioni di EUR o del 4 % del fatturato annuo dell'impresa, se superiore.

50. Con questa distinzione, il legislatore ha fornito una prima indicazione della gravità della violazione in senso astratto. Quanto più grave è la violazione, tanto più elevata sarà la sanzione pecuniaria.

4.2 - Gravità della violazione in ogni singolo caso

51. Il GDPR impone all'autorità di controllo di tenere debito conto della natura, della gravità e della durata della violazione, tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito (articolo 83, paragrafo 2, lettera a), GDPR); il carattere doloso o colposo della violazione (articolo 83, paragrafo 2, lettera b), GDPR; e le categorie di dati personali interessate dalla violazione (articolo 83, paragrafo 2, lettera g), GDPR). Ai fini delle presenti linee guida, l'EDPB si riferisce a questi fattori come alla gravità della violazione.

52. L'autorità di controllo deve esaminare tali fattori alla luce delle circostanze del caso specifico e, sulla base di tale analisi, deve stabilire il livello di gravità come indicato nel paragrafo 60. A questo riguardo, l'autorità di controllo può anche considerare se i dati in questione siano direttamente identificabili. Sebbene nelle presenti linee guida siano esaminati singolarmente, in realtà questi fattori sono spesso interconnessi e devono essere considerati in relazione ai fatti del caso nel suo complesso.

4.2.1 - Natura, gravità e durata della violazione

53. L'articolo 83, paragrafo 2, lettera a), GDPR ha un ambito di applicazione ampio e impone all'autorità di controllo di effettuare un esame completo di tutti gli elementi che costituiscono la violazione e che sono utili per differenziarla da altre violazioni dello stesso tipo. Tale valutazione deve quindi considerare i fattori specifici seguenti:

a) la **natura della violazione**, valutata in base alle circostanze concrete del caso. In questo senso, l'analisi è più specifica rispetto alla classificazione astratta di cui all'articolo 83, paragrafi da 4 a 6, GDPR. L'autorità di controllo può valutare l'interesse che la disposizione violata intende proteggere e la posizione di tale disposizione nel quadro sulla protezione dei dati. Inoltre l'autorità di controllo può considerare in che misura la violazione abbia impedito l'effettiva applicazione della disposizione e il conseguimento dell'obiettivo che tale disposizione intendeva tutelare;

b) la **gravità della violazione**, valutata in base alle circostanze specifiche. Come indicato all'articolo 83, paragrafo 2, lettera a), GDPR, questo aspetto riguarda la natura del trattamento e "l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito" e fornirà un'indicazione della gravità della violazione;

[21] Cfr. a questo proposito anche le linee guida WP 253, pag. 9.

i. la **natura del trattamento**, compreso il contesto nel quale il trattamento è basato a livello funzionale (ad esempio, attività imprenditoriale, senza scopo di lucro, partito politico, ecc.) e tutte le caratteristiche del trattamento [22]. Quando la natura del trattamento comporta rischi più elevati, ad esempio quando lo scopo è quello di monitorare, valutare aspetti personali o prendere decisioni o misure con effetti negativi per gli interessati, a seconda del contesto del trattamento e del ruolo del titolare del trattamento o del responsabile del trattamento, l'autorità di controllo può valutare la possibilità di attribuire un peso maggiore a questo fattore. L'autorità di controllo può inoltre attribuire un peso maggiore a tale fattore qualora esista un evidente squilibrio tra gli interessati e il titolare del trattamento (ad esempio, quando gli interessati sono dipendenti, alunni o pazienti) o qualora il trattamento riguardi interessati vulnerabili, in particolare minori,

ii. l'**oggetto del trattamento**, con riferimento al carattere locale, nazionale o transfrontaliero del trattamento effettuato e alla relazione tra tali informazioni e la portata effettiva del trattamento in termini di assegnazione delle risorse da parte del titolare del trattamento. Questo elemento evidenzia un fattore di rischio reale, legato alla maggiore difficoltà per l'interessato e l'autorità di controllo di limitare condotte illecite con l'estendersi dell'oggetto del trattamento. Quanto più ampio è l'oggetto del trattamento, tanto maggiore è il peso che l'autorità di controllo può attribuire a questo fattore;

iii. la **finalità del trattamento** porterà l'autorità di controllo ad attribuire maggior peso a questo fattore. L'autorità di controllo può anche valutare se il trattamento dei dati personali rientra nelle cosiddette attività principali del titolare del trattamento. Quanto più il trattamento è centrale rispetto alle attività principali del titolare del trattamento o del responsabile del trattamento, tanto più gravi saranno le irregolarità in tale trattamento. In tali circostanze, l'autorità di controllo può attribuire un peso maggiore a questo fattore. Tuttavia possono esserci circostanze nelle quali il trattamento dei dati personali pur discostandosi maggiormente dalle attività principali del titolare o del responsabile del trattamento, incide comunque in modo significativo sulla valutazione (è il caso, ad esempio, del trattamento dei dati personali dei lavoratori, nel quale la violazione incide in modo significativo sulla loro dignità);

iv. il **numero di interessati** concretamente ma anche potenzialmente coinvolti. Quanto più elevato è il numero di interessati coinvolti, tanto maggiore è il peso che l'autorità di controllo può attribuire a questo fattore. In molti casi, si può anche ritenere che la violazione assuma connotazioni "sistemiche" e possa quindi riguardare, anche in tempi diversi, ulteriori interessati che non hanno presentato reclami o segnalazioni all'autorità di controllo. L'autorità di controllo può, a seconda delle circostanze del caso, considerare il rapporto tra il numero di interessati coinvolti e il numero totale di interessati in quel

[22] A titolo di esempio, analizzando l'elemento relativo alla "natura della violazione", nella sua decisione 01/2020 relativa alla controversia sorta sul progetto di decisione dell'autorità di controllo irlandese concernente Twitter International Company ai sensi dell'articolo 65, paragrafo 1, lettera a), GDPR (di seguito, "decisione vincolante dell'EDPB 01/2020"), l'EDPB ha osservato che il "trattamento in questione" riguardava comunicazioni di interessati che avevano deliberatamente scelto di limitare il pubblico di tali comunicazioni, e ha raccomandato di tenere conto di tale aspetto nel valutare la natura del trattamento. In questo contesto, si veda anche la decisione vincolante dell'EDPB 01/2020, paragrafo 186.

contesto (ad esempio, il numero di cittadini, clienti o dipendenti), al fine di valutare se la violazione è di natura sistemica;

v. il **livello del danno** subito e la misura in cui la condotta può ledere i diritti e le libertà individuali. Il riferimento al "livello" del danno subito intende pertanto richiamare l'attenzione delle autorità di controllo sul danno subito, o che potrebbe essere stato subito, come ulteriore parametro distinto rispetto al numero di interessati coinvolti (ad esempio, nei casi in cui il numero di persone interessate dal trattamento illecito è elevato, ma il danno da loro subito è marginale). In base al considerando 75 GDPR, il livello del danno subito si riferisce al danno fisico, materiale o immateriale. La valutazione del danno, in ogni caso, deve essere limitata a quanto è funzionalmente necessario per ottenere una corretta valutazione del livello di gravità della violazione, come indicato nel paragrafo 60 che segue, senza sovrapporsi alle attività delle autorità giudiziarie incaricate di accertare le diverse forme di pregiudizio individuale;

c) la **durata della violazione**, nel senso che un'autorità di controllo può generalmente attribuire un peso maggiore a una violazione di durata maggiore. Quanto più lunga è la durata della violazione, tanto maggiore è il peso che l'autorità di controllo può attribuire a questo fattore. Nel rispetto dell'ordinamento nazionale, se una determinata condotta era illecita anche nel quadro normativo precedente, nel quantificare la sanzione pecuniaria è possibile prendere in considerazione sia il periodo successivo alla data di decorrenza degli effetti del GDPR sia il periodo precedente, tenendo conto delle condizioni di tale quadro.

54. L'autorità di controllo può attribuire un peso ai fattori di cui sopra, a seconda delle circostanze del caso. Se non sono di particolare rilevanza, tali fattori possono anche essere considerati ininfluenti.

4.2.2 - Il carattere doloso o colposo della violazione

55. Nei suoi precedenti orientamenti, l'EDPB ha affermato che "In generale, il 'dolo' comprende sia la consapevolezza che l'intenzionalità in relazione alle caratteristiche di un reato, mentre per 'colposo' si intende che non vi era l'intenzione di causare la violazione nonostante il titolare/responsabile del trattamento abbia violato l'obbligo di diligenza previsto per legge"[23]. Colposo in questo senso non equivale a non volontario.

Esempio 4 - Esempi illustrativi di dolo e negligenza (dalle WP 253)[24]
"Tra le circostanze indicanti il carattere doloso di una violazione figura il trattamento illecito autorizzato esplicitamente dall'alta dirigenza del titolare del trattamento oppure effettuato nonostante i pareri del responsabile della protezione dei dati o ignorando le politiche esistenti, ad esempio ottenendo e trattando dati relativi ai dipendenti di un concorrente con l'intento di screditare tale concorrente sul mercato. Altri esempi sono:

- *modifica di dati personali per dare un'impressione fuorviante (positiva) circa il conseguimento degli obiettivi – episodio riscontrato nel contesto degli obiettivi relativi ai tempi d'attesa ospedalieri;*
- *scambio di dati personali con finalità di marketing, ossia vendita di dati come "approvati" senza verificare/ignorando il parere degli interessati circa le modalità di utilizzo dei propri dati.*

Altre circostanze, quali mancata lettura e non rispetto delle politiche esistenti, errore umano, mancata verifica dei dati personali nelle informazioni pubblicate, incapacità di apportare aggiornamenti tecnici in

[23] Linee guida WP 253, pag. 11.
[24] Esempi citati direttamente dalle linee guida WP 253, pag. 12.

maniera puntuale, mancata adozione delle politiche (piuttosto che la semplice mancata applicazione) possono essere sintomo di negligenza";

56. Il carattere doloso o colposo della violazione (articolo 83, paragrafo 2, lettera b), GDPR) deve essere valutato tenendo conto degli elementi oggettivi di condotta rilevati dalle circostanze del caso. L'EDPB ha evidenziato che è generalmente riconosciuto che le violazioni dolose "da cui emerge il disprezzo per le disposizioni di legge, sono più gravi di quelle colpose"[25]. In caso di violazione dolosa, è probabile che l'autorità di controllo attribuisca maggior peso a questo fattore. A seconda delle circostanze del caso, l'autorità di controllo può anche attribuire importanza al grado di colpa. Nel migliore dei casi, la colpa potrebbe essere considerata ininfluente.

4.2.3 - Categorie di dati personali interessate

57. Per quanto riguarda la prescrizione di tener conto delle categorie di dati personali interessate dalla violazione (articolo 83, paragrafo 2, lettera g), GDPR), il GDPR evidenzia chiaramente i tipi di dati che meritano una protezione speciale e quindi una risposta più severa in termini di sanzioni pecuniarie. Ciò riguarda, come minimo, i tipi di dati di cui agli articoli 9 e 10, GDPR, e i dati che non rientrano nell'ambito di applicazione di tali articoli la cui diffusione causa immediati danni o disagi all'interessato[26] (ad esempio, i dati sull'ubicazione, i dati sulle comunicazioni private, i numeri d'identificazione nazionale, o i dati finanziari, come i riepiloghi delle transazioni o i numeri delle carte di credito)[27]. In generale, quante più sono le categorie di dati coinvolte o quanto più sono sensibili i dati, tanto maggiore è il peso che l'autorità di controllo può attribuire a questo fattore.

58. È inoltre rilevante la quantità di dati relativi a ciascun interessato, considerando che la violazione del diritto alla privacy e alla protezione dei dati personali si aggrava in funzione della quantità di dati relativi a ciascun interessato.

4.2.4 - Classificazione della gravità della violazione e individuazione dell'importo iniziale adeguato

59. La valutazione dei fattori di cui sopra (sezioni 4.2.1-4.2.3) determina la gravità della violazione nel suo complesso. Tale valutazione non è un calcolo matematico in cui i fattori sopra elencati sono considerati singolarmente, bensì una valutazione approfondita delle circostanze concrete del caso, in cui tutti i fattori sopra citati sono interconnessi. Pertanto nel valutare la gravità della violazione occorre considerare la violazione nel suo complesso.

60. In base alla valutazione dei fattori sopra descritti, il livello di gravità della violazione è considerato i) basso, ii) medio o iii) elevato. Queste categorie lasciano impregiudicata la questione se possa essere inflitta o meno una sanzione pecuniaria.

- Nel calcolare la sanzione amministrativa pecuniaria per le violazioni con un **livello di gravità basso**, l'autorità di controllo determinerà l'importo iniziale per l'ulteriore calcolo ad un livello compreso tra lo 0 e il 10 % del limite massimo di legge applicabile.

[25] Linee guida WP 253, pag. 12.
[26] Ibidem, pag. 14.
[27] La diffusione di comunicazioni private e di dati relativi all'ubicazione può causare immediati danni o disagi all'interessato, aspetto che è stato evidenziato dalla protezione speciale concessa dal legislatore dell'UE alle comunicazioni private nell'articolo 7 della Carta dei diritti fondamentali e nella direttiva 2002/58/CE e dalla CGUE per i dati relativi all'ubicazione in determinati casi, si vedano le cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net et al*, punto 117 e la giurisprudenza ivi citata.

- Nel calcolare la sanzione amministrativa pecuniaria per le violazioni con un **livello di gravità medio**, l'autorità di controllo determinerà l'importo iniziale per l'ulteriore calcolo ad un livello compreso tra il 10 e il 20 % del limite massimo di legge applicabile.

- Nel calcolare la sanzione amministrativa pecuniaria per le violazioni con un **livello di gravità elevato**, l'autorità di controllo determinerà l'importo iniziale per l'ulteriore calcolo ad un livello compreso tra il 20 e il 100 % del limite massimo di legge applicabile.

