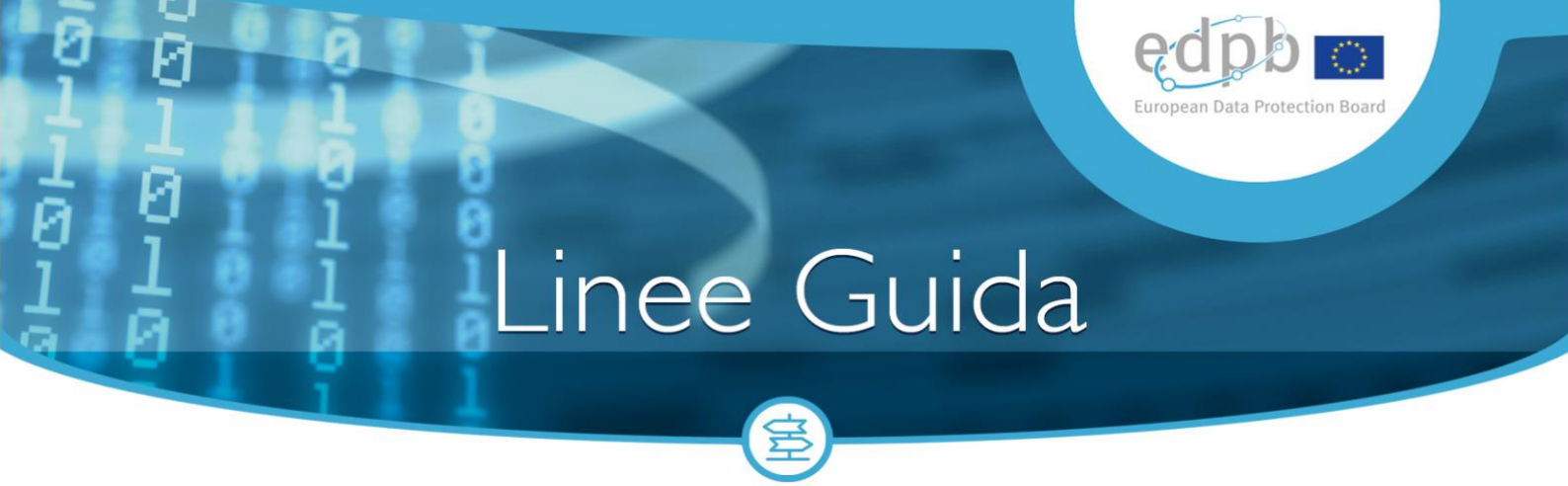

Linee guida 4/2019 sull'articolo 25

Protezione dei dati fin dalla progettazione e per impostazione predefinita

Versione 2.0

Adottate il 20 ottobre 2020

Cronologia delle versioni

Versione 1.0	13 novembre 2019	Adozione delle linee guida per consultazione pubblica
Versione 2.0	20 ottobre 2020	Adozione delle linee guida da parte dell'EDPB dopo la consultazione pubblica

Indice

Il comitato europeo per la protezione dei dati

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) n. 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 (in appresso: il «RGPD»),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificato dalla decisione del comitato misto SEE n. 154/2018, del 6 luglio 2018,

visto l'articolo 12 e l'articolo 22 del proprio regolamento interno,

HA ADOTTATO LE SEGUENTI LINEE GUIDA

Sintesi

In un mondo sempre più digitale, il rispetto dei requisiti della protezione dei dati fin dalla progettazione e della protezione per impostazione predefinita svolge un ruolo cruciale nel promuovere la tutela della vita privata e la protezione dei dati nella società. È pertanto fondamentale che i titolari del trattamento prendano sul serio questa responsabilità e si attengano agli obblighi del RGPD quando progettano i rispettivi trattamenti.

Le presenti linee guida forniscono orientamenti generali sull'obbligo di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita (in appresso «DPbDD») stabilito dall'articolo 25 del RGPD. La DPbDD costituisce un obbligo per tutti i titolari del trattamento, indipendentemente dalle dimensioni e dalla complessità del trattamento stesso. Per poter attuare la DPbDD, è di cruciale importanza che il titolare comprenda i principi della protezione dei dati nonché i diritti e le libertà dell'interessato.

L'obbligo principale consiste nel predisporre misure *adeguate* e garanzie necessarie che permettano un'*attuazione efficace* dei *principi della protezione dei dati* e, di conseguenza*, dei diritti e delle libertà degli interessati fin dalla progettazione e per impostazione predefinita*. L'articolo 25 prescrive gli elementi, sia della progettazione che dell'impostazione predefinita, di cui occorre tenere conto. Tali elementi saranno ulteriormente sviluppati nelle presenti linee guida.

L'articolo 25, paragrafo 1, prevede che il titolare debba prendere in considerazione la DPbDD fin dalla pianificazione di un nuovo trattamento. I titolari attuano la DPbDD *prima* del trattamento e poi *costantemente* durante il trattamento, verificando regolarmente l'efficacia delle misure e delle garanzie individuate. La DPbDD si applica altresì a sistemi preesistenti che trattino dati personali.

Le linee guida contengono inoltre indicazioni per un'efficace attuazione dei principi di protezione dei dati di cui all'articolo 5, elencando gli elementi chiave della progettazione e dell'impostazione predefinita nonché casi pratici a titolo illustrativo. Il titolare deve valutare l'adeguatezza delle misure consigliate nel contesto dello specifico trattamento.

L'EDPB fornisce raccomandazioni su come i titolari del trattamento, i responsabili del trattamento e i produttori possano cooperare per attuare la DPbDD. In particolare, incoraggia i titolari del trattamento nei singoli settori, i responsabili del trattamento e i produttori ad avvalersi della DPbDD quale

strumento per conseguire un vantaggio competitivo nella commercializzazione dei rispettivi prodotti presso i titolari del trattamento e gli interessati, oltre a incoraggiare tutti i titolari del trattamento a servirsi di certificazioni e codici di condotta.

1 AMBITO DI APPLICAZIONE

1. Le linee guida sono incentrate sull'attuazione, da parte dei titolari del trattamento, della DPbDD in virtù dell'obbligo di cui all'articolo 25 del RGPD.[1] Anche altri attori, quali i responsabili del trattamento e i produttori di prodotti, servizi e applicazioni (in prosieguo: «produttori»), che non sono direttamente contemplati dall'articolo 25, possono trovare utili queste linee guida in vista della creazione di prodotti e servizi conformi al RGPD che consentano ai titolari del trattamento di adempiere ai propri obblighi in materia di protezione dei dati.[2] Il considerando 78 del RGPD aggiunge che la DPbDD dovrebbe essere presa in considerazione nell'ambito degli appalti pubblici. Sebbene tutti i titolari abbiano il dovere di integrare la DPbDD nelle attività di trattamento, questa disposizione incentiva l'adozione dei principi di protezione dei dati nella misura in cui le pubbliche amministrazioni dovrebbero dare il buon esempio. Il titolare è tenuto ad assicurare il rispetto degli obblighi di DPbDD in relazione al trattamento svolto dai rispettivi responsabili e sub-responsabili e, pertanto, deve tenerne conto quando stipula contratti con tali soggetti.

2. Il requisito di cui all'articolo 25 obbliga i titolari a provvedere affinché la protezione dei dati sia integrata nel trattamento dei dati personali fin dalla progettazione e per impostazione predefinita durante l'intero ciclo di vita del trattamento. La DPbDD è un requisito anche per i sistemi di trattamento già esistenti all'entrata in vigore del RGPD; i titolari devono far sì che il trattamento sia aggiornato in modo coerente, in linea con il RGPD. Per maggiori informazioni su come mantenere un sistema esistente allineato alla DPbDD, cfr. il sottocapitolo 2.1.4 delle presenti linee guida. Il fulcro della disposizione è garantire una *adeguata* ed *efficace* protezione dei dati *fin dalla progettazione* e una protezione *per impostazione predefinita*, il che significa che i titolari dovrebbero essere in grado di dimostrare che incorporano nel trattamento le misure e le garanzie adeguate ad assicurare l'efficacia dei principi di protezione dei dati, dei diritti e delle libertà degli interessati.

3. Il capitolo 2 delle linee guida è incentrato su un'interpretazione dei requisiti previsti dall'articolo 25 ed esplora gli obblighi giuridici introdotti dalla disposizione. Il capitolo 3 fornisce esempi su come applicare la DPbDD nell'ambito di specifici principi di protezione dei dati.

4. Le linee guide esaminano l'opportunità di stabilire un meccanismo di certificazione per dimostrare la conformità con l'articolo 25 nel capitolo 4, mentre il capitolo 5 riguarda le modalità di verifica dell'attuazione dell'articolo 25 da parte delle autorità di controllo. Infine, le linee guida forniscono alle parti interessate ulteriori raccomandazioni su come attuare con successo la DPbDD. L'EDPB riconosce i problemi che le piccole e medie imprese (in prosieguo: «PMI») incontrano nel dare piena esecuzione agli obblighi della DPbDD e fornisce ulteriori raccomandazioni specifiche per le PMI nel capitolo 6.

[1] Le interpretazioni qui contenute si applicano anche all'articolo 20 della direttiva (UE) 2016/680 e all'articolo 27 del regolamento 2018/1725.

[2] Il considerando 78 del RGPD indica chiaramente questa necessità: «*In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati*.»

2 ANALISI DELL'ARTICOLO 25, PARAGRAFI 1 E 2: PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

5. L'obiettivo del presente capitolo è esplorare e fornire indicazioni sui requisiti relativi rispettivamente alla protezione dei dati fin dalla progettazione di cui all'articolo 25, paragrafo 1, e alla protezione dei dati per impostazione predefinita di cui all'articolo 25, paragrafo 2. La protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita sono concetti complementari che si rafforzano vicendevolmente. Gli interessati trarranno maggiori benefici dalla protezione dei dati per impostazione predefinita se verrà attuata contestualmente la protezione dei dati fin dalla progettazione, e viceversa.

6. La DPbDD è un requisito che si applica a tutti i titolari del trattamento, dalle piccole imprese alle imprese multinazionali. Di conseguenza, la complessità dell'attuazione della DPbDD può variare a seconda dello specifico trattamento. Indipendentemente dalle dimensioni, comunque, in tutti i casi si possono conseguire vantaggi per il titolare del trattamento e per l'interessato attraverso l'attuazione della DPbDD.

2.1 Articolo 25, paragrafo 1: protezione dei dati fin dalla progettazione

2.1.1 Obbligo del titolare del trattamento di attuare misure tecniche e organizzative adeguate e le necessarie garanzie nel trattamento

7. In linea con l'articolo 25, paragrafo 1, il titolare attua *misure* tecniche e organizzative *adeguate* che sono concepite per attuare i principi di protezione dei dati e integra nel trattamento le *necessarie garanzie* per adempiere ai requisiti e tutelare i diritti e le libertà degli interessati. Sia le misure adeguate che le necessarie garanzie intendono perseguire la medesima finalità di tutelare i diritti degli interessati e garantire che la protezione dei loro dati personali sia integrata nel trattamento.

8. Le espressioni *misure tecniche e organizzative* e *necessarie garanzie* possono essere intese in senso lato come qualsiasi metodo o mezzo che un titolare può impiegare nel trattamento. Con il termine *adeguate* si intende che le misure e le necessarie garanzie devono essere idonee a conseguire la finalità prevista, ossia devono attuare *efficacemente* i principi di protezione dei dati[3]. Il requisito di adeguatezza è quindi strettamente connesso al requisito di efficacia.

9. Per garanzia e misura tecnica od organizzativa s'intende tutto ciò che è compreso fra l'uso di soluzioni tecniche avanzate e la formazione di base del personale. Ne sono esempi idonei, a seconda del contesto e dei rischi associati al trattamento in questione, la pseudonimizzazione dei dati personali[4], la memorizzazione di dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico, la possibilità per gli interessati di intervenire nel trattamento, la fornitura di informazioni sulla conservazione dei dati personali, la disponibilità di sistemi di rilevamento di malware, la formazione dei dipendenti sull'«igiene informatica» di base, l'istituzione di sistemi di gestione della privacy e della sicurezza delle informazioni, l'obbligo contrattuale per i responsabili del trattamento di attuare prassi specifiche di minimizzazione dei dati, ecc.

[3] La questione relativa all'«efficacia» è affrontata di seguito al sottocapitolo 2.1.2.
[4] Definita all'articolo 4, paragrafo 5, del RGPD.

10. Standard, migliori prassi e codici di condotta riconosciuti da associazioni e da altri organismi che rappresentano categorie di titolari del trattamento possono essere utili ai fini della determinazione di misure adeguate. Tuttavia, il titolare deve verificare l'adeguatezza delle misure con riguardo allo specifico trattamento.

2.1.2 Volte ad attuare i principi di protezione dei dati in modo efficace e tutelare i diritti e le libertà degli interessati

11. I *principi di protezione dei dati* sono fissati all'articolo 5 (in prosieguo: «i principi»), i *diritti e le libertà degli interessati* sono i diritti e le libertà fondamentali di persone fisiche, e in particolare il loro diritto alla protezione dei dati personali, la cui tutela, a norma dell'articolo 1, paragrafo 2, è l'obiettivo del RGPD (in prosieguo «i diritti»)[5]. La loro precisa formulazione è contenuta nella Carta dei diritti fondamentali dell'UE. È essenziale che il titolare del trattamento comprenda il significato dei *principi* e dei *diritti* in quanto fondamento della protezione offerta dal RGPD e in particolare dall'obbligo della DPbDD.

12. Quando si attuano misure tecniche e organizzative adeguate, tali misure e le garanzie devono essere *concepite* in funzione dell'efficace attuazione di ognuno dei summenzionati principi e della conseguente tutela dei diritti.

Conseguire l'efficacia

13. L'efficacia è al cuore del concetto di protezione dei dati fin dalla progettazione. L'obbligo di attuare i principi in modo efficace comporta che i titolari del trattamento applichino le misure e le garanzie necessarie per la tutela di tali principi, al fine di garantire i diritti degli interessati. Ogni misura attuata deve produrre i risultati perseguiti per il trattamento e previsti dal titolare. Questa osservazione comporta due conseguenze.

14. In primo luogo, ciò significa che l'articolo 25 non richiede l'attuazione di misure tecniche e organizzative specifiche, bensì che le misure e le garanzie scelte siano specificamente connesse all'attuazione dei principi di protezione dei dati nello specifico trattamento. In tal senso, le misure e le garanzie devono essere concepite per essere robuste e il titolare del trattamento deve essere in grado di attuare ulteriori misure al fine di far fronte a un eventuale aumento dei rischi[6]. Il fatto che le misure siano o meno efficaci dipenderà quindi dal contesto del trattamento in questione e dalla valutazione di taluni elementi che devono essere presi in considerazione al momento di determinare i mezzi del trattamento. I suddetti elementi saranno trattati di seguito al sottocapitolo 2.1.3.

15. In secondo luogo, i titolari del trattamento devono essere in grado di dimostrare che i principi siano stati rispettati.

16. Le misure e le garanzie attuate devono conseguire l'effetto auspicato in termini di protezione dei dati e il titolare del trattamento deve disporre della documentazione relativa alle misure tecniche e

[5] Cfr. il considerando 4 del RGPD.

[6] «I principi fondamentali applicabili ai titolari del trattamento (ossia legittimità, minimizzazione dei dati, limitazione delle finalità, trasparenza, integrità dei dati, esattezza dei dati) dovrebbero rimanere gli stessi indipendentemente dal trattamento e dai rischi per gli interessati. Tuttavia, la dovuta considerazione della natura e dell'ambito di tale trattamento è sempre stata parte integrante dell'applicazione di questi principi affinché siano intrinsecamente scalabili». Gruppo di lavoro "Articolo 29", «Statement on the role of a risk-based approach in data protection legal frameworks», WP 218, 30 maggio 2014, pag. 3, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

organizzative.[7] A tale scopo, il titolare può definire idonei indicatori chiave di prestazione (ICP/KPI) per dimostrare l'efficacia. Un ICP è un valore misurabile scelto dal titolare che dimostra con quanta efficacia questi riesca a conseguire il suo obiettivo di protezione dei dati. Gli ICP possono essere *quantitativi*, come la percentuale di falsi positivi o falsi negativi, la riduzione dei reclami, la diminuzione del tempo di risposta quando gli interessati esercitano i loro diritti; o *qualitativi*, come le valutazioni di prestazione, l'uso di tabelle di classificazione o le valutazioni di esperti. In alternativa agli ICP, i titolari possono dimostrare che l'attuazione dei principi è efficace indicando i criteri alla base della loro valutazione dell'efficacia delle misure e delle garanzie scelte.

2.1.3 Elementi di cui tenere conto

17. L'articolo 25, paragrafo 1, elenca gli elementi di cui il titolare deve tenere conto allorché determina le misure riferite a un trattamento specifico. Di seguito sono fornite linee guida sull'applicazione di tali elementi nel processo di progettazione, compresa la progettazione delle impostazioni predefinite. Tutti questi elementi contribuiscono a determinare se una misura sia adeguata ai fini dell'efficace attuazione dei principi; pertanto nessuno fra essi costituisce un obiettivo da raggiungere in quanto tale, trattandosi piuttosto di fattori da considerare nel loro insieme in vista del raggiungimento dell'obiettivo perseguito.

2.1.3.1 Stato dell'arte

18. Il concetto di «stato dell'arte» è rinvenibile in diversi acquis dell'UE, ad es. in materia di tutela dell'ambiente o di sicurezza dei prodotti. Nel RGPD lo «stato dell'arte»[8] è menzionato non soltanto nell'articolo 32 in relazione alle misure di sicurezza[9][10], ma anche nell'articolo 25, cosicché questo parametro di riferimento è applicabile a tutte le misure tecniche e organizzative integrate nel trattamento.