61. Di norma, quanto più grave è la violazione all'interno della propria categoria, tanto più alto sarà probabilmente l'importo iniziale.

62. Gli intervalli all'interno dei quali è determinato l'importo iniziale rimangono soggetti a revisione da parte dell'EDPB e dei suoi membri e possono essere adeguati se necessario.

Esempio 5a - Classificazione della gravità di una violazione (livello di gravità elevato)
Dopo aver indagato su numerosi reclami relativi a chiamate indesiderate presentati da clienti di una compagnia telefonica, l'autorità di controllo competente ha riscontrato che la compagnia telefonica aveva utilizzato i recapiti dei suoi clienti per scopi di marketing telefonico senza una valida base giuridica (violazione dell'articolo 6 GDPR). In particolare, la compagnia telefonica aveva offerto a terzi i nomi e i numeri di telefono registrati dei suoi clienti per scopi di marketing. La compagnia telefonica lo ha fatto nonostante il parere contrario del responsabile della protezione dei dati, non ha preso alcun provvedimento per frenare questa pratica né ha offerto ai clienti alcuna modalità di opposizione. In realtà, la pratica andava avanti da maggio 2018 ed era ancora in corso al momento dell'indagine. La compagnia telefonica in questione operava a livello nazionale e la pratica riguardava tutti i suoi 4 milioni di clienti. L'autorità di controllo ha riscontrato che tutti questi clienti sono stati regolarmente sottoposti a chiamate indesiderate da parte di terzi, senza alcun mezzo efficace per porvi fine.

*L'autorità di controllo è stata incaricata di valutare la gravità del caso. Come punto di partenza, l'autorità di controllo ha rilevato che una violazione dell'articolo 6 GDPR è **elencata tra le violazioni dell'articolo 83, paragrafo 5, GDPR**, e quindi rientra nel livello superiore dell'articolo 83 GDPR. In secondo luogo, l'autorità di controllo ha valutato le circostanze del caso. A questo riguardo, l'autorità di controllo ha attribuito un peso significativo alla **natura della violazione**, in quanto la disposizione violata (articolo 6 GDPR) è alla base della liceità del trattamento dei dati nel suo complesso. L'inosservanza di questa disposizione annulla la liceità del trattamento nel suo insieme. Inoltre l'autorità di controllo ha attribuito un peso significativo alla **durata della violazione**, che è iniziata con l'entrata in vigore del GDPR e non era cessata al momento dell'indagine. Il fatto che la compagnia telefonica operasse a livello nazionale ha aumentato il peso dell''**oggetto del trattamento**. Il **numero di interessati** coinvolti è stato considerato molto elevato (4 milioni, a fronte di una popolazione totale di 14 milioni di persone), mentre **il livello del danno** subito è stato considerato moderato (danno immateriale, sotto forma di fastidio). Quest'ultima valutazione è stata effettuata tenendo conto delle **categorie di dati interessati** (nome e numero di telefono). La gravità della violazione è stata tuttavia accresciuta dal fatto che la violazione è stata commessa ignorando un parere del responsabile della protezione dei dati e, pertanto, è stata considerata **dolosa**.*

*Tenendo conto di quanto precede (natura grave, lunga durata, elevato numero di interessati, portata nazionale, natura dolosa, rispetto al danno moderato), l'autorità di controllo ha concluso che il **livello di gravità** della violazione debba essere considerato **elevato**. L'autorità di controllo determinerà*

l'importo iniziale per l'ulteriore calcolo ad un livello compreso tra il 20 e il 100 % del limite massimo di legge previsto all'articolo 83, paragrafo 5, GDPR.

Esempio 5b - Classificazione della gravità di una violazione (livello di gravità medio)
Un'autorità di controllo ha ricevuto da un ospedale una notifica di violazione dei dati personali. Da tale notifica è emerso che diversi membri del personale hanno potuto visualizzare parti di cartelle cliniche di pazienti a cui, in base al reparto di appartenenza, non avrebbero dovuto avere accesso. L'ospedale aveva lavorato alle procedure per regolare l'accesso alle cartelle cliniche dei pazienti e aveva attuato misure rigorose per l'accesso riservato. Il personale di un reparto poteva quindi accedere solo alle informazioni mediche relative a quel reparto specifico. Inoltre l'ospedale aveva investito nella sensibilizzazione del personale alla privacy. Tuttavia, come è emerso, si erano verificati problemi riguardo al controllo delle autorizzazioni. I membri del personale che si trasferivano da un reparto all'altro erano ancora in grado di accedere alle cartelle cliniche dei loro "vecchi" reparti e l'ospedale non disponeva di procedure per abbinare la posizione attuale dei membri del personale con la rispettiva autorizzazione. Un'indagine interna dell'ospedale ha dimostrato che almeno 150 membri del personale (su 3 500) avevano autorizzazioni inesatte, che riguardavano almeno 20 000 delle 95 000 cartelle cliniche dei pazienti. L'ospedale ha potuto dimostrare che in almeno 16 casi i membri del personale avevano utilizzato le loro autorizzazioni per visualizzare cartelle cliniche dei pazienti. L'autorità di controllo ha ritenuto che vi sia stata una violazione dell'articolo 32, GDPR.

Nel valutare la gravità del caso, l'autorità di controllo ha rilevato innanzitutto che una violazione dell'articolo 32 GDPR è ***elencata tra le violazioni dell'articolo 83, paragrafo 4, GDPR,*** *e rientra quindi nel livello inferiore dell'articolo 83, GDPR. In secondo luogo, l'autorità di controllo ha valutato le circostanze del caso. A questo riguardo, l'autorità di controllo ha ritenuto che, sebbene il* ***numero di interessati danneggiati*** *dalla violazione sia stato solo di 16, potenzialmente avrebbe potuto essere di 20 000 nelle circostanze del caso e addirittura di 95 000, data la natura sistemica del problema. Inoltre l'autorità di controllo ha classificato la violazione come* ***colposa****, ma con un livello di gravità basso, il che è stato considerato un fattore neutro nelle circostanze di questo caso particolare, in quanto l'ospedale non ha adottato politiche di autorizzazione laddove avrebbe sicuramente dovuto farlo, ma ha comunque adottato misure rigorose per limitare l'accesso. Questa valutazione non è stata influenzata dal fatto che altre politiche di protezione e sicurezza dei dati erano state attuate con successo, come disposto dal GDPR. Infine l'autorità di controllo ha attribuito un peso significativo al fatto che le cartelle cliniche dei pazienti contengono dati sanitari, che sono* ***categorie particolari di dati*** *ai sensi dell'articolo 9 GDPR.*

Tenendo conto di tutto quanto sopra (natura del trattamento e categorie particolari di dati rispetto al numero di interessati coinvolti effettivamente e potenzialmente), l'autorità di controllo ha concluso che il ***livello di gravità*** *della violazione debba essere considerato* ***medio****. L'autorità di controllo determinerà l'importo iniziale per l'ulteriore calcolo ad un livello compreso tra il 10 e il 20 % del limite massimo di legge previsto all'articolo 83, paragrafo 4, GDPR.*

Esempio 5c - Classificazione della gravità di una violazione (livello di gravità basso)
Un'autorità di controllo ha ricevuto numerosi reclami sul modo in cui un negozio online gestisce il diritto di accesso degli interessati. Secondo i denuncianti, la gestione delle loro richieste di accesso ha richiesto tra i quattro e i sei mesi, un lasso di tempo che supera i tempi consentiti dal GDPR. L'autorità di controllo esamina i reclami e scopre che il negozio online risponde alle richieste di accesso con un ritardo massimo di tre mesi nel 5 % dei casi. In totale, il negozio riceveva circa 1 000 richieste di accesso annualmente e ha confermato che 950 di queste erano gestite in tempo. Inoltre

il negozio online disponeva di politiche per garantire che tutte le richieste di accesso fossero gestite in modo corretto e completo. Tuttavia l'autorità di controllo ha concluso che il negozio online ha violato l'articolo 12, paragrafo 3, GDPR, e ha deciso di irrogare una sanzione pecuniaria.

Nell'ambito del calcolo dell'importo della sanzione pecuniaria da irrogare, l'autorità di controllo è stata incaricata di valutare la gravità del caso. Come punto di partenza, l'autorità di controllo ha rilevato che una violazione dell'articolo 12 GDPR è ***elencata tra le violazioni dell'articolo 83, paragrafo 5, GDPR*** *, e quindi rientra nel livello superiore dell'articolo 83 GDPR. In secondo luogo, l'autorità di controllo ha valutato le circostanze del caso. A questo riguardo, l'autorità di controllo ha analizzato attentamente la* ***natura della violazione****. Sebbene il diritto di accesso tempestivo ai dati personali sia un elemento cardine dei diritti degli interessati, l'autorità di controllo ha ritenuto che la violazione fosse di gravità limitata a questo riguardo, dal momento che, alla fine, tutte le richieste erano state gestite e con un ritardo limitato. Nel considerare la* ***finalità del trattamento****, l'autorità di controllo ha riscontrato che il trattamento dei dati personali non era l'attività principale del negozio online, ma era comunque un'importante attività accessoria per conseguire l'obiettivo di vendere prodotti online. L'autorità di controllo ha ritenuto che questo elemento aumentasse la gravità della violazione. D'altra parte, il* ***livello del danno*** *subito dagli interessati è stato considerato minimo, in quanto tutte le richieste di accesso erano state gestite entro sei mesi.*

Tenendo conto di tutto quanto sopra (natura della violazione, finalità del trattamento e livello del danno), l'autorità di controllo ha concluso che il ***livello di gravità*** *della violazione debba essere considerato* ***basso****. L'autorità di controllo determinerà l'importo iniziale per l'ulteriore calcolo ad un livello compreso tra il 0 e il 10 % del limite massimo di legge previsto all'articolo 83, paragrafo 5, GDPR.*

4.3 - Fatturato dell'impresa al fine di irrogare una sanzione pecuniaria effettiva, dissuasiva e proporzionata

63. A norma del GDPR, ogni autorità di controllo è tenuta a provvedere affinché le sanzioni amministrative inflitte siano in ogni singolo caso effettive, proporzionate e dissuasive (articolo 83, paragrafo 1, GDPR). L'applicazione di questi principi del diritto dell'Unione europea può avere conseguenze di ampia portata nei singoli casi, poiché i punti di partenza che il GDPR offre per il calcolo delle sanzioni amministrative pecuniarie si applicano sia alle microimprese sia alle multinazionali. Al fine di infliggere sanzioni che siano in tutti i casi effettive, proporzionate e dissuasive, le autorità di controllo dovrebbero adeguare le sanzioni pecuniarie amministrative all'interno dell'intero intervallo disponibile fino al limite massimo di legge. Di conseguenza, l'importo della sanzione pecuniaria può aumentare o diminuire significativamente, a seconda delle circostanze del caso.

64. L'EDPB ritiene che sia giusto che i punti di partenza individuati di seguito riflettano una distinzione delle dimensioni dell'impresa e quindi prende in considerazione il fatturato [28]. L'EDPB segue le prescrizioni dell'articolo 83 GDPR, il GDPR nel suo complesso e la giurisprudenza consolidata della CGUE secondo cui il fatturato di un'impresa può costituire un'indicazione delle dimensioni e del potere economico della

[28] Cfr. anche la decisione vincolante 1/2021 dell'EDPB, paragrafi 411 e 412: "[Nella misura in cui] il fatturato di un'impresa non sia rilevante esclusivamente ai fini della determinazione dell'importo massimo della sanzione pecuniaria a norma dell'articolo 83, paragrafi da 4 a 6, GDPR, ma possa essere preso in considerazione anche ai fini del calcolo della sanzione stessa, se del caso, al fine di garantire che essa sia effettiva, proporzionata e dissuasiva ai sensi dell'articolo 83, paragrafo 1, GDPR". Il fatturato dell'impresa interessata è ulteriormente approfondito nella sezione 6.2 delle presenti linee guida.

medesima[29]. Tuttavia ciò non esime l'autorità di controllo dalla responsabilità di effettuare una revisione dell'effettività, della dissuasività e della proporzionalità al termine del calcolo (cfr. capitolo 7). Tale revisione riguarda tutte le circostanze del caso, incluso ad esempio l'accumulo di violazioni multiple, gli aumenti e le riduzioni per le circostanze aggravanti e attenuanti e le circostanze finanziarie/socio-economiche. Tuttavia spetta all'autorità di controllo garantire che le stesse circostanze non siano conteggiate due volte. In particolare, le autorità di controllo non dovrebbero, ai sensi del capitolo 7, ripetere gli aumenti o le riduzioni rispetto al fatturato dell'azienda, bensì dovrebbero rivedere la loro valutazione dell'adeguatezza dell'importo iniziale.

65. Per le ragioni sopra descritte, l'autorità di controllo può prendere in considerazione la possibilità di adeguare l'importo iniziale corrispondente alla gravità della violazione nei casi in cui tale violazione sia commessa da un'impresa con un fatturato annuo non superiore a 2 milioni di EUR, un fatturato annuo non superiore a 10 milioni di EUR o un fatturato annuo non superiore a 50 milioni di EUR[30].

- **Per le imprese con un fatturato annuo ≤ 2 milioni di EUR**, le autorità di controllo possono valutare di procedere ai calcoli sulla base di un importo compreso tra lo 0,2 % e lo 0,4 % dell'importo iniziale individuato.

- **Per le imprese con un fatturato annuo compreso tra 2 milioni di EUR e 10 milioni di EUR**, le autorità di controllo possono valutare di procedere ai calcoli sulla base di un importo compreso tra lo 0,3 % e il 2 % dell'importo iniziale individuato.

- **Per le imprese con un fatturato annuo compreso tra 10 milioni di EUR e 50 milioni di EUR**, le autorità di controllo possono valutare di procedere ai calcoli sulla base di un importo compreso tra l'1,5 % e il 10 % dell'importo iniziale individuato.