19. Nell'ambito dell'articolo 25, il riferimento allo «stato dell'arte» impone l'obbligo ai titolari, allorché determinano le misure tecniche e organizzative adeguate, **di tenere conto degli attuali progressi compiuti dalla tecnologia** disponibile sul mercato. Ciò comporta che i titolari debbano essere a conoscenza dei progressi tecnologici e rimanere sempre aggiornati sulle opportunità e i rischi per il trattamento, in termini di protezione dei dati, derivanti dalle tecnologie e su come mettere in atto e aggiornare le misure e le garanzie che *assicurano un'attuazione efficace* dei principi e dei diritti degli interessati tenendo conto dell'evoluzione del panorama tecnologico.

20. Lo «stato dell'arte» è un concetto dinamico che non può essere definito staticamente con riguardo a un determinato momento, bensì dovrebbe essere oggetto di una valutazione *continuativa* nel contesto dei progressi tecnologici. Di fronte a tali progressi, un titolare può riscontrare che una misura in precedenza atta a conferire un livello di protezione adeguato ora non lo è più. Trascurare

[7] Cfr. i considerando 74 e 78.

[8] Cfr. decisione «Kalkar» della Corte costituzionale federale tedesca nel 1978: https://germanlawarchive.iuscomp.org/?p=67 che può offrire un fondamento metodologico per una definizione oggettiva del concetto. Su tale fondamento, lo "stato dell'arte" in termini di livello tecnologico si collocherebbe tra il livello tecnologico delle «conoscenze e ricerche scientifiche esistenti» e le più consolidate «regole tecniche generalmente riconosciute». Lo «stato dell'arte» può quindi essere identificato nel livello tecnologico di un servizio, una tecnologia o un prodotto come esistenti sul mercato e in grado di conseguire gli obiettivi individuati nel modo più efficace.

[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security

[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

l'aggiornamento sui progressi tecnologici potrebbe, quindi, comportare una mancata osservanza dell'articolo 25.

21. Il criterio dello «stato dell'arte» non si applica esclusivamente alle misure tecnologiche, ma anche a quelle organizzative. La mancanza di misure organizzative adeguate può ridurre o compromettere del tutto l'efficacia di una tecnologia scelta. Possono costituire esempi di misure organizzative l'adozione di politiche interne, la formazione aggiornata in materia di tecnologia, sicurezza e protezione dei dati nonché politiche di gestione e di *governance* della sicurezza informatica.

22. Quadri di riferimento standard, certificazioni, codici di condotta ecc. esistenti e riconosciuti possono contribuire a indicare l'attuale «stato dell'arte» nello specifico ambito di utilizzo. Qualora tali standard esistano e prevedano un livello elevato di protezione per l'interessato in conformità (o in misura superiore) ai requisiti giuridici, i titolari dovrebbero tenerne conto nella progettazione e nell'attuazione delle misure di protezione dei dati.

2.1.3.2 Costi di attuazione

23. Il titolare può tenere conto del costo di attuazione allorché sceglie e applica misure tecniche e organizzative adeguate e garanzie necessarie che mettono efficacemente in atto i principi al fine di tutelare i diritti degli interessati. Il costo si riferisce alle risorse in generale, compresi il tempo e le risorse umane.

24. Il fattore costo implica che il titolare non impieghi una quantità sproporzionata di risorse nel caso in cui esistano misure alternative, meno dispendiose, ma efficaci. Tuttavia, il costo di attuazione rappresenta un fattore di cui tenere conto nel realizzare la protezione dei dati fin dalla progettazione, e non già un motivo per astenersi dal realizzarla.

25. Le misure individuate devono pertanto garantire che l'attività di trattamento prevista dal titolare non comporti trattamenti di dati personali in violazione dei principi, indipendentemente dal costo di tali misure. I titolari devono essere in grado di gestire i costi complessivi per poter attuare efficacemente tutti i principi e, di conseguenza, tutelare i diritti.

2.1.3.3 Natura, ambito di applicazione, contesto e finalità del trattamento

26. I titolari devono tenere conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento allorché determinano le misure necessarie.

27. Questi fattori devono essere interpretati in modo coerente con il ruolo ad essi attribuito in altre disposizioni del RGPD, quali gli articoli 24, 32 e 35, allo scopo di integrare principi di protezione dei dati nella progettazione del trattamento.

28. In breve, il concetto di **natura** può essere inteso come le caratteristiche intrinseche[11] del trattamento. L'**ambito di applicazione** fa riferimento alla dimensione e all'ampiezza del trattamento. Il **contesto** riguarda le circostanze nel trattamento che possono influenzare le aspettative degli interessati, mentre la **finalità** si riferisce agli obiettivi del trattamento.

[11] Ne sono esempi le categorie particolari di dati personali, il processo decisionale automatizzato, i rapporti di forza asimmetrici, l'imprevedibilità del trattamento, la difficoltà per l'interessato di esercitare i propri diritti, ecc.

2.1.3.4 Rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento

29. Il RGPD adotta un approccio coerente basato sul rischio in molte delle sue disposizioni, negli articoli 24, 25, 32 e 35, al fine di individuare le misure tecniche e organizzative adeguate per tutelare le persone fisiche e i loro dati personali nonché adempiere ai requisiti del RGPD. I beni da tutelare sono sempre gli stessi (le persone fisiche, mediante la protezione dei loro dati personali), identici sono i rischi (per i diritti delle persone fisiche), e identiche le condizioni di cui tenere conto (natura, ambito di applicazione, contesto e finalità del trattamento).

30. Nell'analizzare i rischi ai fini del rispetto di quanto prevede l'articolo 25, il titolare deve individuare i rischi per i diritti degli interessati associati a una violazione dei principi, e determinare la loro probabilità e gravità al fine di attuare misure efficaci di mitigazione di tali rischi. Un esame sistematico e approfondito del trattamento è fondamentale nel corso della valutazione dei rischi. Per esempio, un titolare valuta i rischi specifici associati all'assenza di un consenso liberamente espresso, assenza che rappresenta una violazione del principio di liceità, nel trattamento dei dati personali di minori in quanto gruppo vulnerabile, ove non sussista alcun altro fondamento giuridico, e attua misure adeguate per contrastare e mitigare efficacemente i rischi associati a questo gruppo di interessati.

31. Le «Linee guida in materia di valutazione d'impatto sulla protezione dei dati» dell'EDPB[12], che descrivono un approccio utile a stabilire se un trattamento possa presentare un rischio elevato o meno per l'interessato, forniscono anche indicazioni su come valutare i rischi per la protezione dei dati ed effettuarne una valutazione. Tali linee guida possono altresì risultare utili durante la valutazione dei rischi in tutti gli articoli summenzionati, compreso l'articolo 25.

32. L'approccio basato sul rischio non esclude l'utilizzo di dati di riferimento, migliori prassi e standard. Questi potrebbero fornire strumenti utili ai titolari per affrontare rischi simili in situazioni analoghe (natura, ambito di applicazione, contesto e finalità del trattamento). Tuttavia, permane l'obbligo previsto dall'articolo 25 (nonché dagli articoli 24, 32 e 35, paragrafo 7, lettera c)), di tenere conto dei «*rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento*». Pertanto i titolari, anche ove supportati da tali strumenti, devono sempre effettuare caso per caso una valutazione dei rischi per la protezione dei dati insiti nell'attività di trattamento corrente e verificare l'efficacia delle misure e delle garanzie adeguate proposte. Potrebbe rendersi necessario anche effettuare una valutazione d'impatto sulla protezione dei dati, ovvero aggiornare una tale valutazione ove già esistente.

2.1.4 Aspetto temporale

2.1.4.1 Al momento di determinare i mezzi del trattamento

33. La protezione dei dati fin dalla progettazione deve essere attuata «*al momento di determinare i mezzi del trattamento*».

34. I «*mezzi del trattamento*» variano dagli elementi generali della progettazione di un trattamento fino a quelli dettagliati, e comprendono l'architettura, le procedure, i protocolli, il layout e l'aspetto.

[12] Gruppo di lavoro dell'articolo 29, «Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679», WP 248 rev. 01, 4 ottobre 2017, ec.europa.eu/newsroom/document.cfm?doc_id=47711 - approvate dall'EDPB.

35. Il *«momento di determinare i mezzi del trattamento»* si riferisce al periodo in cui il titolare decide come verrà effettuato il trattamento e il modo in cui si svolgerà, nonché i meccanismi che verranno impiegati per effettuarlo. È nel processo di adozione di queste decisioni che il titolare deve valutare le misure e le garanzie adeguate per attuare efficacemente i principi e i diritti degli interessati nel trattamento e considerare i rischi e gli elementi, quali lo stato dell'arte, il costo di attuazione, la natura, l'ambito di applicazione, il contesto e la finalità, ivi compreso il tempo per ottenere e poter utilizzare il software, l'hardware e i servizi per il trattamento dei dati.

36. La considerazione dei requisiti di DPbDD in fase precoce è di importanza cruciale per attuare con successo i principi e tutelare i diritti degli interessati. Inoltre, dal punto di vista del rapporto costi/benefici, è anche nell'interesse dei titolari tenere conto della DPbDD prima piuttosto che dopo, poiché potrebbe risultare difficile e costoso modificare in un momento successivo pianificazioni già definite e trattamenti già progettati.