66. Per gli stessi motivi, l'autorità di controllo può prendere in considerazione la possibilità di adeguare l'importo iniziale corrispondente alla gravità della violazione nei casi in cui tale violazione sia commessa da un'impresa con un fatturato annuo non superiore a 100 milioni di EUR, un fatturato annuo non superiore a 250 milioni di EUR e un fatturato annuo non superiore a 500 milioni di EUR[31].

- Per **le imprese con un fatturato annuo compreso tra 50 milioni di EUR e 100 milioni di EUR**, le autorità di controllo possono valutare di procedere ai calcoli sulla base di un importo compreso tra l'8 % e il 20 % dell'importo iniziale individuato.

- Per **le imprese con un fatturato annuo compreso tra 100 milioni di EUR e 250 milioni di EUR**, le autorità di controllo possono valutare di procedere ai calcoli sulla base di un importo compreso tra il 15 % e il 50 % dell'importo iniziale individuato.

[29] Secondo quando affermato dal Tribunale nella causa T-25/06, *Alliance One International, Inc. contro Commissione europea*, punto 211, facendo riferimento ad altra giurisprudenza, ad esempio la causa T-9/99, *HFB e altri contro Commissione*, punti 528 e 529, e la causa T-175/05, *Akzo Nobel e altri contro Commissione,* punto 114.

[30] Queste cifre relative al fatturato si ispirano alla raccomandazione della Commissione del 6 maggio 2003 concernente la definizione di microimprese, piccole e medie imprese. Per determinare i punti di partenza, l'EDPB si basa sul solo fatturato annuo dell'impresa (cfr. il capitolo 6 che segue).

[31] Tali cifre sono aggiunte per colmare il divario tra la soglia più alta del paragrafo precedente e la soglia di fatturato individuata all'articolo 83, paragrafi da 4 a 6, GDPR.

- Per **le imprese con un fatturato annuo compreso tra 250 milioni di EUR e 500 milioni di EUR**, le autorità di controllo possono valutare di procedere ai calcoli sulla base di un importo compreso tra il 40 % e il 100 % dell'importo iniziale individuato.

- Per le imprese **con un fatturato annuo superiore a 500 milioni di EUR,** le autorità di controllo possono prendere in considerazione la possibilità di procedere senza un adeguamento dell'importo iniziale individuato. In effetti, tali imprese supereranno il limite massimo di legge statico e, quindi, la dimensione dell'impresa si riflette già nel limite massimo di legge dinamico utilizzato per determinare l'importo iniziale per l'ulteriore calcolo basato sulla valutazione della gravità della violazione.

67. Di norma, quanto maggiore è il fatturato dell'impresa all'interno del suo livello applicabile, tanto più alto sarà probabilmente l'importo iniziale. Quest'ultimo aspetto è particolarmente vero per le imprese più grandi, per le quali la categoria degli importi iniziali ha l'intervallo più ampio.

68. Inoltre l'autorità di controllo non ha l'obbligo di applicare tale adeguamento se dal punto di vista dell'effettività, della capacità dissuasiva e della proporzionalità non è necessario adeguare l'importo iniziale della sanzione pecuniaria.

69. Occorre ribadire che tali cifre sono i punti di partenza per l'ulteriore calcolo, e non importi fissi (cartellini dei prezzi) per le violazioni delle disposizioni del GDPR. L'autorità di controllo può, a sua discrezione, utilizzare l'intero intervallo per la sanzione pecuniaria, a partire da qualsiasi importo fino al limite massimo di legge, facendo in modo che la sanzione pecuniaria sia adattata alle circostanze del caso, come richiesto dalla Corte di giustizia nel caso in cui sia utilizzata una base iniziale astratta.

Esempio 6a - Individuazione della base iniziale per l'ulteriore calcolo
Una catena di supermercati con un fatturato di 450 milioni di EUR ha violato l'articolo 12 GDPR. L'autorità di controllo, sulla base di un'attenta analisi delle circostanze del caso, ha deciso che il ***livello di gravità*** *della violazione è* ***basso****. Per determinare il punto di partenza per l'ulteriore calcolo, l'autorità di controllo accerta innanzitutto che l'articolo 12 GDPR sia elencato nell'articolo 83, paragrafo 5, lettera b), GDPR e che, in base al fatturato dell'impresa (450 milioni di EUR), si applichi il limite massimo di legge di 20 milioni di EUR.*

In base al livello di gravità determinato dall'autorità di controllo (basso), si dovrebbe prendere in considerazione un importo iniziale compreso tra 0 e 2 milioni di EUR (tra lo 0 e il 10 % del limite massimo di legge applicabile, cfr. il paragrafo 60 che precede).

L'autorità di controllo ritiene che un adeguamento al 90 % dell'importo iniziale sia giustificato in base alle dimensioni dell'impresa, il cui fatturato ammonta a 450 milioni di EUR. Tale importo costituisce la base per l'ulteriore calcolo, che dovrebbe portare a un importo finale non superiore al limite massimo di legge applicabile di 20 milioni di EUR.

Esempio 6b - Individuazione della base iniziale per l'ulteriore calcolo
Si scopre che una start-up di una app di incontri con un fatturato di 500 000 EUR ha venduto dati personali sensibili dei suoi clienti a diversi intermediari di dati a scopi di analisi, violando così gli articoli 9 e 5, paragrafo 1, lettera a), GDPR. L'autorità di controllo, sulla base di un'attenta analisi delle circostanze del caso, ha deciso che il ***livello di gravità*** *della violazione è* ***elevato****. Per determinare il punto di partenza per l'ulteriore calcolo, l'autorità di controllo si accerta innanzitutto*

che gli articoli 9 e 5, GDPR, siano elencati nell'articolo 83, paragrafo 5, lettera a), GDPR e che, in base al fatturato dell'impresa (500 000 EUR), si applichi il limite massimo di legge di 20 milioni di EUR.

In base al livello di gravità determinato dall'autorità di controllo (elevato), si dovrebbe prendere in considerazione un importo iniziale compreso tra 4 e 20 milioni di EUR (tra il 20 % e il 100 % del limite massimo di legge applicabile, cfr. il paragrafo 60 che precede).

L'autorità di controllo ritiene che un adeguamento al ribasso fino allo 0,25 % dell'importo iniziale sia giustificato in base alle dimensioni dell'impresa, che ha un fatturato di 500 000 EUR. Tale importo costituisce la base per l'ulteriore calcolo, che dovrebbe portare a un importo finale non superiore al limite massimo applicabile di 20 milioni di EUR.

CAPITOLO 5 – CIRCOSTANZE AGGRAVANTI E ATTENUANTI

5.1 - Individuazione dei fattori aggravanti e attenuanti

70. In base alla struttura del GDPR, dopo aver valutato la natura, la gravità e la durata della violazione, nonché il carattere doloso o colposo della medesima e le categorie di dati personali interessate, l'autorità di controllo deve prendere in considerazione i restanti fattori aggravanti e attenuanti elencati nell'articolo 83, paragrafo 2, GDPR.

71. Per quanto riguarda la valutazione di questi elementi, gli aumenti o le riduzioni di una sanzione pecuniaria non possono essere predeterminati mediante tabelle o percentuali. Si ribadisce che l'effettiva quantificazione della sanzione pecuniaria dipenderà da tutti gli elementi raccolti nel corso dell'indagine e da ulteriori considerazioni legate anche alle precedenti esperienze sanzionatorie dell'autorità di controllo.

72. Per chiarezza, occorre notare che ogni criterio dell'articolo 83, paragrafo 2, GDPR - che sia valutato ai sensi del capitolo 4 o del presente capitolo - deve essere preso in considerazione una sola volta nell'ambito della valutazione complessiva dell'articolo 83, paragrafo 2, GDPR.

5.2 - Le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati

73. Un primo passo per determinare se si sono verificate circostanze aggravanti o attenuanti, è quello di esaminare l'articolo 83, paragrafo 2, lettera c), che riguarda "le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati".

74. Come ricordato nelle linee guida WP253, i titolari del trattamento e i responsabili del trattamento dei dati hanno già l'obbligo di "attuare misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, di condurre valutazioni di impatto sulla protezione dei dati e di mitigare i rischi arrecati ai diritti e alle libertà personali dal trattamento dei dati personali". Tuttavia, in caso di violazione, il titolare del trattamento o il responsabile del trattamento dovrebbe "fare quanto in suo potere per ridurre le conseguenze della violazione per il o i soggetti coinvolti"[32].

75. L'adozione di misure adeguate per attenuare il danno subito dagli interessati può essere considerata un fattore attenuante che riduce l'importo della sanzione pecuniaria.

[32] Linee guida WP 253, pag. 12.

76. Le misure adottate devono essere valutate, in particolare, per quanto riguarda l'elemento della tempestività, ossia il momento in cui sono attuate dal titolare del trattamento o dal responsabile del trattamento, e la loro efficacia. In questo senso, è più probabile che siano considerate un fattore attenuante le misure attuate spontaneamente prima della presa di conoscenza da parte del titolare del trattamento o del responsabile del trattamento dell'avvio dell'indagine dell'autorità di controllo, rispetto alle misure attuate successivamente.

5.3 - Grado di responsabilità del titolare del trattamento o del responsabile del trattamento

77. In base all'articolo 83, paragrafo 2, lettera d), si dovrà valutare il grado di responsabilità del titolare del trattamento o del responsabile del trattamento, tenendo conto delle misure da essi messe in atto ai sensi degli articoli 25 e 32 GDPR. Conformemente alle linee guida WP 253, "[l]a domanda cui l'autorità di controllo deve quindi rispondere è la seguente: in che misura il titolare del trattamento ha fatto quanto ci si aspettava facesse, considerando la natura, le finalità o l'entità del trattamento, alla luce degli obblighi imposti dal regolamento?"[33].

78. In particolare, per quanto riguarda questo criterio, devono essere valutati il rischio residuo per le libertà e i diritti degli interessati, il danno causato agli interessati e il danno che persiste dopo l'adozione delle misure da parte del titolare del trattamento, nonché il grado di solidità delle misure adottate ai sensi degli articoli 25 e 32 GDPR.

79. A questo riguardo, l'autorità di controllo può anche considerare se i dati in questione siano direttamente identificabili e/o disponibili senza protezione tecnica[34]. Tuttavia occorre tenere presente che l'esistenza di tale protezione non costituisce necessariamente un fattore attenuante (cfr. il paragrafo 82); dipende dalle circostanze del caso.

80. Per valutare adeguatamente gli elementi di cui sopra, l'autorità di controllo deve prendere in considerazione qualsiasi documentazione pertinente fornita dal titolare del trattamento o dal responsabile del trattamento, ad esempio nel contesto dell'esercizio del diritto di difesa. In particolare, tale documentazione potrebbe fornire prove di quando sono state adottate le misure e di come sono state attuate, se il titolare del trattamento e il responsabile del trattamento hanno interagito (se applicabile), o se ci sono stati contatti con il responsabile della protezione dei dati o con gli interessati (se applicabile).

81. Dato il maggiore livello di responsabilità previsto dal GDPR rispetto alla direttiva 95/46/CE[35], è probabile che il livello di responsabilità del titolare del trattamento o del responsabile del trattamento sia considerato un fattore aggravante o neutro. Solo in circostanze eccezionali, quando il titolare del trattamento o il responsabile del trattamento è andato oltre gli obblighi che gli sono stati imposti, questo sarà considerato un fattore attenuante.

5.4 - Precedenti violazioni commesse dal titolare del trattamento o dal responsabile del trattamento

82. Le precedenti violazioni sono violazioni già accertate prima dell'emissione della decisione. In caso di cooperazione ai sensi del capo VII GDPR, le precedenti violazioni sono quelle già accertate prima dell'emissione del progetto di decisione (ai sensi dell'articolo 60, GDPR).

[33] Ibidem, pag. 13.
[34] Ibidem, pagg. 14 e 15.
[35] Ibidem, pag. 13.

83. Ai sensi dell'articolo 83, paragrafo 2, lettera e), GDPR, al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa si deve tenere conto di eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento. Una formulazione analoga si trova nel considerando 148 GDPR.

5.4.1 - Tempistica

84. In primo luogo, occorre considerare il momento in cui si è verificata la violazione precedente, considerando che più lungo è il tempo che intercorre tra una violazione precedente e quella attualmente oggetto di indagine, minore è l'importanza della violazione. Di conseguenza, quanto più tempo è trascorso da quando è stata commessa la violazione, tanto minore sarà l'importanza attribuitale dalle autorità di controllo. Tale valutazione è lasciata a discrezione dell'autorità di controllo, nel rispetto delle leggi e dei principi nazionali ed europei applicabili.

85. Tuttavia poiché le violazioni commesse molto tempo prima potrebbero essere ancora interessanti per valutare i "precedenti" del titolare del trattamento o del responsabile del trattamento, non devono essere stabiliti termini di estinzione fissi a tal fine. Ad ogni modo, alcune leggi nazionali impediscono all'autorità di controllo di prendere in considerazione le violazioni precedenti dopo un periodo di tempo stabilito. Analogamente alcune leggi nazionali impongono un obbligo di cancellazione dei provvedimenti iscritti dopo un certo periodo di tempo, il che impedisce alle autorità di controllo competenti di prendere in considerazione tali precedenti.

86. Per lo stesso motivo, è opportuno notare che le violazioni del GDPR, essendo più recenti, devono essere considerate più pertinenti rispetto alle violazioni delle disposizioni nazionali adottate per l'attuazione della direttiva 95/46/CE (se le leggi nazionali consentono che tali violazioni siano prese in considerazione dall'autorità di controllo).

5.4.2 - Oggetto

87. Ai fini dell'articolo 83, paragrafo 2, lettera e), GDPR, potrebbero essere considerate "pertinenti" le precedenti violazioni aventi oggetto uguale o diverso da quello sottoposto a indagine.