2.1.4.2 All'atto del trattamento stesso (mantenimento e verifica dei requisiti in materia di protezione dei dati)

37. Una volta avviato il trattamento, il titolare è tenuto a mantenere su base continuativa la DPbDD, ossia a dare attuazione efficace e costante ai principi al fine di tutelare i diritti, tenendosi aggiornato sullo stato dell'arte, riesaminando il livello di rischio, ecc. La natura, l'ambito di applicazione e il contesto delle operazioni di trattamento, nonché il rischio possono mutare nel corso del trattamento, comportando per il titolare l'obbligo di verificare tali operazioni per mezzo di valutazioni e riesami periodici dell'efficacia delle misure e garanzie che ha scelto.

38. L'obbligo di mantenere, verificare e aggiornare, ove necessario, il trattamento si applica altresì ai sistemi preesistenti. Ciò implica che i sistemi progettati prima dell'entrata in vigore del RGPD devono essere sottoposti a verifiche e manutenzione per garantire l'applicazione di misure e garanzie che mettano in atto i principi e i diritti degli interessati in modo efficace, come indicato nelle presenti linee guida.

39. Tale obbligo si estende anche ai trattamenti svolti per mezzo di responsabili del trattamento. Le operazioni di trattamento effettuate dai responsabili dovrebbero essere regolarmente esaminate e valutate dai titolari per garantire che continuino a rispettare i principi e permettano ai titolari di adempiere ai rispettivi obblighi in tale contesto.

2.2 Articolo 25, paragrafo 2: protezione dei dati per impostazione predefinita

2.2.1 Siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento

40. In ambito informatico, per «impostazione predefinita» si intende comunemente un valore preesistente o preselezionato di un'impostazione configurabile che viene assegnato a un'applicazione informatica, a un programma informatico o a una periferica. Tali impostazioni sono anche chiamate «impostazioni di fabbrica», specialmente per i dispositivi elettronici.

41. Pertanto, l'espressione «per impostazione predefinita» nell'ambito del trattamento di dati personali si riferisce alle scelte compiute rispetto a valori di configurazione od opzioni di trattamento che sono rispettivamente fissati o prescritte in un sistema di trattamento (un'applicazione informatica, un servizio o una periferica o una procedura di trattamento manuale), tali da incidere sulla quantità dei dati personali raccolti, sulla portata del trattamento, sul periodo di conservazione e sull'accessibilità.

42. Il titolare dovrebbe scegliere, assumendosene la responsabilità, opzioni e impostazioni predefinite per il trattamento tali da garantire che venga effettuato per impostazione predefinita solo il trattamento strettamente necessario per conseguire la specifica e lecita finalità. In questo caso, i titolari dovrebbero affidarsi alla loro valutazione della necessità del trattamento in relazione alle basi giuridiche di cui all'articolo 6, paragrafo 1. Ciò significa che, per impostazione predefinita, il titolare non deve raccogliere più dati del necessario, non deve trattare i dati acquisiti oltre quanto sia necessario per le sue finalità né deve conservarli per un periodo superiore a quello necessario. Il requisito di base prevede che la protezione dei dati sia integrata nel trattamento per impostazione predefinita.

43. Il titolare è tenuto a definire in anticipo per quali finalità specifiche, esplicite e legittime i dati personali vengono raccolti e trattati.[13] Le misure devono, per impostazione predefinita, essere adeguate a garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento. Le linee guida dell'EDPS per valutare la necessità e la proporzionalità delle misure che limitano il diritto alla protezione dei dati personali possono essere utili anche per decidere quali dati sia necessario trattare per conseguire una finalità specifica[14] [15] [16].

44. Se il titolare utilizza software commerciali o di terzi, deve eseguire una valutazione dei rischi del prodotto e accertarsi che siano disattivate le funzioni che non hanno una base giuridica o non sono compatibili con le finalità previste del trattamento.

45. Le stesse considerazioni si applicano alle misure organizzative a sostegno dei trattamenti. Esse dovrebbero essere concepite, sin dall'inizio, per trattare soltanto la quantità minima di dati personali necessari per i trattamenti specifici. Ciò dovrebbe essere tenuto particolarmente in conto nello stabilire le modalità di accesso ai dati da parte di personale con ruoli ed esigenze di accesso diversi.

46. La nozione di «misure tecniche e organizzative» adeguate nel contesto della protezione dei dati per impostazione predefinita va dunque intesa nel senso già indicato al sottocapitolo 2.1.1, ma riferendola specificamente all'attuazione del principio della minimizzazione dei dati.

47. L'obbligo sopra illustrato di trattare solo i dati personali necessari per ciascuna finalità specifica si applica agli elementi indicati qui di seguito.

2.2.2 Perimetro dell'obbligo di minimizzazione dei dati

48. L'articolo 25, paragrafo 2, indica il perimetro dell'obbligo di minimizzazione dei dati, affermando che tale obbligo vale per la quantità di dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità dei dati.

[13] Articolo 5, paragrafo 1, lettere da b) a e) del RGPD.
[14] EDPS, «Guidelines on assessing the necessity and proportionality of measures that limit the right to data protection», 25 febbraio 2019, edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf
[15] Cfr. anche EDPS, «Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit» , https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en
[16] Per maggiori informazioni in merito alla necessità, cfr. il documento del Gruppo di lavoro "Articolo 29", «Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE», WP 217, 9 aprile 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf

2.2.2.1 Quantità dei dati personali raccolti

49. I titolari dovrebbero tenere conto sia del volume dei dati personali sia delle tipologie, delle categorie e del livello di dettaglio dei dati personali richiesti per le finalità del trattamento. Le loro scelte nella progettazione dovrebbero tenere conto dei maggiori rischi per i principi di integrità e riservatezza, di minimizzazione dei dati e della limitazione della conservazione connessi alla raccolta di grandi quantità di dati personali dettagliati, rispetto ai minori rischi associati alla raccolta di quantità minori di dati e/o di informazioni meno dettagliate sugli interessati. In ogni caso, le impostazioni predefinite non devono includere la raccolta di dati personali che non sono necessari per la specifica finalità del trattamento. In altre parole, se determinate categorie di dati personali sono superflue o se non sono necessari dati particolareggiati, perché sono sufficienti dati meno granulari, allora quelli in eccesso non sono raccolti.

50. Gli stessi requisiti di base valgono per i servizi indipendentemente dalla piattaforma o dal dispositivo in uso; è possibile raccogliere solo i dati personali necessari per la finalità considerata.

2.2.2.2 La portata del trattamento

51. I trattamenti[17] effettuati sui dati personali devono limitarsi a quanto è necessario. Molte operazioni di trattamento possono contribuire a realizzare la finalità perseguita dallo specifico trattamento. Nondimeno, il fatto che taluni dati personali siano necessari per conseguire una determinata finalità non significa che sia possibile sottoporre a trattamento tutte le tipologie di tali dati e con qualsiasi frequenza. I titolari dovrebbero inoltre fare attenzione a non ampliare i limiti delle «finalità compatibili» di cui all'articolo 6, paragrafo 4, e avere presente quali trattamenti possano corrispondere alle ragionevoli aspettative degli interessati.

2.2.2.3 Il periodo di conservazione

52. I dati personali raccolti non devono essere conservati se non sono necessari per la finalità del trattamento e non sussiste altra finalità compatibile né altro fondamento giuridico ai sensi dell'articolo 6, paragrafo 4. Qualsiasi conservazione dovrebbe essere obiettivamente giustificabile da parte del titolare del trattamento in quanto necessaria, in base al principio di responsabilizzazione.

53. Il titolare del trattamento deve limitare il periodo di conservazione all'arco di tempo necessario per il raggiungimento della specifica finalità. Se i dati personali non sono più necessari ai fini del trattamento, allora per impostazione predefinita sono cancellati o resi anonimi. La durata del periodo di conservazione dipenderà pertanto dalla finalità del trattamento in questione. Questo obbligo è direttamente correlato al principio di limitazione della conservazione di cui all'articolo 5, paragrafo 1, lettera e), e viene attuato per impostazione predefinita, ossia il titolare dovrebbe disporre di procedure sistematiche per la cancellazione o l'anonimizzazione dei dati, integrate nel trattamento.

[17] Ai sensi dell'articolo 4, paragrafo 2, del RGPD, il trattamento include 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.

54. L'anonimizzazione[18] dei dati personali costituisce un'alternativa alla cancellazione, a condizione che siano presi in considerazione tutti gli elementi contestuali pertinenti e che siano regolarmente valutate la probabilità e la gravità del rischio, compreso il rischio di re-identificazione.[19]

2.2.2.4 Accessibilità dei dati

55. Il titolare dovrebbe prevedere limitazioni quanto ai soggetti abilitati all'accesso e alla tipologia dell'accesso ai dati personali sulla base di una valutazione della necessità e assicurare che i dati personali siano realmente accessibili a chi ne ha bisogno in caso di necessità, ad esempio in situazioni critiche. I controlli dell'accesso dovrebbero essere effettuati per l'intero flusso di dati durante il trattamento.

56. L'articolo 25, paragrafo 2, stabilisce peraltro che non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica. Il titolare deve limitare l'accessibilità, per impostazione predefinita, e dare all'interessato la possibilità di intervenire prima di pubblicare o altrimenti rendere disponibili i suoi dati personali a un numero indefinito di persone fisiche.

57. Rendere disponibili i dati personali a un numero indefinito di persone potrebbe comportare una divulgazione dei dati ancora più ampia rispetto a quella inizialmente prevista, il che è particolarmente pertinente nel contesto di Internet e dei motori di ricerca; perciò i titolari dovrebbero, per impostazione predefinita, dare agli interessati l'opportunità di intervenire prima che i dati personali vengano messi a disposizione pubblicamente su Internet. Questo aspetto è particolarmente importante nel caso di minori e gruppi vulnerabili.

58. A seconda della base giuridica del trattamento, le modalità di intervento potrebbero variare in rapporto al contesto del trattamento (per esempio può essere necessario richiedere il consenso per la diffusione di dati personali o prevedere impostazioni di privacy affinché gli interessati stessi possano controllare l'accesso del pubblico).

59. Anche nell'ipotesi in cui i dati personali siano diffusi con il permesso e la consapevolezza di un interessato, ciò non significa che ogni altro titolare in grado di accedere ai dati personali possa trattarli liberamente per le proprie finalità; questi deve infatti disporre di una specifica base giuridica[20].

[18] Gruppo di lavoro dell'articolo 29, «Parere 05/2014 sulle tecniche di anonimizzazione», WP 216, 10 aprile 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_it.pdf

[19] Cfr. articolo 4, paragrafo 1, del RGDP, considerando 26 del RGDP, Gruppo di lavoro "Articolo 29", «Parere 05/2014 sulle tecniche di anonimizzazione». Si veda anche la sottosezione sulla «limitazione della conservazione» alla sezione 3 del presente documento, che indica la necessità da parte del titolare di garantire l'efficacia delle tecniche di anonimizzazione attuate.

[20] Cfr. causa Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia n. 931/13.

3 ATTUAZIONE DEI PRINCIPI DI PROTEZIONE NEL TRATTAMENTO DEI DATI PERSONALI UTILIZZANDO LA PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E LA PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

60. In tutte le fasi della progettazione delle attività di trattamento, compresi gli appalti, le gare di appalto, l'esternalizzazione, lo sviluppo, il supporto, la manutenzione, il collaudo, la conservazione, la cancellazione ecc., il titolare dovrebbe tenere conto e considerare i vari elementi della DPbDD, illustrati con esempi riportati in questo capitolo nel contesto dell'attuazione dei principi[21] [22] [23].

61. I titolari devono applicare i principi per attuare la DPbDD; tali principi, che includono la trasparenza, la liceità, la correttezza, la limitazione delle finalità, la minimizzazione dei dati, l'esattezza, la limitazione della conservazione, l'integrità, la riservatezza e la responsabilizzazione, sono indicati nell'articolo 5 e nel considerando 39 del RGPD. Per avere una conoscenza approfondita delle modalità di attuazione della DPbDD, si sottolinea l'importanza di comprendere il significato di ciascuno di questi principi.

62. Nella presentazione degli esempi su come rendere operativa la DPbDD, sono stati stilati elenchi degli **elementi chiave della DPbDD** per ciascuno dei principi. Gli esempi, pur sottolineando lo specifico principio di protezione dei dati in questione, possono sovrapporsi anche con altri principi strettamente connessi. L'EDPB evidenzia che gli elementi fondamentali e gli esempi presentati di seguito non sono né esaustivi né vincolanti, ma sono da intendersi come elementi di guida per ciascuno dei principi. I titolari devono valutare come garantire la conformità ai principi nel contesto del concreto trattamento in questione.

63. Benché questa sezione tratti nello specifico l'attuazione dei principi, il titolare dovrebbe altresì mettere in atto soluzioni *appropriate* ed *efficaci* per tutelare i diritti degli interessati, anche ai sensi del capo III del RGPD, ove ciò non sia già prescritto dai principi stessi.

64. Il principio di responsabilizzazione ha natura trasversale: prevede che il titolare risponda della scelta delle misure tecniche e organizzative necessarie.

3.1 Trasparenza[24]

65. Il titolare deve essere chiaro e trasparente con l'interessato su come raccoglierà, utilizzerà e condividerà i dati personali. Trasparenza significa consentire agli interessati di comprendere e, se necessario, avvalersi dei loro diritti come fissati negli articoli da 15 a 22. Il principio trova fondamento

[21] Si possono trovare maggiori esempi nel documento dell'autorità norvegese per la protezione dei dati. «Software Development with Data Protection by Design and by Default» (Sviluppo di software con protezione dei dati fin dalla progettazione e protezione per impostazione predefinita). 28 novembre 2017. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729

[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers

[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

[24] Approfondimenti su come interpretare il concetto di trasparenza si possono trovare nel documento del Gruppo di lavoro dell'articolo 29, «Linee guida sulla trasparenza ai sensi del regolamento 2016/679», WP 260 rev. 01, 11 aprile 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 - approvate dall'EDPB.

negli articoli 12, 13, 14 e 34. Le misure e le garanzie tese a sostenere il principio di trasparenza dovrebbero anche concorrere all'attuazione di questi articoli.

66. Gli elementi chiave della progettazione e dell'impostazione predefinita per quanto riguarda il principio della trasparenza possono includere:

- chiarezza – le informazioni sono fornite in un linguaggio chiaro e semplice, conciso e comprensibile;
- semantica – la comunicazione deve avere un significato chiaro per il pubblico a cui è rivolta;
- accessibilità – le informazioni sono facilmente accessibili per l'interessato;
- contestualità – le informazioni devono essere fornite al momento opportuno e nella forma adeguata;
- pertinenza – le informazioni devono essere pertinenti e applicabili all'interessato specifico;
- progettazione universale – le informazioni sono accessibili a tutti gli interessati, compreso l'utilizzo di linguaggi leggibili da una macchina per agevolare e automatizzare la leggibilità e la chiarezza;
- comprensibilità – gli interessati devono avere una buona comprensione di ciò che possono aspettarsi dal trattamento dei loro dati personali, in particolare quando si tratti di minori o di soggetti appartenenti ad altre categorie vulnerabili;
- multicanalità – le informazioni dovrebbero essere fornite attraverso canali e mezzi di comunicazione diversi, non solo quelli testuali, per aumentare la probabilità che raggiungano efficacemente l'interessato;
- approccio multilivello – le informazioni devono essere fornite secondo un approccio multilivello, in modo da garantire un equilibrio tra completezza e comprensibilità, rispecchiando le ragionevoli aspettative degli interessati.

Esempio[25]

Un titolare sta progettando una politica sulla privacy sul proprio sito web per conformarsi agli obblighi di trasparenza. La politica sulla privacy non deve contenere una quantità eccessiva di informazioni di difficile comprensione per l'interessato medio, deve essere scritta in un linguaggio chiaro e conciso e consentire all'utente del sito di comprendere le modalità di trattamento dei suoi dati personali. Il titolare fornisce pertanto informazioni secondo un approccio multilivello, evidenziando i punti più importanti. Vengono rese facilmente accessibili informazioni più dettagliate e sono messi a disposizione menu a discesa e collegamenti ad altre pagine per spiegare ulteriormente i vari punti e i concetti contenuti nella politica. Il titolare fa anche in modo che le informazioni siano fornite con più canali, prevedendo video che illustrano i punti più importanti delle informazioni in forma testuale. La sinergia tra le varie pagine è fondamentale per garantire che l'approccio multilivello non aumenti la confusione anziché ridurla.

La politica sulla privacy non deve essere di difficile accesso per gli interessati. Pertanto, viene messa a disposizione ed è visibile su tutte le pagine del sito in questione di modo che l'interessato acceda sempre alle informazioni con un semplice clic. Le informazioni fornite sono altresì concepite in conformità con le migliori prassi e standard di progettazione universale per renderle accessibili a tutti.

Inoltre, le informazioni necessarie dovrebbero essere messe a disposizione nel giusto contesto e al momento adeguato. Poiché il titolare svolge molte operazioni di trattamento impiegando i dati raccolti sul sito, non è sufficiente che pubblichi una politica generale sulla privacy soltanto sul sito per

[25] L'autorità francese per la protezione dei dati ha pubblicato diversi esempi che illustrano le migliori prassi su come informare gli utenti nonché altri principi di trasparenza: https://design.cnil.fr/en/

conformarsi agli obblighi di trasparenza. Il titolare progetta quindi un flusso di informazioni che fornisce all'interessato le informazioni pertinenti nei contesti adeguati utilizzando ad es. snippet informativi o pop up. Ad esempio, quando si chiede all'interessato di accedere ai suoi dati personali, il titolare lo informa sulle modalità del trattamento spiegando perché tali dati siano necessari per quest'ultimo.

3.2 Liceità

67. Il titolare deve identificare una base giuridica valida per il trattamento dei dati personali. Le misure e le garanzie dovrebbero concorrere all'obbligo di assicurare che l'intero ciclo di vita del trattamento sia in linea con la pertinente base giuridica.