88. Sebbene tutte le violazioni precedenti possano fornire un'indicazione sull'atteggiamento generale del titolare del trattamento o del responsabile del trattamento nei confronti dell'osservanza del GDPR, le violazioni aventi lo stesso oggetto devono essere considerate più importanti, in quanto più vicine alla violazione attualmente oggetto di indagine, soprattutto quando il titolare del trattamento o il responsabile del trattamento ha commesso in precedenza la stessa violazione (violazioni ripetute). Pertanto, le violazioni aventi lo stesso oggetto devono essere considerate più pertinenti rispetto alle violazioni precedenti riguardanti una diversa materia.

89. Ad esempio, il fatto che il titolare del trattamento o il responsabile del trattamento non sia riuscito in passato a rispondere tempestivamente agli interessati che esercitavano i loro diritti, deve essere considerato più pertinente quando la violazione oggetto di indagine si riferisce anche alla mancanza di risposta a un interessato che esercita i propri diritti, rispetto a quando si riferisce a una violazione dei dati personali.

90. Occorre tuttavia tenere in debita considerazione le violazioni precedenti aventi oggetto diverso, ma commesse con le stesse modalità, in quanto potrebbero essere indicative di problemi persistenti all'interno dell'organizzazione del titolare del trattamento o del responsabile del trattamento. Ad esempio, questo

sarebbe il caso di violazioni derivanti dall'aver ignorato il parere espresso dal responsabile della protezione dei dati.

5.4.3 - Altre considerazioni

91. Se si considera una precedente violazione delle disposizioni nazionali adottate per l'attuazione della direttiva 95/46/CE, le autorità di controllo devono considerare il fatto che le prescrizioni della direttiva e del GDPR potrebbero essere diverse (se le leggi nazionali consentono che tali violazioni siano prese in considerazione dall'autorità di controllo).

92. Nel considerare la pertinenza di una precedente violazione, l'autorità di controllo deve tenere conto dello stato della procedura in cui è stata accertata la precedente violazione - in particolare di eventuali misure adottate dall'autorità di controllo o dall'autorità giudiziaria - in conformità della legge nazionale.

93. Le violazioni precedenti possono essere prese in considerazione anche quando sono state accertate da un'altra autorità di controllo in relazione allo stesso titolare del trattamento o responsabile del trattamento. Ad esempio, l'autorità di controllo capofila che si occupa di una violazione mediante il meccanismo di cooperazione (sportello unico) ai sensi dell'articolo 60 GDPR potrebbe prendere in considerazione le violazioni precedentemente accertate in casi locali da un'altra autorità di controllo, riguardanti lo stesso titolare/responsabile del trattamento. Analogamente, le violazioni precedentemente accertate dall'autorità di controllo capofila potrebbero essere prese in considerazione qualora una diversa autorità debba gestire un reclamo a essa proposto nei casi il cui impatto è solo locale, ai sensi dell'articolo 56, paragrafo 2, GDPR. Nel caso in cui non esista un'autorità di controllo capofila (ad esempio, nel caso in cui il titolare del trattamento o il responsabile del trattamento non sia stabilito nell'Unione europea), le autorità di controllo potrebbero anche prendere in considerazione le violazioni precedentemente accertate da un'altra autorità di controllo in relazione allo stesso titolare/responsabile del trattamento.

94. L'esistenza di violazioni precedenti può essere considerata un fattore aggravante nel calcolo della sanzione pecuniaria. Il peso attribuito a questo fattore deve essere determinato in base alla natura e alla frequenza delle violazioni precedenti. L'assenza di violazioni precedenti, tuttavia, non può essere considerata un fattore attenuante, in quanto la conformità al GDPR è la norma. Se non vi sono violazioni precedenti, questo fattore può essere considerato neutro.

5.5 - Il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi

95. L'articolo 83, paragrafo 2, lettera f) prevede che l'autorità di controllo tenga conto del grado di cooperazione del titolare del trattamento o del responsabile del trattamento con l'autorità di controllo, al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi.

96. Prima di passare ad esaminare il livello di cooperazione che il titolare del trattamento o il responsabile del trattamento ha instaurato con l'autorità di controllo, occorre ribadire che sul titolare del trattamento o sul responsabile del trattamento grava un obbligo generale di cooperazione ai sensi dell'articolo 31 GDPR e che la mancanza di cooperazione può comportare l'applicazione della sanzione pecuniaria prevista dall'articolo 83, paragrafo 4, lettera a), GDPR. È pertanto opportuno tenere conto del fatto che l'obbligo ordinario di cooperazione è obbligatorio e quindi dovrebbe essere considerato un fattore neutro (e non attenuante).

97. Tuttavia se la cooperazione con l'autorità di controllo ha limitato o evitato le ripercussioni negative sui diritti delle persone che si sarebbero altrimenti potute verificare, l'autorità di controllo può considerarla un fattore attenuante ai sensi dell'articolo 83, paragrafo 2, lettera f), GDPR, riducendo così l'importo della sanzione pecuniaria. Ciò può ad esempio avvenire quando un titolare del trattamento o un responsabile del trattamento "ha risposto in modo particolare alle richieste dell'autorità di controllo durante la fase di indagine nel caso specifico limitando in tal modo in maniera significativa le ripercussioni sulle persone"[36].

5.6 - La maniera in cui l'autorità di controllo ha preso conoscenza della violazione

98. In base all'articolo 83, paragrafo 2, lettera h), la maniera in cui la l'autorità di controllo ha preso conoscenza della violazione potrebbe essere un fattore – aggravante o attenuante – pertinente. Nel valutare questo aspetto, può essere particolarmente rilevante chiedersi se, e in caso affermativo, in che misura il titolare del trattamento o il responsabile del trattamento abbia notificato la violazione di propria iniziativa, prima che l'autorità di controllo ne venisse a conoscenza tramite - ad esempio - un reclamo o un'indagine. Tale circostanza non è rilevante se il titolare del trattamento è soggetto a specifici obblighi di notifica (come nel caso di violazioni di dati personali ai sensi dell'articolo 33)[37]. In questi casi, la notifica deve essere considerata un fattore neutro[38].

99. Nel caso in cui l'autorità di controllo sia venuta a conoscenza della violazione ad esempio tramite un reclamo o un'indagine, anche questo elemento dovrebbe essere considerato, di norma, neutro. L'autorità di controllo può considerare tale circostanza attenuante se il titolare del trattamento o il responsabile del trattamento ha notificato la violazione di propria iniziativa, prima che l'autorità di controllo prendesse conoscenza del caso.

5.7 - Rispetto dei provvedimenti disposti in precedenza in relazione allo stesso oggetto

100. L'articolo 83, paragrafo 2, lettera i), GDPR stabilisce che "qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti" deve essere preso in considerazione al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa.

101. A differenza dell'articolo 83, paragrafo 2, lettera e), GDPR, questa valutazione si riferisce solo ai provvedimenti che le stesse autorità di controllo hanno disposto in precedenza nei confronti dello stesso titolare del trattamento o responsabile del trattamento in relazione allo stesso oggetto[39].

102. A questo proposito, il titolare del trattamento o il responsabile del trattamento potrebbe avere la ragionevole aspettativa che il rispetto dei provvedimenti precedentemente disposti nei suoi confronti impedisca che in futuro si verifichi una violazione avente lo stesso oggetto. Tuttavia poiché la conformità ai provvedimenti precedentemente disposti è obbligatoria per il titolare del trattamento o il responsabile del trattamento, non deve essere presa in considerazione come fattore attenuante di per sé. Per contro, affinché questo fattore

[36] Linee guida WP 253, pag. 14.
[37] È opportuno sottolineare che una violazione dei dati personali non implica necessariamente una violazione del GDPR.
[38] Sottolineato dalle linee guida WP 253, pag. 15.
[39] Ibidem.

sia applicato come attenuante, occorre un impegno rafforzato da parte del titolare del trattamento o del responsabile del trattamento nell'adempimento dei provvedimenti precedenti, ad esempio l'adozione di ulteriori provvedimenti rispetto a quelli disposti dall'autorità di controllo.

103. Viceversa, l'inosservanza di un potere correttivo precedentemente disposto può essere considerata sia come un fattore aggravante, sia come una violazione diversa in sé, ai sensi dell'articolo 83, paragrafo 5, lettera e), e dell'articolo 83, paragrafo 6, GDPR. Occorre pertanto tenere presente che lo stesso comportamento non conforme non può portare a una situazione in cui è punito due volte.

5.8 - Adesione ai codici di condotta approvati o ai meccanismi di certificazione approvati

104. L'articolo 83, paragrafo 2, lettera j), GDPR stabilisce che l'adesione a codici di condotta ai sensi dell'articolo 40 GDPR o a meccanismi di certificazione approvati ai sensi dell'articolo 42 GDPR può essere un fattore pertinente.

105. Come ricordato dalle linee guida WP 253, l'adesione a codici di condotta ai sensi dell'articolo 40 GDPR o a meccanismi di certificazione approvati ai sensi dell'articolo 42 GDPR può costituire in alcune circostanze un fattore attenuante. I codici di condotta approvati conterranno, ai sensi dell'articolo 40, paragrafo 4, GDPR, "i meccanismi che consentono all'organismo [di controllo] di effettuare il controllo obbligatorio del rispetto delle norme del codice". Alcune forme di sanzionamento dei comportamenti non conformi possono essere applicate tramite il regime di monitoraggio, ai sensi dell'articolo 41, paragrafo 4, GDPR, compresa la sospensione o l'esclusione del titolare del trattamento o del responsabile del trattamento interessato dalla comunità incaricata di gestire il codice. Sebbene l'autorità di controllo possa prendere in considerazione le sanzioni precedentemente inflitte relative al regime di autoregolamentazione, ai sensi dell'articolo 41, paragrafo 4, GDPR, i poteri dell'organismo di controllo si espletano "fatti salvi i compiti e i poteri dell'autorità di controllo competente", il che significa che l'autorità di controllo non ha l'obbligo di tenere conto delle sanzioni imposte dall'organismo di controllo[40].

106. D'altra parte, se il mancato rispetto dei codici di condotta o della certificazione ha pertinenza diretta con la violazione, l'autorità di controllo può considerarlo una circostanza aggravante.

5.9 - Altre circostanze aggravanti e attenuanti

107. L'articolo 83, paragrafo 2, lettera k), GDPR lascia all'autorità di controllo la possibilità di tenere conto di eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso. Nel singolo caso possono entrare in gioco molti elementi, che non possono essere tutti codificati o elencati e di cui si dovrà tenere conto affinché la sanzione pecuniaria applicata sia in ogni singolo caso effettiva, proporzionata e dissuasiva.

108. L'articolo 83, paragrafo 2, lettera k), GDPR cita esempi di "eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso" ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione". Si ritiene che tale disposizione sia di fondamentale importanza per adeguare l'importo della sanzione pecuniaria al caso specifico. In questo senso, si ritiene che debba essere interpretata come un esempio del principio di equità e giustizia applicato al singolo caso.

[40] Ibidem.

109. L'ambito di applicazione di questa disposizione, che è necessariamente aperto, dovrebbe includere tutte le considerazioni motivate relative al contesto socio-economico in cui opera il titolare del trattamento o il responsabile del trattamento, quelle relative al contesto giuridico e quelle relative al contesto di mercato[41].

110. In particolare, il guadagno economico derivante dalla violazione potrebbe essere una circostanza aggravante se il caso fornisce informazioni relative ai profitti tratti dalla violazione del GDPR.

111. Potrebbero essere considerate ai sensi dell'articolo 83, paragrafo 2, lettera k), GDPR anche circostanze eccezionali che possono determinare cambiamenti significativi nel contesto socio-economico (ad esempio, l'insorgere di una grave emergenza pandemica che potrebbe cambiare radicalmente il modo in cui viene effettuato il trattamento dei dati personali).

N.B.: gli esempi riportati nel presente capitolo illustrano l'effetto che le circostanze aggravanti e attenuanti possono avere sull'importo della sanzione pecuniaria. Gli aumenti o le riduzioni menzionati in questi casi immaginari non possono essere considerati precedenti o indicazioni di percentuali da utilizzare in casi reali.

Esempio 7a - Valutazione delle circostanze aggravanti e attenuanti
Un club sportivo ha fatto uso di telecamere con tecnologia di riconoscimento facciale collocate all'entrata di una delle sue sedi, allo scopo di identificare i clienti al momento dell'ingresso. Poiché la società sportiva ha violato l'articolo 9 GDPR (trattamento dei dati biometrici senza una valida deroga), l'autorità di controllo competente a indagare sulla violazione ha deciso di infliggere una sanzione pecuniaria. Tenendo conto di tutte le circostanze pertinenti del caso, l'autorità di controllo ha ritenuto che si trattasse di una violazione con un livello di gravità elevato e, poiché la società sportiva aveva un fatturato annuo di 150 milioni di EUR, è stato ritenuto appropriato un importo iniziale di 2 000 000 EUR (corrispondente al limite massimo della categoria).

Tuttavia lo stesso club sportivo era stato sanzionato due anni prima per aver utilizzato la tecnologia delle impronte digitali ai tornelli in un'altra sede. L'autorità di controllo ha deciso di tenerne conto come recidiva (articolo 83, paragrafo 2, lettera e), GDPR). A tale riguardo, ha attribuito importanza al fatto che si trattava quasi dello stesso oggetto e che la violazione era stata commessa solo due anni prima. Per effetto di questo fattore aggravante, l'autorità di controllo ha deciso di aumentare la sanzione pecuniaria, portandola in questo caso particolare a 2 600 000 EUR[42], senza superare il limite massimo di legge applicabile di 20 milioni di EUR.

N.B.: gli esempi riportati nel presente capitolo illustrano l'effetto che le circostanze aggravanti e attenuanti possono avere sull'importo della sanzione pecuniaria. Gli aumenti o le riduzioni menzionati in questi casi immaginari non possono essere considerati precedenti o indicazioni di percentuali da utilizzare in casi reali.

[41] L'EDPB ha deliberato in merito a questa questione nella decisione vincolante EDPB 3/2022 relativa alla controversia presentata dall'autorità di controllo irlandese su Meta Platforms Ireland Limited e il relativo Servizio Facebook (articolo 65 GDPR) (di seguito "decisione vincolante EDPB 3/2022"), punto 368.

[42] Ciò dimostra che le categorie ai fini degli importi iniziali non limitano le capacità delle autorità di controllo di tenere conto di circostanze aggravanti e attenuanti per determinare un importo superiore o inferiore alle categorie. Come ribadito nella sezione 4.3., tali cifre sono i punti di partenza per l'ulteriore calcolo, e non importi fissi (cartellini dei prezzi) per le violazioni delle disposizioni del GDPR. L'autorità di controllo può, a sua discrezione, utilizzare l'intero intervallo per la sanzione pecuniaria, a partire da qualsiasi importo superiore a 0 EUR fino al limite massimo di legge, facendo in modo che la sanzione pecuniaria sia adattata alle circostanze del caso.

Esempio 7b - Valutazione delle circostanze aggravanti e attenuanti
L'operatore di una piattaforma di noleggio auto a breve termine ha subito una violazione dei dati che ha reso vulnerabili i dati personali dei suoi clienti per un breve periodo di tempo. Tenendo conto di tutte le circostanze pertinenti del caso, l'autorità di controllo ha ritenuto che le carenze dell'operatore nella messa in sicurezza della sua piattaforma violassero l'articolo 32 GDPR e che si trattasse di una violazione con un livello di gravità basso; poiché inoltre il fatturato annuo dell'operatore ammontava a 255 milioni di EUR, è stato ritenuto appropriato un importo iniziale di 260 000 EUR.

I dati personali compromessi includevano copie di patenti di guida e documenti d'identità. Per questo motivo, tutti i clienti che hanno subito la violazione dei dati sono stati costretti a richiedere nuovamente tali documenti per limitare la possibilità di furto di identità. Nell'informare gli interessati di questo incidente, l'operatore ha offerto a tutti assistenza per richiedere nuovamente i documenti in questione presso le opportune istituzioni pubbliche e ha creato un sistema per rimborsare le eventuali tasse pagate. L'autorità di controllo ha considerato tali provvedimenti come "misure […] per attenuare il danno subito dagli interessati" (articolo 83, paragrafo 2, lettera c), GDPR), che hanno avuto un effetto attenuante sulla sanzione pecuniaria. Dato l'atteggiamento proattivo e l'efficacia dei provvedimenti adottati dall'operatore, l'autorità di controllo ha deciso di ridurre la multa a 225 000 EUR, senza superare[43], anche in questo caso, il limite massimo di legge di 10 milioni di EUR.

Gli esempi riportati nel presente capitolo illustrano l'effetto che le circostanze aggravanti e attenuanti possono avere sull'importo della sanzione pecuniaria. Gli aumenti o le riduzioni menzionati in questi casi immaginari non possono essere considerati precedenti o indicazioni di percentuali da utilizzare in casi reali.

Esempio 7c - Valutazione delle circostanze aggravanti e attenuanti
Una piccola agenzia di rating del credito è stata giudicata colpevole di aver violato diverse disposizioni a tutela dei diritti degli interessati, in particolare perché ha addebitato ai suoi clienti una tassa per l'esercizio del diritto di accesso. L'agenzia lo ha fatto per tutte le richieste di accesso, non solo per quelle menzionate all'articolo 12, paragrafo 5, lettera a), GDPR. Tenendo conto di tutte le circostanze pertinenti del caso, l'autorità di controllo ha ritenuto elevato il livello di gravità delle violazioni e, poiché il fatturato annuo dell'agenzia ammontava a 35 milioni di EUR, ha ritenuto appropriato un importo iniziale di 100 000 EUR.

Tuttavia l'autorità di controllo ha ritenuto che il fatto che l'agenzia fosse stata in grado di trarre profitto dalla violazione fosse una circostanza aggravante (articolo 83, paragrafo 2, lettera k), GDPR). Al fine di controbilanciare i guadagni derivanti dalla violazione mantenendo, al contempo, una sanzione pecuniaria effettiva, dissuasiva e proporzionata, in questo caso l'autorità di controllo ha deciso di aumentare la sanzione pecuniaria a 130 000 EUR, senza superare il limite massimo di legge di 20 milioni di EUR.

Gli esempi riportati nel presente capitolo illustrano l'effetto che le circostanze aggravanti e attenuanti possono avere sull'importo della sanzione pecuniaria. Gli aumenti o le riduzioni menzionati in questi casi immaginari non possono essere considerati precedenti o indicazioni di percentuali da utilizzare in casi reali.

[43] Cfr. la nota precedente.

Esempio 7d - Valutazione delle circostanze aggravanti e attenuanti
Un'impresa è risultata aver violato le disposizioni del GDPR, in particolare per aver venduto a suoi partner, a fini di prospezione commerciale, la propria banca dati contenente dati personali relativi a persone che non avevano prestato il loro consenso alla prospezione a fini commerciali.

Considerando tutte le circostanze pertinenti del caso, l'autorità di controllo ha ritenuto medio il livello di gravità delle violazioni e, poiché il fatturato annuo dell'impresa ammontava a 45 milioni di EUR, ha ritenuto appropriato un importo iniziale di 150 000 EUR.

Inoltre l'autorità ha ritenuto che si trattasse di una violazione che ha avvantaggiato il titolare del trattamento, perché il fatto di non aver raccolto il consenso delle persone per la trasmissione dei loro dati ai fini dell'invio di pubblicità mirata ha aumentato la massa di dati che ha potuto rivendere in seguito. L'autorità di controllo ha ritenuto quindi che il fatto che l'agenzia fosse stata in grado di trarre profitto dalla violazione fosse una circostanza aggravante (articolo 83, paragrafo 2, lettera k), GDPR).

Al fine di controbilanciare i guadagni derivanti dalla violazione mantenendo, al contempo, una sanzione pecuniaria effettiva, dissuasiva e proporzionata, in questo caso l'autorità di controllo ha deciso di aumentare la sanzione pecuniaria a 200 000 EUR senza superare il limite massimo di legge di 20 milioni di EUR.

CAPITOLO 6 – LIMITE MASSIMO DI LEGGE E RESPONSABILITÀ DELLE IMPRESE

6.1 - Determinazione del limite massimo di legge

112. Come già evidenziato nelle linee guida WP 253, il GDPR non fissa importi fissi per violazioni specifiche. Il regolamento prevede invece importi massimi complessivi[44] e quindi segue la tradizione generale del diritto dell'UE sulle sanzioni già sancita da altri atti giuridici[45].

113. Gli importi di cui all'articolo 83, paragrafi da 4 a 6, GDPR costituiscono il limite massimo di legge e vietano alle autorità di controllo di irrogare sanzioni pecuniarie che risultino superiori agli importi massimi applicabili. Al fine di determinare il limite massimo di legge corretto, occorre prendere in considerazione l'articolo 83, paragrafo 3, GDPR[46], ove applicabile (cfr. la sezione 3.1.2). Nel calcolare le sanzioni pecuniarie sulla base delle presenti linee guida, ogni autorità di controllo deve quindi fare in modo di non superare tali importi massimi. A seconda del singolo caso, possono diventare pertinenti importi massimi diversi.

[44] Considerando 150 GDPR, seconda frase: "Il presente regolamento dovrebbe specificare le violazioni, indicare il limite massimo e i criteri per prevedere la relativa sanzione amministrativa pecuniaria, che dovrebbe essere stabilita dall'autorità di controllo competente in ogni singolo caso, tenuto conto di tutte le circostanze pertinenti della situazione specifica, in particolare della natura, gravità e durata dell'infrazione e delle relative conseguenze, nonché delle misure adottate per assicurare la conformità agli obblighi derivanti dal presente regolamento e prevenire o attenuare le conseguenze della violazione".
[45] In particolare, l'articolo 23, paragrafo 2, del regolamento (CE) n. 1/2003 del Consiglio, del 16 dicembre 2002, concernente l'applicazione delle regole di concorrenza di cui agli articoli 81 e 82 del trattato.
[46] Cfr. anche la decisione vincolante 1/2021 dell'EBPB, paragrafo 326.

6.1.1 - Importi massimi statici

114. L'articolo 83, paragrafi da 4 a 6, GDPR, prevede di norma importi statici e opera una distinzione tra le violazioni di diverse categorie di obblighi ai sensi del GDPR. Come spiegato in precedenza, l'articolo 83, paragrafo 4, GDPR prevede sanzioni pecuniarie fino a 10 milioni di EUR per la violazione degli obblighi ivi indicati, mentre l'articolo 83, paragrafi 5 e 6, GDPR, prevede sanzioni pecuniarie fino a 20 milioni di EUR per la violazione degli obblighi ivi indicati.

6.1.2 - Importi massimi dinamici

115. Nel caso di un'impresa[47], l'intervallo per la sanzione pecuniaria può spostarsi verso un importo massimo più elevato[48] in base al fatturato. Tale importo massimo basato sul fatturato è dinamico e personalizzato in relazione all'impresa, al fine di rispettare i principi di effettività, proporzionalità e dissuasività.

116. Più precisamente, l'articolo 83, paragrafo 4, GDPR prevede un importo massimo del 2 % e l'articolo 83, paragrafi 5 e 6 un importo massimo del 4 % del fatturato annuo totale dell'esercizio precedente dell'impresa. Il disposto del GDPR prevede che sia considerato l'importo massimo statico o l'importo massimo dinamico basato sul fatturato, "se superiore". Di conseguenza, tali importi massimi basati sul fatturato si applicano solo se superano il massimo statico nel singolo caso. Ciò avviene quando il fatturato annuo totale dell'impresa nell'esercizio precedente ammonta a più di 500 milioni di EUR[49].

Esempio 8a - Limite massimo dinamico
Un'agenzia di informazioni creditizie (CRA) raccoglie e vende tutti i dati sull'affidabilità creditizia di tutti i cittadini dell'UE a società pubblicitarie e di vendita al dettaglio senza disporre di una base giuridica. Il fatturato annuo mondiale della CRA dell'anno precedente ammonta a 3 miliardi di EUR. In questo caso, la CRA ha violato tra l'altro l'articolo 6, che può essere punito con una sanzione pecuniaria ai sensi dell'articolo 83, paragrafo 5, GDPR. Il limite massimo statico ammonterebbe a 20 milioni di EUR. Il limite massimo dinamico ammonterebbe a 120 milioni di EUR (4 % di 3 miliardi di EUR). La sanzione pecuniaria può arrivare a 120 milioni di EUR, poiché questo massimo dinamico è superiore al massimo statico di 20 milioni di EUR. Di conseguenza, la sanzione pecuniaria può superare il massimo statico di 20 milioni di EUR, ma non deve superare il limite massimo di legge applicabile di 120 milioni di EUR.

Esempio 8b - Limite massimo statico
Un rivenditore di occhiali da sole gestisce un negozio online che consente ai clienti di effettuare ordini. Tramite il modulo d'ordine, il rivenditore tratta anche i dati personali, tra cui i dati del conto bancario. Il rivenditore non prevede un'adeguata crittografia del trasporto (https), per cui durante la transazione i dati potrebbero essere intercettati da terzi. Il rivenditore viola l'articolo 32, paragrafo 1, GDPR, e può essere sanzionato ai sensi dell'articolo 83, paragrafo 4, GDPR. Il fatturato annuo del rivenditore a livello mondiale dell'anno precedente ammonta a 450 milioni di EUR. In questo caso, il limite massimo statico di 10 milioni di EUR è superiore al limite massimo dinamico di 9 milioni di EUR (=2 % di 450 milioni di EUR), per cui prevale il limite massimo di 10 milioni di EUR. La sanzione pecuniaria non deve quindi superare il limite massimo di legge di 10 milioni di EUR.

[47] Per quanto riguarda il termine "impresa", si rimanda alla sezione 6.2.1 delle presenti linee guida.
[48] Per quanto riguarda il termine "fatturato", si rimanda alla sezione 6.2.2 delle presenti linee guida.
[49] Il 2 % di 500 milioni è pari a 10 milioni (l'importo massimo statico previsto dall'articolo 83, paragrafo 4, GDPR) e il 4 % di 500 milioni ammonta a 20 milioni (l'importo massimo statico previsto all'articolo 83, paragrafo 5, GDPR).

Esempio 8c - Titolari del trattamento e responsabili del trattamento diversi da un'impresa
Un comune dispone di un sistema online che consente ai suoi cittadini di registrarsi per gli appuntamenti, ad esempio per richiedere un passaporto o una licenza di matrimonio. Il comune è l'unico titolare del trattamento di tale sistema online. Purtroppo, si scopre che il sistema trasmette anche in modo permanente i dati raccolti ai server esterni di un responsabile del trattamento in un paese terzo inadeguato, dove i dati vengono conservati. Non sono state adottate garanzie adeguate per quanto riguarda il trasferimento a un paese terzo. A eccezione del trasferimento, i dati sono raccolti e trattati sulla base di un consenso valido. Il comune ha violato l'articolo 44 GDPR trasferendo categorie particolari di dati personali in un paese terzo inadeguato senza opportune garanzie. Può essere pertanto sanzionato ai sensi dell'articolo 83, paragrafo 5. Poiché il comune non risponde alla definizione di impresa, si applica il massimo legale statico, per cui la sanzione pecuniaria non deve superare i 20 milioni di EUR. Tuttavia tale motivazione è valida solo se lo Stato membro in cui si trova il comune in questione non ha previsto norme specifiche che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro (articolo 83, paragrafo 7, GDPR).

6.2 - Determinazione del fatturato dell'impresa e responsabilità delle imprese

117. Al fine di determinare il fatturato corretto per calcolare il massimo legale dinamico, è importante comprendere i concetti di impresa e fatturato utilizzati all'articolo 83, paragrafi da 4 a 6, GDPR. A questo proposito, occorre prestare la massima attenzione ai considerando del GDPR, forniti dal legislatore europeo come guida all'interpretazione del medesimo.