68. Tra gli elementi principali della progettazione e dell'impostazione predefinita ai fini della liceità possono figurare:
    - pertinenza –al trattamento è applicata la corretta base giuridica;
    - differenziazione[26] – occorre differenziare la base giuridica utilizzata per ciascuna attività di trattamento;
    - finalità specifica – la corretta base giuridica deve essere chiaramente connessa alla specifica finalità di trattamento[27];
    - necessità – il trattamento deve essere necessario e non soggetto a condizioni affinché la sua finalità sia lecita;
    - autonomia – all'interessato dovrebbe essere garantito il massimo grado possibile di autonomia in relazione al controllo dei propri dati personali nel quadro della base giuridica;
    - ottenimento del consenso – il consenso deve essere liberamente espresso, specifico, informato e inequivocabile[28]. Occorre considerare in particolare la capacità dei minori di fornire un consenso informato;
    - revoca del consenso – se il consenso è la base giuridica, il trattamento dovrebbe agevolarne la revoca. La revoca del consenso deve essere altrettanto facile quanto la sua prestazione. In caso contrario, il meccanismo del consenso attuato dal titolare non è conforme al RGPD[29];
    - bilanciamento degli interessi – se la base giuridica è costituita da interessi legittimi, il titolare deve effettuare un bilanciamento ponderato, considerando in particolare lo squilibrio tra i rapporti di forza, specificamente nel caso di minori e altri gruppi vulnerabili. Devono essere previste misure e garanzie per attenuare l'impatto negativo sugli interessati;
    - predeterminazione – la base giuridica è stabilita prima che il trattamento abbia luogo;
    - cessazione – se la base giuridica non è più valida, il trattamento cessa di conseguenza;
    - adeguamento – se vi è una modifica valida della base giuridica per il trattamento, quest'ultimo deve essere adeguato in base alla nuova base giuridica[30];

[26] EDPB, «Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati», versione 2.0, 8 ottobre 2019, edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_it.pdf

[27] Cfr. sezione sulla limitazione delle finalità di seguito.

[28] Cfr. le Linee guida 05/2020 sul consenso a norma del regolamento 2016/679, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_it

[29] Cfr. le Linee guida 05/2020 sul consenso a norma del regolamento 2016/679, pag. 24, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_it

[30] Se il consenso è la base giuridica originaria, cfr. le Linee guida 05/2020 sul consenso a norma del regolamento 2016/679, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_it

- attribuzione di responsabilità – ogniqualvolta sia prevista la contitolarità del trattamento, le parti devono suddividersi in modo chiaro e trasparente le rispettive responsabilità nei confronti dell'interessato ed elaborare le misure del trattamento conformemente a tale attribuzione di responsabilità.

Esempio

Una banca intende offrire un servizio per migliorare l'efficienza nella gestione delle richieste di mutuo. L'idea alla base del servizio è che la banca può recuperare i dati sul cliente direttamente dalle amministrazioni tributarie, previa autorizzazione di queste ultime. Questo esempio non tiene conto del trattamento di dati personali provenienti da altre fonti.

Ottenere dati personali sulla situazione finanziaria dell'interessato è necessario per espletare formalità su richiesta dell'interessato prima di sottoscrivere un contratto di mutuo[31]. Tuttavia, raccogliere dati personali direttamente dall'amministrazione tributaria non è considerato necessario, perché il cliente può sottoscrivere un contratto fornendo per proprio conto le informazioni provenienti dall'amministrazione tributaria. Anche se la banca potrebbe avere un interesse legittimo ad acquisire la documentazione direttamente presso le competenti autorità, ad esempio per garantire un'efficace elaborazione della richiesta di mutuo, fornire alle banche l'accesso diretto ai dati personali dei richiedenti comporta un rischio connesso all'uso o al potenziale abuso dei diritti di accesso.

Nell'attuazione del principio di liceità, il titolare comprende che, in questo contesto, non può utilizzare il criterio della «necessità a fini contrattuali» per la parte del trattamento che prevede la raccolta dei dati personali direttamente dalle amministrazioni tributarie. Il fatto che questo specifico trattamento presenti un rischio, che vede l'interessato assumere un ruolo meno attivo nel trattamento dei propri dati, è un fattore rilevante nella valutazione della liceità del trattamento stesso. La banca conclude che questa parte del trattamento deve fondarsi su un'altra base giuridica pertinente. Nello Stato membro in cui ha sede il titolare del trattamento la normativa in vigore permette alla banca di raccogliere informazioni direttamente presso le autorità tributarie, ove l'interessato vi abbia previamente acconsentito.

La banca presenta quindi le informazioni relative al trattamento sulla piattaforma per la richiesta online in modo tale da consentire agli interessati di comprendere facilmente quali trattamenti siano necessitati e quali siano opzionali. Le opzioni di trattamento, per impostazione predefinita, non consentono di ricavare i dati direttamente da altri fonti se non dall'interessato, e l'opzione per la raccolta diretta delle informazioni è presentata in modo tale da non dissuadere l'interessato dall'astenersi. Qualsiasi consenso fornito per la raccolta dei dati direttamente presso altri titolari rappresenta un diritto di accesso temporaneo a un insieme specifico di informazioni.

Ogni consenso fornito è trattato elettronicamente in modo documentabile e gli interessati dispongono di un meccanismo di facile utilizzo per controllare ciò a cui hanno dato il consenso e revocare tale consenso.

Il titolare ha valutato preventivamente tali requisiti della DPbDD e include tutti questi criteri nelle specifiche del capitolato per l'appalto di fornitura della piattaforma. Il titolare comprende che se non include i requisiti della DPbDD nel capitolato d'appalto, potrebbe essere troppo tardi o troppo costoso attuare la protezione dei dati successivamente.

[31] Cfr. articolo 6, paragrafo 1, lettera b), del RGPD.

3.3 Correttezza

69. La correttezza è un principio di natura trasversale secondo cui i dati personali non devono essere trattati in modo ingiustificatamente dannoso, illegittimamente discriminatorio, imprevisto o fuorviante per l'interessato. Le misure e le garanzie che attuano il principio della correttezza supportano anche i diritti e le libertà degli interessati, in particolare il diritto all'informazione (trasparenza), il diritto di intervenire nel trattamento (accesso, cancellazione, portabilità dei dati, rettificazione) e il diritto di limitazione del trattamento (il diritto a non essere sottoposto a un processo decisionale automatizzato e non subire discriminazioni nel contesto di tali processi).

70. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi alla correttezza, possono figurare:
    - autonomia – agli interessati dovrebbe essere garantito il massimo grado possibile di autonomia nel determinare l'utilizzo cui sono sottoposti i loro dati personali, nonché l'ambito di applicazione e le condizioni di tale utilizzo o trattamento;
    - interazione – gli interessati devono essere in grado di comunicare ed esercitare i propri diritti in relazione ai dati personali trattati dal titolare;
    - aspettativa – il trattamento dovrebbe corrispondere alle aspettative ragionevoli degli interessati;
    - nessuna discriminazione – il titolare non discrimina ingiustamente gli interessati;
    - nessuno sfruttamento – il titolare non deve sfruttare le esigenze o le vulnerabilità degli interessati;
    - libertà di scelta – il titolare non dovrebbe «catturare» (*lock-in*) i propri utenti in modo scorretto. Qualora un servizio che prevede il trattamento di dati personali abbia natura proprietaria, gli utenti potrebbero essere "catturati" rispetto a tale servizio, il che può essere scorretto qualora pregiudichi la possibilità per gli interessati di esercitare il diritto alla portabilità dei dati ai sensi dell'articolo 20;
    - equilibrio dei rapporti di forza - tale equilibrio dovrebbe essere un obiettivo chiave della relazione tra titolare e interessato. Occorre evitare gli squilibri nei rapporti di forza e, qualora ciò non sia possibile, è necessario individuarli e tenerne conto al fine di adottare adeguate contromisure;
    - assenza di trasferimento di rischi – i titolari non dovrebbero trasferire i rischi di impresa agli interessati;
    - assenza di prassi ingannevoli – le informazioni e le opzioni relative al trattamento dei dati devono essere fornite in modo obiettivo e neutrale, evitando formulazioni o meccanismi ingannevoli o manipolatori;
    - rispetto dei diritti – il titolare deve rispettare i diritti fondamentali degli interessati e attuare misure e garanzie adeguate, senza comprimere tali diritti se non ove ciò sia espressamente giustificato dalla legge;
    - eticità – il titolare dovrebbe guardare all'impatto complessivo del trattamento sui diritti e sulla dignità delle persone;
    - veridicità – il titolare deve dichiarare le proprie modalità di trattamento dei dati personali e deve agire secondo quanto dichiarato in merito, senza fuorviare gli interessati;

- intervento umano – il titolare deve integrare un intervento umano *qualificato* in grado di individuare le distorsioni (*bias*) che le macchine possono generare, conformemente al diritto di non essere sottoposto a un processo decisionale automatizzato di cui all'articolo 22[32];
- imparzialità degli algoritmi – valutare periodicamente se gli algoritmi funzionino in linea con le finalità e adeguarli per attenuare le distorsioni individuate e garantire l'imparzialità del trattamento. Gli interessati dovrebbero essere informati in merito al trattamento dei dati personali attraverso algoritmi che ne facciano oggetto di analisi o previsioni, per esempio riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti[33].

Esempio 1

Un titolare gestisce un motore di ricerca che tratta per lo più dati personali generati dagli utenti. Il titolare trae beneficio dall'avere grandi quantità di dati personali e dal poterli usare per offrire pubblicità mirata; pertanto, intende esercitare un'influenza sugli interessati per rendere possibile una raccolta e un utilizzo più ampi dei loro dati personali. Il consenso sarà raccolto presentando all'interessato diverse opzioni di trattamento.

Nell'attuazione del principio della correttezza, tenendo conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, il titolare comprende che non può presentare le opzioni in modo da indurre l'interessato a consentirgli di raccogliere più dati personali di quanto avverrebbe se le opzioni fossero presentate in modo corretto e neutrale. Ciò significa che il titolare non può presentare le opzioni di trattamento in modo tale da rendere difficile per gli interessati astenersi dalla condivisione dei propri dati ovvero modificare le proprie impostazioni di privacy e limitare il trattamento. Questi sono esempi di *dark pattern* (modelli oscuri) contrari allo spirito dell'articolo 25. Le opzioni predefinite per il trattamento non devono essere invasive e la scelta di consentire un ulteriore trattamento dovrebbe essere presentata in modo da non esercitare pressione sull'interessato affinché presti il suo consenso. Pertanto, il titolare presenta con identica visibilità le opzioni connesse alla prestazione ovvero al rifiuto del consenso, descrivendo accuratamente le conseguenze per l'interessato nei rispettivi casi.

Esempio 2

Un altro titolare tratta dati personali per fornire un servizio di streaming, in cui gli utenti possono scegliere tra il normale abbonamento di qualità standard e l'abbonamento premium di qualità più elevata. Come parte dell'abbonamento premium è prevista la prioritizzazione del servizio clienti.

Con riguardo al principio della correttezza, questo servizio prioritario concesso agli abbonati premium non può dar luogo a discriminazioni nei confronti dei normali abbonati in relazione all'esercizio dei loro diritti ai sensi dell'articolo 12 del RGPD. Ciò significa che, sebbene gli abbonati premium ricevano un

[32] Cfr. le Linee guida in materia di processi decisionali automatizzati relativi alle persone fisiche e profilazione ai fini del regolamento 2016/679, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826

[33] Cfr. il considerando 71 del RGPD.

servizio prioritario, tale priorità non può comportare l'assenza di misure adeguate a rispondere alle richieste dei normali abbonati senza indebito ritardo, e in ogni caso entro un mese dalla ricezione.

I clienti premium possono pagare per ricevere un servizio migliore, ma tutti gli interessati devono godere di condizioni identiche e non discriminatorie ai fini dell'esercizio dei diritti e delle libertà di cui all'articolo 12.

3.4 Limitazione delle finalità[34]

71. Il titolare deve raccogliere dati per finalità specifiche, esplicite e legittime e non trattarli ulteriormente in modo incompatibile con le finalità per le quali sono stati raccolti.[35] La progettazione del trattamento dovrebbe pertanto essere definita da quanto necessario per conseguire le finalità. In caso di trattamento ulteriore, il titolare deve prima assicurarsi che tale trattamento abbia finalità compatibili con quelle originarie e progettarlo di conseguenza. La compatibilità o meno della nuova finalità è valutata in base ai criteri di cui all'articolo 6, paragrafo 4.

72. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi alla limitazione delle finalità, possono figurare:
    - predeterminazione – le finalità legittime sono determinate prima della progettazione del trattamento;
    - specificità – le finalità sono specificate ed esplicite in merito al motivo per cui i dati personali vengono trattati;
    - orientamento in base alla finalità – la finalità del trattamento dovrebbe orientare la progettazione del trattamento e determinarne i limiti;
    - necessità – la finalità determina quali sono i dati personali necessari per il trattamento;
    - compatibilità – qualsiasi nuova finalità deve essere compatibile con la finalità originaria per la quale sono stati raccolti i dati e orientare le modifiche rilevanti nella progettazione;
    - limitazione di trattamenti ulteriori – il titolare non dovrebbe collegare set di dati o effettuare ulteriori trattamenti per finalità diverse che sono incompatibili;
    - limitazioni del riutilizzo – il titolare dovrebbe adottare misure tecniche, tra cui l'hashing e la cifratura, per limitare la possibilità di riutilizzare i dati personali. Il titolare dovrebbe inoltre prevedere misure organizzative, quali politiche e obblighi contrattuali, che limitino il riutilizzo di dati personali;
    - riesame periodico – il titolare dovrebbe verificare periodicamente se il trattamento sia necessario per le finalità per le quali sono stati raccolti i dati e testare la progettazione di tale trattamento con riguardo al principio di limitazione delle finalità.

Esempio

Il titolare tratta i dati personali dei suoi clienti. La finalità del trattamento è l'esecuzione del contratto, ossia poter fornire i beni all'indirizzo corretto e ottenere il pagamento. I dati personali conservati sono lo storico degli acquisti, il nome, l'indirizzo fisico, l'indirizzo di posta elettronica e il numero di telefono.

[34] Il Gruppo di lavoro "Articolo 29" ha elaborato linee guida per comprendere il principio della limitazione delle finalità ai sensi della direttiva 95/46/CE. Sebbene il parere non sia adottato dall'EDPB, può tuttavia essere pertinente in quanto il principio è formulato in termini identici a quelli di cui al RGPD. Gruppo di lavoro"Articolo 29", «Opinion 03/2013 on purpose limitation», WP 203, 2 aprile 2013, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_it.pdf

[35] Articolo 5, paragrafo 1, lettera b) del RGPD.

Il titolare sta valutando l'acquisto di un prodotto per la gestione dei rapporti con la clientela che consolida tutti i dati sui clienti relativi alle vendite, al marketing e all'assistenza alla clientela. Il prodotto consente di conservare tutte le chiamate, le attività, i documenti, le e-mail e le campagne di marketing per avere una panoramica a 360 gradi del singolo cliente. Inoltre, esso è in grado di analizzare automaticamente il potere di acquisto dei clienti utilizzando le informazioni pubbliche. La finalità dell'analisi è consentire un migliore orientamento delle attività promozionali, che non rientrano nell'originaria finalità legittima del trattamento.

Per conformarsi al principio della limitazione delle finalità, il titolare impone al fornitore del prodotto di mappare le diverse attività di trattamento che utilizzano i dati personali per le finalità che gli interessano.

Dopo aver ricevuto i risultati della mappatura, il titolare valuta se la nuova finalità di marketing e quella di pubblicità mirata siano compatibili con le finalità originarie definite in fase di acquisizione dei dati e se esista una base giuridica sufficiente per il relativo trattamento. Se l'esito della valutazione non è positivo, il titolare non procederà all'utilizzo delle rispettive funzionalità. In alternativa, il titolare potrebbe scegliere di non effettuare la valutazione e rinunciare semplicemente ad avvalersi delle funzionalità del prodotto descritte.

3.5 Minimizzazione dei dati

73. Solo i dati personali che sono adeguati, pertinenti e limitati a quanto **necessario** per la finalità sono sottoposti a trattamento.[36] Di conseguenza, il titolare deve predeterminare quali caratteristiche e parametri dei sistemi di trattamento nonché quali funzioni di supporto siano consentiti. La minimizzazione dei dati realizza e rende operativo il principio di necessità. Nel proseguire il trattamento, il titolare dovrebbe valutare periodicamente se i dati personali trattati siano ancora adeguati, pertinenti e necessari o se occorra cancellarli o renderli anonimi.

74. I titolari dovrebbero, in primo luogo, valutare se abbiano bisogno o meno di trattare i dati personali per le finalità che interessano loro. Il titolare dovrebbe verificare se sia possibile conseguire le finalità pertinenti trattando una quantità inferiore di dati personali o disponendo di dati personali meno dettagliati o aggregati, oppure senza doverli trattare affatto[37]. Questa verifica dovrebbe essere eseguita prima di qualunque trattamento, ma potrebbe anche aver luogo in qualsiasi momento nel corso del ciclo di vita del trattamento. Ciò è altresì conforme con l'articolo 11.

75. La minimizzazione può anche riferirsi al grado di identificazione. Se la finalità del trattamento non richiede che i set di dati definitivi si riferiscano a una persona fisica identificata o identificabile (come nelle statistiche), ma lo richiede il trattamento iniziale (ad es. prima dell'aggregazione dei dati), il titolare cancella o rende anonimi i dati personali non appena non sia più necessaria l'identificazione. Oppure, se l'identificazione continua a essere necessaria per le altre attività di trattamento, i dati personali dovrebbero essere pseudonimizzati al fine di ridurre i rischi per i diritti degli interessati.

76. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi alla minimizzazione dei dati, possono figurare:

[36] Articolo 5, paragrafo 1, lettera c) del RGPD.
[37] Il considerando 39 del RGPD stabilisce quanto segue: «[...] I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi.»