6.2.1 - Definizione di impresa e responsabilità delle imprese

118. Per quanto riguarda il termine "impresa", il legislatore europeo fornisce ulteriori chiarimenti espliciti. Il considerando 150 GDPR recita: "Se le sanzioni amministrative sono inflitte a imprese, le imprese dovrebbero essere intese quali definite agli articoli 101 e 102 TFUE a tali fini".

119. Pertanto, l'articolo 83, paragrafi da 4 a 6, GDPR, alla luce del considerando 150, si basa sul concetto di impresa ai sensi degli articoli 101 e 102 TFUE[50], fatti salvi l'articolo 4, punto 18, GDPR (che fornisce una definizione di impresa) e l'articolo 4, punto 19, GDPR (che definisce un gruppo imprenditoriale). Il primo concetto è utilizzato principalmente nel capo V GDPR, nella frase "gruppo di imprese che svolgono un'attività economica comune". Inoltre il termine è applicato in senso generale, non come destinatario di una disposizione o di un obbligo.

120. Di conseguenza, nei casi in cui il titolare del trattamento o il responsabile del trattamento sia (parte di) un'impresa ai sensi degli articoli 101 e 102 TFUE, il fatturato combinato di tale impresa nel suo complesso può essere utilizzato per determinare il limite massimo dinamico della sanzione pecuniaria (cfr. la sezione 6.2.2), e per garantire che la sanzione pecuniaria risultante sia conforme ai principi di effettività, proporzionalità e capacità dissuasiva (articolo 83, paragrafo 1, GDPR)[51].

121. La CGUE ha elaborato una vasta giurisprudenza sul concetto di impresa. Il termine "impresa", "abbraccia qualsiasi entità che esercita un'attività economica, a prescindere dallo status giuridico di detta entità e dalle

[50] Come già chiarito nel WP 253 e successivamente confermato dall'EDPB nell'approvazione 1/2018 del 25 maggio 2018. Si veda anche la decisione vincolante1/2021 dell'EDPB, paragrafo 292 e il Tribunale regionale LG di Bonn, caso 29 OWi 1/20, 11 novembre 2020, punto 92.
[51] Cfr. la decisione vincolante 1/2021 dell'EDPB, paragrafi 412 e 423, e anche le cause C-286/13 P, *Dole food and Dole Fresh Fruit Europe contro Commissione europea*, punto 149 e C-189/02 P, *Dansk Rørindustri e altri contro Commissione*, punto 258.

sue modalità di finanziamento"[52]. Ai fini del diritto della concorrenza, le "imprese" sono quindi assimilate a unità economiche piuttosto che a unità giuridiche. Diverse società appartenenti allo stesso gruppo possono formare un'unità economica e quindi un'impresa ai sensi degli articoli 101 e 102 TFUE[53].

122. In linea con la giurisprudenza consolidata della CGUE, il termine "impresa" di cui agli articoli 101 e 102 TFUE può riferirsi a una singola unità economica, anche qualora tale unità economica sia costituita da più persone fisiche o giuridiche. Il fatto che diverse entità formino o meno una singola unità economica dipende in larga misura dal fatto che le singole entità godano di libera capacità decisionale o che un'entità leader, ossia la società madre, eserciti un'influenza determinante sulle altre[54]. I criteri per determinarlo si basano sui legami economici, giuridici e organizzativi tra la società madre e la sua controllata, ad esempio l'importo della partecipazione, i legami personali o organizzativi, le istruzioni e l'esistenza di accordi aziendali[55].

123. In linea con la dottrina in materia di singola unità economica, l'articolo 83, paragrafi da 4 a 6, GDPR segue il principio della responsabilità diretta dell'impresa, che implica che tutte le azioni od omissioni compiute da persone fisiche autorizzate ad agire per conto delle imprese sono imputabili a queste ultime e sono considerate come un'azione e una violazione commessa direttamente dalle imprese stesse[56]. Il fatto che alcuni dipendenti non abbiano rispettato un codice di condotta non è sufficiente a impedire tale imputabilità[57] che, invece, viene meno soltanto quando la persona fisica agisce esclusivamente per i suoi scopi privati o per gli scopi di terzi, diventando così essa stessa un titolare del trattamento distinto (ossia la persona fisica ha agito andando oltre l'autorità conferitale)[58]. Questo principio riguardante l'ambito della responsabilità dell'impresa proprio del diritto dell'Unione europea è prevalente e non deve essere compromesso limitandolo agli atti di alcuni funzionari (come i responsabili principali) in contrasto con il diritto nazionale. Non è rilevante quale persona fisica abbia agito e per conto di quale delle entità. L'autorità di controllo e gli organi giurisdizionali nazionali non devono quindi essere tenuti a determinare o identificare una persona fisica nel corso delle indagini o nell'ambito della decisione di irrogazione della sanzione pecuniaria[59].

---

[52] Causa C-41/90, *Klaus Höfner e Fritz Elser contro Macrotron GmbH*, punto 21. Cfr. anche, ad esempio, le cause riunite C-159 e 160/91, *Poucet and Pistre contro Assurances Générales de France*, punto 17; la causa C-364/92, *SAT Fluggesellschaft mbH contro Eurocontrol*, punto 18; le cause riunite da C-180 a 184/98, *Pavlov e altri*, punto 74; e la causa C-138/11, *Compass-Datenbank GmbH contro Republik Österreich*, punto 35.

[53] Causa C-516/15 P, *Akzo Nobel e a. contro Commissione*, punto 48.

[54] Per chiarire, la "capacità decisionale" che deve essere valutata per stabilire se una società madre esercita un'influenza determinante sugli altri membri del gruppo si riferisce alla capacità decisionale in relazione alla condotta della controllata "sul mercato". Tale capacità è diversa e completamente distinta dall'influenza che una società madre può o meno avere sul trattamento in questione e, in particolare, dalla capacità di prendere decisioni in relazione alle "finalità e ai mezzi" del trattamento. Tali aspetti devono essere valutati nell'ambito dell'eventuale esame dell'identità del titolare del trattamento dei dati e non sono rilevanti per la valutazione dell'influenza determinante ai fini della costituzione di una singola unità economica.

[55] Cfr. la causa C-90/09 P, *General Química e altri contro Commissione*. Il criterio principale per stabilirlo è l'"influenza determinante", che dovrebbe essere interpretata sulla base di prove concrete (legami economici, organizzativi e giuridici). Inoltre esiste una presunzione semplice di influenza nel caso di una controllata al 100 %. Cfr. la causa C-97/08 P, *Akzo Nobel e altri contro Commissione europea* e le cause riunite C-293/13 e 294/13 P, *Fresh Del Monte*.

[56] Cfr. le cause riunite da C-100 a 103/80, *SA Musique Diffusion française e altri contro Commissione*, punto 97 e la causa C-338/00 P, *Volkswagen contro Commissione*, punti da 93 a 98.

[57] Causa C-501/11 P, *Schindler Holding e altri contro Commissione*, punto 114. È importante quindi per le imprese che il loro sistema di gestione della conformità non sia un semplice "scudo di carta", ma sia realmente efficace nella pratica.

[58] Cfr. in particolare le linee guida 07/2020 sui concetti di titolare del trattamento o responsabile del trattamento nel GDPR (di seguito "Linee guida dell'EDPB 07/2020"), paragrafo 19.

[59] Causa C-338/00 P, *Volkswagen contro Commissione*, punti 97 e 98; qualsiasi ordinamento nazionale in conflitto non è conforme al GDPR e al principio di efficacia e pertanto non deve essere applicato.

124. Nel caso specifico in cui una società madre detenga il 100 % o quasi delle azioni di una controllata che abbia violato l'articolo 83 GDPR, e sia quindi in grado di esercitare un'influenza determinante sulla condotta di quest'ultima, si può presumere che la società madre eserciti effettivamente tale influenza determinante sulla condotta della sua controllata (la cosiddetta presunzione *Akzo*)[60]. Ciò vale anche se la società madre non detiene le azioni del capitale totale direttamente, ma indirettamente tramite una o più controllate[61]. Ad esempio, potrebbe esserci anche una catena di controllate, nella quale un'entità detiene il 100 % o quasi delle azioni di un'entità intermedia che, a sua volta, detiene il 100 % o quasi delle azioni di un'altra entità, e così via. Inoltre una società madre potrebbe detenere il 100 % o quasi delle azioni di due entità che detengono ciascuna circa il 50 % di un'entità, garantendo così alla società madre un'influenza determinante su tutte. In tali circostanze, è sufficiente che l'autorità di controllo dimostri che la controllata è, direttamente o indirettamente, interamente o quasi interamente di proprietà della società madre, per presumere - come regola di esperienza pratica - che la società madre eserciti un'influenza determinante.

125. Tuttavia, la presunzione *Akzo* non è assoluta, ma può essere confutata da altre prove[62]. Per confutare la presunzione, la società (o le società) deve fornire prove relative ai legami organizzativi, economici e giuridici tra la controllata e la sua società madre, atti a dimostrare che non costituiscono una singola unità economica nonostante detengano il 100 % o quasi delle azioni. Per accertare se una controllata agisce in modo autonomo, si deve tenere conto di tutti i fattori pertinenti relativi ai vincoli che legano la controllata alla società madre, che possono variare da caso a caso e non possono quindi essere elencati in modo esaustivo.

126. Se, invece, la società madre non detiene la totalità o la quasi totalità del capitale, l'autorità di controllo deve dimostrare ulteriori fatti per giustificare l'esistenza di una singola unità economica. In tal caso, l'autorità di controllo deve dimostrare non solo che la società madre ha la capacità di esercitare un'influenza determinante sulla controllata, ma anche che l'ha effettivamente esercitata, in modo da poter intervenire in qualsiasi momento nella libertà di scelta della controllata e determinarne il comportamento. La natura o il tipo di istruzione è irrilevante nel determinare l'influenza della società madre.

127. La sanzione pecuniaria è irrogata[63] ai (co-)titolari del trattamento/responsabili del trattamento, e l'autorità di controllo competente ha la possibilità di ritenere la società madre responsabile in solido[64] per il pagamento della sanzione pecuniaria.

6.2.2 - Determinazione del fatturato

128. Il fatturato è ricavato dai conti annuali dell'impresa, che sono redatti con riferimento all'esercizio sociale e forniscono una panoramica dell'esercizio finanziario passato della società o del gruppo di società (conti consolidati). Il fatturato è definito come la somma di tutti i beni e servizi venduti. "Ricavi netti": gli importi provenienti dalla vendita di prodotti e dalla prestazione di servizi, dopo aver dedotto gli sconti concessi sulle

[60] Causa C-97/08 P, *Akzo Nobel e altri contro Commissione*, punti 59 e 60.
[61] Cause T-38/05, *Agroexpansión contro Commissione*, e C-508/11 P, *Eni contro Commissione*, punto 48.
[62] Cfr., tra gli altri, la causa C-595/18 P, *The Goldman Sachs Group contro Commissione*, ECLI: EU: C: 2021:73, punto 32, citando la causa C 611/18 P, *Pirelli & C. contro Commissione*, non pubblicata, punto 68, e la giurisprudenza citata.
[63] La decisione nella quale viene irrogata la sanzione pecuniaria è indirizzata e consegnata ai titolari del trattamento/ responsabili del trattamento in quanto autori della violazione e può essere indirizzata e consegnata anche ad altre persone giuridiche della singola unità economica che sono responsabili in solido della sanzione pecuniaria.
[64] Decisione vincolante 1/2021 dell'EDPB, paragrafo 290.

vendite, l'imposta sul valore aggiunto (IVA) e le altre imposte direttamente connesse con i ricavi delle vendite e delle prestazioni[65].

129. Il fatturato è ricavato dalla presentazione del conto economico[66]. Il fatturato netto comprende i ricavi derivanti dalla vendita, dal noleggio e dal leasing di prodotti e i ricavi derivanti dalla vendita di servizi, al netto delle detrazioni sulle vendite (ad esempio, sconti, ribassi) e dell'IVA.

130. Se l'impresa è soggetta all'obbligo di redigere un bilancio annuale consolidato[67], tale bilancio consolidato della società madre a capo del gruppo è pertinente ai fini della determinazione del fatturato combinato dell'impresa[68]. Se tale bilancio non esiste, si dovrà ottenere e utilizzare qualsiasi altro documento utile per dedurre il fatturato annuo mondiale annuo dell'impresa nell'esercizio sociale pertinente.

131. L'articolo 83, paragrafi da 4 a 6, GDPR stabilisce che debba essere utilizzato il fatturato mondiale totale annuo dell'esercizio finanziario precedente. Per quanto riguarda la questione di quale sia l'evento a cui si riferisce il termine "precedente", la giurisprudenza della CGUE in materia di diritto della concorrenza deve essere applicata anche per le sanzioni pecuniarie del GDPR, in modo che l'evento pertinente sia la decisione di irrogazione della sanzione pecuniaria emessa dall'autorità di controllo e non il momento della violazione né la decisione del tribunale[69]. In caso di trattamento transfrontaliero, la decisione di irrogazione della sanzione pecuniaria pertinente non è il progetto di decisione, bensì la decisione finale emessa dall'autorità di controllo capofila[70]. Qualora il progetto di decisione entri nel processo di codecisione ai sensi dell'articolo 60 verso la fine di un anno civile, per cui è improbabile che la decisione finale sia adottata entro lo stesso anno civile, l'autorità di controllo capofila calcolerà la sanzione pecuniaria proposta in riferimento alle informazioni finanziarie più aggiornate disponibili alla data in cui il progetto di decisione è stato trasmesso alle autorità di controllo interessate per ottenere il loro parere. Tali informazioni saranno poi aggiornate, se necessario, prima della finalizzazione e dell'adozione della decisione nazionale definitiva da parte dell'autorità di controllo capofila.

CAPITOLO 7 – EFFETTIVITÀ, PROPORZIONALITÀ E DISSUASIVITÀ

132. La sanzione amministrativa inflitta per le violazioni del GDPR di cui all'articolo 83, paragrafi da 4 a 6, deve essere effettiva, proporzionata e dissuasiva in ogni singolo caso. In altre parole, l'importo della sanzione pecuniaria inflitta è adattato in funzione della violazione commessa nel suo contesto specifico. L'EDPB ritiene che spetti alle autorità di controllo verificare se l'importo della sanzione pecuniaria risponde a tali requisiti o se occorre adeguarlo ulteriormente.

---

[65] Cfr. ad es., l'articolo 2, paragrafo 5, della direttiva 2013/34/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativa ai bilanci d'esercizio, ai bilanci consolidati e alle relative relazioni di talune tipologie di imprese, recante modifica della direttiva 2006/43/CE del Parlamento europeo e del Consiglio e abrogazione delle direttive 78/660/CEE e 83/349/CEE (di seguito "direttiva 2013/34/UE"), applicabile alle società a responsabilità limitata, o legislazione applicabile simile e l'articolo 5, paragrafo 1, del regolamento (CE) n. 139/2004 del Consiglio relativo al controllo delle concentrazioni tra imprese (di seguito "regolamento comunitario sulle concentrazioni").

[66] Cfr., ad esempio, gli allegati V o VI di cui all'articolo 13, paragrafo 1, direttiva 2013/34/UE alla voce "ricavi netti delle vendite e delle prestazioni", o la legislazione applicabile simile.

[67] Cfr., ad esempio, l'articolo 21 e seguenti della direttiva 2013/34/UE, o una normativa applicabile analoga.

[68] C-58/12 P *Groupe Gascogne SA contro Commissione Europea*, ECLI:EU:C:2013:770, punti 54 e 55.

[69] Tribunale regionale LG Bonn, causa 29 OWi 1/20, 11 novembre 2020, punto 95, con riferimento alla causa C-637/13 P, *Badezimmerkartell Laufen Austria*, punto 49 e alla causa C-408/12 P, *YKK et al*, punto 90.

[70] Decisione vincolante 1/2021 dell'EDPB, paragrafo 298.

133. Come spiegato nel capitolo 4, la valutazione eseguita in tale capitolo riguarda tutti gli aspetti della sanzione imposta e tutte le circostanze del caso, incluso ad esempio l'accumulo di violazioni multiple, gli aumenti e le riduzioni per le circostanze aggravanti e attenuanti e le circostanze finanziarie/socio-economiche. Tuttavia spetta all'autorità di controllo garantire che le stesse circostanze non siano contate due volte.

134. Nel caso in cui tali adeguamenti meritino un aumento della sanzione pecuniaria, tale aumento non può - per definizione - superare il limite massimo di legge individuato nel capitolo 6.

7.1 - Effettività

135. In linea generale, una sanzione pecuniaria può essere considerata effettiva se consegue gli obiettivi per i quali è stata inflitta. L'obiettivo potrebbe essere quello di ripristinare la conformità alle norme oppure di punire un comportamento illecito (o entrambi)[71]. Inoltre il considerando 148 GDPR sottolinea che le sanzioni amministrative pecuniarie dovrebbero essere imposte "per rafforzare il rispetto delle norme del presente regolamento". L'importo della sanzione pecuniaria inflitta sulla base delle presenti linee guida dovrebbe quindi essere sufficiente a conseguire tali obiettivi.

136. Come disposto dall'articolo 83, paragrafo 2, GDPR, l'autorità di controllo deve valutare l'effettività della sanzione pecuniaria in ogni singolo caso. A tal fine, si dovrebbe prestare debita attenzione alle circostanze del caso, e in particolare alla valutazione di cui sopra[72], tenendo presente che la sanzione pecuniaria deve essere anche proporzionata e dissuasiva, come indicato di seguito.

7.2 - Proporzionalità

137. Secondo il principio di proporzionalità le misure adottate non devono eccedere i limiti di quanto è idoneo e necessario per il conseguimento degli scopi legittimi perseguiti dalla normativa di cui trattasi; qualora sia possibile una scelta tra più misure appropriate, si deve ricorrere alla meno restrittiva e gli inconvenienti causati non devono essere sproporzionati rispetto agli scopi perseguiti[73].

138. Ne consegue che gli importi delle sanzioni pecuniarie non devono essere sproporzionati rispetto alle finalità perseguite (vale a dire il rispetto alle norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e delle norme relative alla libera circolazione dei dati personali) e che l'importo della sanzione pecuniaria inflitta deve essere proporzionato alla violazione, valutata complessivamente, tenendo conto, in particolare, della gravità di quest'ultima[74].

139. L'autorità di controllo deve quindi verificare che l'importo della sanzione pecuniaria sia **proporzionato** sia alla gravità della violazione sia alle dimensioni dell'impresa a cui appartiene l'entità che ha commesso la

[71] Linee guida WP 253, pag. 6.
[72] Come specificato anche al considerando 148 GDPR: "[…] alla natura, alla gravità e alla durata della violazione, al carattere doloso della violazione e alle misure adottate per attenuare il danno subito, al grado di responsabilità o eventuali precedenti violazioni pertinenti, alla maniera in cui l'autorità di controllo ha preso conoscenza della violazione, al rispetto dei provvedimenti disposti nei confronti del titolare del trattamento o del responsabile del trattamento, all'adesione a un codice di condotta e eventuali altri fattori aggravanti o attenuanti".
[73] Causa T-704/14, *Marine Harvest/Commissione*, punto 580, con riferimento alla causa T-332/09, *Electrabel contro Commissione*, punto 279.
[74] Ibidem.

violazione[75], e che la sanzione pecuniaria irrogata non ecceda quindi quanto necessario per il conseguimento degli scopi perseguiti dal GDPR.

140. Come particolare derivato del principio di proporzionalità, l'autorità di controllo può valutare - conformemente all'ordinamento nazionale - la possibilità di ridurre ulteriormente la sanzione pecuniaria sulla base del principio dell'incapacità contributiva. Eventuali riduzioni di questo tipo richiedono circostanze eccezionali. In linea con gli orientamenti della Commissione europea per il calcolo delle ammende[76], devono esserci prove oggettive dalle quali risulti che l'imposizione della sanzione pecuniaria pregiudicherebbe irrimediabilmente la redditività economica dell'impresa interessata. Inoltre i rischi devono essere valutati in presenza di un contesto sociale ed economico particolare.

a) **Redditività economica:** l'impresa è tenuta a fornire dati finanziari dettagliati (per gli ultimi cinque anni, nonché proiezioni per l'anno in corso e per i successivi due anni) per consentire all'autorità di controllo di esaminare l'evoluzione prevedibile di fattori chiave quali solvibilità, liquidità e redditività. Gli organi giurisdizionali europei hanno affermato che la semplice circostanza che un'impresa si trovi in una situazione finanziaria di passività, o che lo sarà dopo una sanzione pecuniaria elevata, non soddisfa il requisito "dal momento che il riconoscimento di un tale obbligo procurerebbe un vantaggio concorrenziale ingiustificato alle imprese meno idonee alle condizioni del mercato"[77] La valutazione della capacità dell'impresa di pagare la sanzione pecuniaria prende in considerazione anche i possibili piani di ristrutturazione e il loro stato di attuazione, i rapporti con partner/istituti finanziari esterni come le banche e i rapporti con gli azionisti[78].

b) **Prova della perdita di valore:** una riduzione della sanzione pecuniaria può essere concessa solo se la sua irrogazione mette a rischio la redditività economica di un'impresa e fa sì che i suoi beni perdano tutto il loro valore o la maggior parte di esso[79]. Deve essere dimostrato un legame causale diretto tra la sanzione pecuniaria e la significativa perdita di valore dei beni. Non esiste alcuna accettazione automatica del fatto che il fallimento o l'insolvenza comportino necessariamente una perdita significativa del valore dei beni. Inoltre non si può dire che la sanzione pecuniaria abbia messo a rischio la redditività economica di un'impresa quando essa stessa aveva deciso di cessare le sue attività e di vendere tutti i suoi beni. L'impresa deve dimostrare che probabilmente uscirà dal mercato e i suoi beni saranno smantellati o venduti a prezzi fortemente scontati, senza possibilità alternative che l'impresa (o i suoi beni) continui a operare. Ciò significa che l'autorità di controllo dovrebbe richiedere all'impresa di dimostrare che non vi sono chiare indicazioni che

[75] Cfr., a questo proposito, la causa C-387/97, *Commissione contro Grecia*, punto 90, e la causa C-278/01, *Commissione contro Spagna*, punto 41, in cui l'ammenda doveva essere "adeguat[a] alle circostanze e commisurat[a] sia all'inadempimento accertato sia alla capacità finanziaria dello Stato membro di cui trattasi".

[76] Su questo principio, si vedano ad esempio gli orientamenti della Commissione per il calcolo delle ammende inflitte in applicazione dell'articolo 23, paragrafo 2, lettera a), del regolamento (CE) n. 1/2003 (2006/C 210/02).

[77] Cfr. cause riunite C-189/02 P, C-202/02 P, da C-205/02 P a C-208/02 P e C-213/02 P, *Dansk Rørindustri e altri contro Commissione*, punto 327, citando le cause riunite 96/82-102/82, 104/82, 105/82, 108/82 e 110/82, *NV IAZ International Belgium e altri contro Commissione*, punti 54 e 55. Ciò è stato ripetuto più di recente nella causa C-308/04 P, *SGL Carbon contro Commissione*, punto 105, e nella causa T-429/10 (cause riunite T-426/10, T-427/10, T-428/10, T-429/10, T-438/12, T-439/12, T-440/12, T-441/12), *Global Steel Wire contro Commissione*, punti 492 e 493.

[78] Cfr. la causa T-429/10 (cause riunite T-426/10, T-427/10, T-428/10, T-429/10, T-438/12, T-439/12, T-440/12, T-441/12), *Global Steel Wire contro Commissione*, punti da 521 a 527.

[79] Cfr. cause riunite T-236/01, T-239/01, da T-244/01 a T-246/01, T-251/01 e T-252/01, *Tokai Carbon e altri contro Commissione*, punto 372 e la causa T-64/02, *Heubach contro Commissione*, punto 163. Cfr. la causa T-393/10 INTP, *Westfälische Drahtindustrie e altri contro Commissione*, punti 293 e 294.

l'impresa (o i suoi beni) saranno acquisiti da un'altra impresa/proprietario e continueranno a operare.

c) **Contesto sociale ed economico particolare:** il contesto economico particolare può essere preso in considerazione se il settore interessato sta attraversando una crisi ciclica (ad esempio, soffre di sovraccapacità o di calo dei prezzi) o se le imprese hanno difficoltà ad accedere al capitale o al credito a causa delle condizioni economiche prevalenti. È probabile che un contesto sociale particolare sia presente in un contesto di disoccupazione elevata e/o crescente a livello regionale o più ampio. Può anche essere valutato considerando le conseguenze che il pagamento della sanzione pecuniaria può avere in termini di aumento della disoccupazione o di deterioramento dei settori economici a monte e a valle[80].

141. Se i criteri sono soddisfatti, le autorità di controllo possono prendere in considerazione l'incapacità contributiva dell'impresa e ridurre la sanzione pecuniaria di conseguenza.

7.3 - Dissuasività

142. Una sanzione pecuniaria dissuasiva infine è quella che ha un vero effetto dissuasivo[81]. A questo proposito, si può operare una distinzione tra "dissuasione generale" (dissuadere gli altri dal commettere la stessa violazione in futuro) e "dissuasione specifica" (dissuadere il destinatario della sanzione pecuniaria dal commettere nuovamente la stessa violazione)[82]. Nell'irrogare una sanzione pecuniaria, l'autorità di controllo prende in considerazione sia la dissuasione generale sia quella specifica.

143. Dissuasiva è una sanzione che induce l'individuo ad astenersi dal violare gli scopi e le norme di diritto dell'Unione. A tal proposito non contano solo il tipo e la misura della sanzione, ma anche la probabilità con la quale la stessa può essere irrogata: chi commette un'infrazione deve temere di essere effettivamente punito con una sanzione. Sotto questo profilo il criterio della capacità dissuasiva si sovrappone a quello dell'effettività[83].

144. Le autorità di controllo possono valutare la possibilità di aumentare la sanzione pecuniaria se ritengono che l'importo non sia sufficientemente dissuasivo. In alcune circostanze può essere giustificata l'applicazione di un coefficiente moltiplicatore di dissuasione[84]. Tale coefficiente moltiplicatore può essere fissato a discrezione dell'autorità di controllo, al fine di rispondere agli obiettivi di dissuasività di cui sopra.

CAPITOLO 8 – FLESSIBILITÀ E VALUTAZIONE PERIODICA

145. I capitoli precedenti delineano un metodo generale per il calcolo delle sanzioni pecuniarie e contribuiscono a migliorare l'armonizzazione e la trasparenza per quanto riguarda la prassi delle autorità di controllo in materia di imposizione delle sanzioni pecuniarie. Tuttavia tale metodo generale non deve essere frainteso come una forma di calcolo automatico o aritmetico. La singola determinazione di una sanzione pecuniaria deve sempre basarsi su una valutazione umana di tutte le circostanze pertinenti del caso e deve essere effettiva, proporzionata e dissuasiva in relazione al caso di specie.

[80] Cfr. la causa C-308/04 P, *SGL Carbon contro Commissione*, punto 106.
[81] Cfr. il parere dell'avvocato generale Geelhoed nella causa C-304/02, *Commissione contro Francia*, punto 39.
[82] Cfr., tra l'altro, la causa C-511/11 P, *Versalis Spa contro Commissione*, punto 94.
[83] Parere dell'avvocato generale Kokott nelle cause riunite C-387/02, C-391/02 e C-403/02, *Silvio Berlusconi e altri*, punto 89.
[84] Cfr. segnatamente la causa C-289/04 P, *Showa Denko contro Commissione*, punti 28-39.

146. Occorre tenere conto del fatto che le presenti linee guida non possono prevedere tutte le possibili particolarità di un caso e, sotto questo profilo, non possono costituire una guida esaustiva per le autorità di controllo. Esse sono pertanto soggette a un riesame periodo al fine di valutare se la loro applicazione permette di conseguire effettivamente gli obiettivi previsti dal GDPR. L'EDPB può rivedere le presenti linee guida in base alle ulteriori esperienze delle autorità di controllo nell'applicazione pratica quotidiana e può sospenderle, cambiarle, limitarle, modificarle o sostituirle in qualsiasi momento con effetto *ex nunc*.

ALLEGATO - TABELLA ILLUSTRATIVA DELLE LINEE GUIDA 04/2022 SUL CALCOLO DELLE SANZIONI AMMINISTRATIVE PECUNIARIE AI SENSI DEL GDPR

Guida alla lettura

- La presente tabella deve essere letta unitamente alle linee guida nella loro interezza e non è da intendersi come una sintesi completa delle linee guida o come un'alternativa ad un loro esame complessivo.
- La presente tabella ha uno scopo puramente illustrativo e non è una rappresentazione completa né conclusiva della posizione dell'EDPB sul calcolo delle sanzioni amministrative pecuniarie.
- La tabella si articola in due fasi: una che illustra l'intervallo dell'importo iniziale basato sulla gravità della violazione, e una che illustra l'intervallo dell'importo iniziale dopo l'adeguamento applicato in base alle dimensioni dell'impresa.
- Le cifre utilizzate come importi iniziali corrispondono, da una parte, alla raccomandazione della Commissione relativa alle PMI e al modo in cui i fatturati menzionati in tale raccomandazione si rapportano al fatturato scaturente dall'articolo 83 GDPR[85]; dall'altra, per quanto riguarda la gravità della violazione, le cifre si basano sulle informazioni derivanti dalla pratica attuale di irrogazione delle sanzioni pecuniarie e su approfonditi test interni condotti con modelli di irrogazione delle sanzioni pecuniarie nel corso di diversi anni. L'EDPB è convinto che questi punti di partenza rendano giustizia ai principi di effettività, proporzionalità e dissuasività, come prescritto dall'articolo 83, paragrafo 1, GDPR.
- Tuttavia, come sempre, l'EDPB è consapevole che il calcolo di una sanziona amministrativa pecuniaria non sia un esercizio puramente matematico e che i casi reali e la pratica porteranno inevitabilmente a un ulteriore affinamento dei punti di partenza di questa tabella. A tal fine, le linee guida specificano che la tabella e le cifre in essa contenute rimangono sotto stretta osservazione da parte dell'EDPB e saranno adattate se necessario.
- Occorre ribadire anche che tali cifre sono i punti di partenza per l'ulteriore calcolo, e non importi fissi (cartellini dei prezzi). L'autorità di controllo dispone del potere discrezionale di utilizzare l'intero intervallo della sanzione, a partire da qualsiasi importo fino al limite massimo di legge.
- Nella prima fase, quanto più grave è la violazione all'interno della propria categoria, tanto più alto sarà probabilmente l'importo iniziale.
- Nella seconda fase, per determinare l'importo iniziale definitivo si utilizzano principalmente le percentuali, sebbene gli adeguamenti al ribasso possano essere effettuati fino a una determinata percentuale dell'importo iniziale stabilito nella fase 1. Ciò significa che la percentuale scelta nella fase 2 sarà utilizzata come coefficiente moltiplicatore per l'importo iniziale determinato nella fase 1. Quanto maggiore è il fatturato dell'impresa all'interno del suo livello applicabile, tanto più alto sarà probabilmente l'importo iniziale nella fase 2.
- Nella seconda fase gli importi illustrano semplicemente il limite minimo e quello massimo che possono essere applicati nella categoria. L'importo iniziale definitivo si collocherà all'interno di questi estremi. Gli intervalli della seconda fase servono quindi come controllo di conformità per il funzionario incaricato del caso.

[85] Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (notificata con il numero C(2003) 1422), (2003/361/CE).

- Occorre rilevare che nella fase 2 non è previsto alcun adeguamento per le imprese con un fatturato pari o superiore a 500 milioni EUR, poiché queste imprese supereranno il limite massimo di legge statico e, quindi, la dimensione dell'impresa si riflette nel limite massimo di legge dinamico utilizzato per determinare l'importo di partenza per l'ulteriore calcolo nella fase 1.
- L'applicazione della metodologia, compreso l'uso delle tabelle, è illustrata da due esempi alla fine del presente allegato.

Fase 1 Calcolo dell'importo iniziale in base alla gravità

N.B.: quanto più grave è la violazione all'interno della propria categoria, tanto più alto sarà probabilmente l'importo iniziale in questa prima fase.

	Livello di gravità basso		**Livello di gravità medio**		**Livello di gravità elevato**	
	Intervallo statico	*Intervallo dinamico* nel caso di un fatturato > 500 Mio	*Intervallo statico*	*Intervallo dinamico nel caso di un fatturato > 500 Mio*	*Intervallo statico*	*Intervallo dinamico nel caso di un fatturato > 500 Mio*
Articolo 83, paragrafo 4, GDPR	0 - 1 Mio	0 - 0,2 % del fatturato annuo	1 Mio - 2 Mio	0,2 % - 0,4 % del fatturato annuo	2 Mio - 10 Mio	0,4 % - 2 % del fatturato annuo
Articolo 83, paragrafi 5 e 6, GDPR	0 – 2 Mio	0 - 0,4 % del fatturato annuo	2 Mio - 4 Mio	0,4 % - 0,8 % del fatturato annuo	4 Mio - 20 Mio	0,8 % - 4 % del fatturato annuo

Fase 2 Adeguamento dell'importo iniziale in base alle dimensioni dell'impresa (applicabile solo alle imprese alle quali si applica l'intervallo legale statico)

N.B.: quanto maggiore è il fatturato dell'impresa all'interno del suo livello applicabile, tanto più alto sarà probabilmente l'importo iniziale nella seconda fase.

Articolo 83, paragrafo 4, GDPR

	Livello di gravità basso	**Livello di gravità medio**	**Livello di gravità elevato**
Imprese con un fatturato compreso tra 250 milioni di EUR e 500 milioni di EUR	40 - 100 % dell'importo iniziale		
	0 – 1 Mio	400 000 – 2 Mio	800 000 – 10 Mio

	Livello di gravità basso	**Livello di gravità medio**	**Livello di gravità elevato**
Imprese con un fatturato compreso tra 100 milioni di EUR e 250 milioni di EUR	15 - 50 % dell'importo iniziale		
	0 - 500 000	150 000 – 1 Mio	300 000 – 5 Mio
Imprese con un fatturato compreso tra 50 milioni di EUR e 100 milioni di EUR	8 – 20 % dell'importo iniziale		
	0 - 200 000	80 000 - 400 000	160 000 – 2 Mio
Imprese con un fatturato compreso tra 10 milioni di EUR e 50 milioni di EUR	1,5 – 10 % dell'importo iniziale		
	0 - 100 000	15 000 - 200 000	30 000 – 1 Mio
Imprese con un fatturato compreso tra 2 milioni di EUR e 10 milioni di EUR	0,3 – 2 % dell'importo iniziale		
	0 - 20 000	3 000 - 40 000	6 000 - 200 000
Imprese con un fatturato fino a 2 milioni di EUR	0,2 - 0,4 % dell'importo iniziale		
	0 - 4 000	2 000 - 8 000	4 000 - 40 000

Articolo 83, paragrafi 5 e 6, GDPR

	Livello di gravità basso	**Livello di gravità medio**	**Livello di gravità elevato**
Imprese con un fatturato compreso tra 250 milioni di EUR e 500 milioni di EUR	40 – 100 % dell'importo iniziale		
	0 – 2 Mio	800 000 – 4 Mio	1,6 Mio– 20 Mio
Imprese con un fatturato compreso tra 100 milioni di EUR e 250 milioni di EUR	15 - 50 % dell'importo iniziale		
	0 – 1 Mio	300 000 – 2 Mio	600 000 – 10 Mio
Imprese con un fatturato compreso tra 50 milioni di EUR e 100 milioni di EUR	8 – 20 % dell'importo iniziale		
	0 - 400 000	160 000 - 800 000	320 000 – 4 Mio
Imprese con un fatturato compreso tra 10 milioni di EUR e 50 milioni di EUR	1,5 – 10 % dell'importo iniziale		
	0 - 200 000	30 000 - 400 000	60 000 – 2 Mio
Imprese con un fatturato compreso tra 2 milioni di EUR e 10 milioni di EUR	0,3 – 2 % dell'importo iniziale		
	0 - 40 000	6 000 - 80 000	12 000 - 400 000
Imprese con un fatturato fino a 2 milioni di EUR	0,2 - 0,4 % dell'importo iniziale		
	0 - 8 000	4 000 - 16 000	8 000 - 80 000

Approccio fase per fase su come applicare il capitolo 4 delle linee guida sull'irrogazione delle sanzioni pecuniarie, comprese le tabelle

Esempio A

Si è scoperto che un'impresa di social media con un fatturato di 200 milioni di EUR ha venduto i dati sensibili dei suoi utenti a diversi intermediari di dati. Ai fini di questo esempio, l'impresa ha violato solo l'articolo 9 GDPR. L'autorità di controllo, dopo aver analizzato tutte le circostanze pertinenti del caso ai sensi dell'articolo 83, paragrafo 2, lettere a), b) e g), ha deciso che il livello di gravità della violazione è elevato.

Dopodiché, l'autorità di controllo deve decidere l'importo iniziale per l'ulteriore calcolo. L'articolo 9 è elencato nell'articolo 83, paragrafo 5, lettera a), GDPR, che stabilisce che il limite massimo di legge è pari a 20 milioni di EUR o al 4 % del fatturato annuo. In questo caso, il fatturato dell'impresa è inferiore a 500 milioni di EUR, il che significa che si applicano l'intervallo e il limite massimo statici. Pertanto, si dovrebbe prendere in considerazione un importo iniziale compreso tra il 20 e il 100 % del limite massimo di legge applicabile, vale a dire 4 milioni di EUR e 20 milioni di EUR. Considerando che quanto più grave è la violazione all'interno della propria categoria, tanto più alto sarà probabilmente l'importo iniziale, l'autorità di controllo decide che l'importo iniziale basato sulla gravità della violazione, come indicato nella fase 1, dovrebbe essere di 10 milioni di EUR.

Nella fase 2, l'importo di partenza individuato nella fase 1 sarà adeguato in base alle dimensioni dell'impresa. Il fatturato annuo dell'impresa è pari a 200 milioni di EUR e quindi rientra nell'intervallo tra 100 e 250 milioni di EUR. Ciò significa che l'importo iniziale sarà adeguato a un importo compreso tra il 15 % e il 50 % dell'importo iniziale. Considerando che quanto maggiore è il fatturato dell'impresa all'interno del suo livello applicabile, tanto più alto sarà probabilmente l'importo iniziale, l'autorità di controllo decide che un adeguamento fino al 40 % dell'importo iniziale stabilito nella fase 1 è giustificato in base alle dimensioni dell'impresa. In questo caso, l'importo iniziale dopo l'adeguamento sarà di 4 milioni di EUR.

Per assicurarsi che tale importo iniziale sia in linea con le linee guida, è possibile effettuare un controllo incrociato con gli intervalli che figurano nella tabella applicabile. Considerando che è applicabile l'articolo 83, paragrafo 5, GDPR, che l'impresa ha un fatturato compreso tra 100 e 250 milioni di EUR e che il livello di gravità è elevato, l'importo iniziale dovrebbe essere compreso tra 600 000 EUR e 10 milioni di EUR. L'autorità di controllo conclude che un importo iniziale di 4 milioni di EUR rientra nell'intervallo tra 600 000 EUR e 10 milioni di EUR. l'importo iniziale è pertanto in linea con le linee guida.

L'autorità di controllo procede quindi al calcolo della sanzione pecuniaria sulla base del resto delle linee guida.

Esempio B

Una catena alberghiera con un fatturato di 2 miliardi di EUR ha violato l'articolo 12 GDPR. L'autorità di controllo, dopo aver analizzato le circostanze del caso ai sensi dell'articolo 83, paragrafo 2, lettere a), b) e g), ha deciso che il livello di gravità della violazione è medio.

Dopodiché, l'autorità di controllo deve decidere l'importo iniziale per l'ulteriore calcolo. L'autorità di controllo si accerta innanzitutto che l'articolo 12 GDPR sia elencato nell'articolo 83, paragrafo 5, lettera b), GDPR. Il fatturato dell'impresa è di 2 miliardi di EUR, ovvero superiore a 500 milioni di EUR,

e quindi si applica il massimo dinamico. Ciò significa che il limite massimo di legge corrisponde al 4 % del fatturato annuo dell'impresa, pari a 80 milioni di EUR. Il livello di gravità è medio e, pertanto, l'importo iniziale deve essere considerato tra il 10 e il 20 % del limite massimo di legge applicabile, ossia lo 0,4 % e lo 0,8 % del fatturato annuo, che equivale a un importo iniziale compreso tra 8 e 16 milioni di EUR.

Considerando che quanto più grave è la violazione all'interno della propria categoria, tanto più alto sarà probabilmente l'importo iniziale, l'autorità di controllo ritiene che, in ragione della gravità della violazione, l'importo iniziale debba essere di 12 milioni di EUR, ossia il 15 % del limite massimo di legge applicabile e lo 0,6 % del fatturato annuo dell'impresa.

Poiché il fatturato annuo dell'impresa è superiore a 500 milioni di EUR e si applica il massimo legale dinamico, le dimensioni dell'impresa si riflettono già nel massimo legale dinamico utilizzato per determinare l'importo iniziale. Di conseguenza, non viene applicato alcun ulteriore adeguamento.

L'autorità di controllo procede quindi al calcolo della sanzione pecuniaria sulla base del resto delle linee guida.