- evitare il trattamento dei dati – evitare del tutto il trattamento dei dati personali quando ciò sia possibile per la finalità pertinente;
- limitazione – la quantità di dati personali raccolti va limitata a ciò che è necessario per la specifica finalità;
- limitazione dell'accesso – definire il trattamento dei dati in modo tale che un numero minimo di persone abbia bisogno di accedere ai dati personali per esercitare le proprie funzioni, e limitare l'accesso di conseguenza;
- pertinenza – i dati personali devono essere pertinenti al trattamento in questione e il titolare deve essere in grado di dimostrare tale pertinenza;
- necessità – ogni categoria di dati personali deve essere necessaria per le finalità specificate e dovrebbe essere trattata soltanto se non è possibile conseguire la specifica finalità con altri mezzi;
- aggregazione – quando possibile, utilizzare dati aggregati;
- pseudonimizzazione – pseudonimizzare i dati personali quando non è più necessario disporre di dati personali identificabili e memorizzare le chiavi di identificazione separatamente;
- anonimizzazione e cancellazione – se i dati personali non sono necessari per la specifica finalità (o non lo sono più), devono essere resi anonimi o cancellati;
- flusso dei dati – il flusso dei dati deve essere efficiente così da non creare copie ulteriori rispetto a quanto necessario;
- «stato dell'arte» – il titolare dovrebbe applicare tecnologie aggiornate e adeguate per evitare o minimizzare il trattamento dei dati.

Esempio 1

Una libreria intende aumentare le entrate vendendo i libri online. Il proprietario vuole creare un modello standardizzato per il procedimento di ordinazione. Per garantire che i clienti forniscano tutte le informazioni richieste, il proprietario della libreria rende obbligatori tutti i campi del modulo (se non si compilano tutti i campi il cliente non può effettuare l'ordine). Inizialmente, il proprietario del negozio online usa un modulo di contatto standard in cui si chiedono al cliente informazioni quali la data di nascita, il numero di telefono e l'indirizzo di casa. Tuttavia, i campi del modulo non sono tutti necessari per l'acquisto e la spedizione dei libri. In questo caso specifico, se l'interessato paga il prodotto in anticipo, la sua data di nascita e il suo numero di telefono non sono necessari per l'acquisto. Ciò significa che questi campi del modulo web non devono essere necessariamente compilati per ordinare il prodotto, a meno che il titolare possa dimostrare chiaramente che la loro compilazione è altrimenti indispensabile, e per quali motivi. Inoltre, vi sono situazioni in cui l'indirizzo non è necessario. Per esempio, quando si ordina un e-book, il cliente può scaricare il prodotto direttamente sul proprio dispositivo.

Il proprietario decide quindi di creare due moduli web: uno per ordinare i libri con un campo contenente l'indirizzo del cliente e un altro per ordinare gli e-book senza il campo dell'indirizzo.

Esempio 2

Un'azienda di trasporto pubblico intende raccogliere informazioni statistiche basate sui tragitti dei viaggiatori che consentano di operare scelte adeguate sulle modifiche degli orari del trasporto pubblico

e sugli itinerari dei treni. I passeggeri devono passare il loro biglietto attraverso un lettore ogni volta che salgono o scendono da un mezzo di trasporto. Sulla base di una valutazione dei rischi per i diritti e le libertà dei passeggeri legati alla raccolta dei loro itinerari di viaggio, il titolare stabilisce che è possibile identificare i passeggeri ove questi risiedano o lavorino in aree scarsamente popolate attraverso l'identificazione del singolo itinerario, desumibile grazie all'identificativo del biglietto. Poiché tale identificativo non è necessario per ottimizzare gli orari del trasporto pubblico e gli itinerari dei treni, il titolare non lo conserva. Una volta terminato il tragitto, il titolare conserva solo i singoli itinerari di viaggio in modo da non poter identificare i tragitti collegati a uno specifico biglietto, memorizzando soltanto le informazioni sui singoli percorsi di viaggio.

Qualora si manifesti comunque il rischio di identificare una persona esclusivamente a partire dal suo itinerario di viaggio , il titolare attua misure statistiche per ridurre tale rischio, per esempio eliminando le informazioni sul luogo di partenza e di destinazione.

Esempio 3

Un corriere intende valutare l'efficacia delle sue consegne in termini di tempistiche, programmazione del lavoro e consumo di carburante. Per raggiungere questo obiettivo, il corriere deve trattare una serie di dati personali relativi sia ai dipendenti (conducenti) sia ai clienti (indirizzi, articoli da spedire, ecc.). Questo trattamento comporta rischi sia in termini di sorveglianza dei dipendenti, per i quali occorrono specifiche salvaguardie di natura giuridica, sia in termini di rilevamento delle abitudini dei clienti attraverso la conoscenza dei prodotti consegnati nel tempo. Tali rischi possono essere significativamente ridotti tramite una pseudonimizzazione adeguata dei dati relativi a dipendenti e clienti. In particolare, con una rotazione frequente dei codici di pseudonimizzazione e focalizzandosi su macro-aree anziché sui singoli indirizzi, si realizza un'efficace minimizzazione dei dati e il titolare può concentrarsi esclusivamente sul processo di spedizione e sulla finalità di ottimizzazione delle risorse senza sconfinare nel monitoraggio dei comportamenti dei singoli (clienti o dipendenti).

Esempio 4

Un ospedale sta acquisendo dati sui pazienti nell'ambito di un sistema informativo ospedaliero (cartelle cliniche elettroniche). Il personale ospedaliero ha bisogno di accedere ai fascicoli dei pazienti per poter adottare decisioni informate in merito alla loro assistenza e alle cure, nonché al fine di documentare tutte le attività effettuate in materia di diagnosi, assistenza e cura. Per impostazione predefinita, l'accesso è consentito solo ai membri del personale medico cui sia affidata la cura del rispettivo paziente nel reparto specifico cui questi è stato assegnato. Il gruppo di persone che ha accesso al fascicolo di un paziente viene ampliato se nella cura sono coinvolti altri reparti o unità diagnostiche. Una volta dimesso il paziente e completata la fatturazione, l'accesso è limitato a un piccolo gruppo di dipendenti, per ciascun reparto specifico, che risponde alle richieste di informazioni mediche o di consultazione effettuate da altri fornitori di servizi medici, previa autorizzazione del paziente in questione.

3.6 Esattezza

77. I dati personali devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati[38].

78. I requisiti dovrebbero essere esaminati in relazione ai rischi e alle conseguenze derivanti dall'utilizzo concreto dei dati. I dati inesatti potrebbero costituire un rischio per i diritti e le libertà degli interessati, ad esempio quando conducono a una diagnosi errata o a un trattamento errato di un protocollo sanitario, oppure un'immagine errata di una persona può portare a decisioni erronee sia attraverso processi manuali sia attraverso un processo decisionale automatizzato o l'impiego di tecniche di intelligenza artificiale.

79. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi all'esattezza, possono figurare:
    - fonte dei dati – le fonti dei dati personali dovrebbero essere affidabili in termini di esattezza dei dati;
    - grado di esattezza – ciascun elemento dei dati personali deve essere il più esatto possibile in base alle necessità delle finalità specifiche;
    - esattezza misurabile – occorre ridurre il numero di falsi positivi/negativi, per esempio le distorsioni generate nell'ambito delle decisioni automatizzate e dell'intelligenza artificiale;
    - verifica – a seconda della natura dei dati, e in relazione alla frequenza delle relative modifiche, il titolare dovrebbe verificare la correttezza dei dati personali presso l'interessato prima del trattamento e nelle sue diverse fasi (per esempio rispetto ai requisiti di età);
    - cancellazione/rettifica – il titolare dovrebbe cancellare o rettificare tempestivamente i dati inesatti e, in particolare, agevolare questa procedura se gli interessati sono o erano minori e successivamente desiderano eliminare i suddetti dati personali[39];
    - evitare la propagazione di errori – i titolari dovrebbero attenuare l'effetto di un errore accumulato nella catena di trattamento;
    - accesso – gli interessati dovrebbero ricevere informazioni sui dati personali e disporre di un accesso efficace agli stessi, ai sensi degli articoli da 12 a 15 del RGPD, per controllarne l'esattezza e apportare le rettifiche ove necessario;
    - esattezza permanente – i dati personali dovrebbero essere esatti in tutte le fasi del trattamento e nelle fasi critiche dovrebbero essere effettuate verifiche di esattezza;
    - aggiornamento – i dati personali sono aggiornati qualora ciò sia necessario per la specifica finalità;
    - progettazione dei dati – impiego di caratteristiche organizzative e tecnologiche di progettazione per ridurre le eventuali inesattezze, per esempio proponendo scelte concise e predeterminate anziché campi a testo libero.

Esempio 1

Una compagnia assicurativa desidera servirsi dell'intelligenza artificiale (IA) per eseguire la profilazione dei clienti che acquistano le polizze, utilizzandola quale fondamento del suo processo decisionale in fase di calcolo del rischio assicurativo. Nel determinare come sviluppare tali soluzioni di IA, la compagnia stabilisce i mezzi del trattamento: in tale contesto dovrebbe considerare la protezione dei dati fin dalla progettazione al momento di scegliere un'applicazione di IA da un fornitore e decidere come utilizzarla.

[38] Articolo 5, paragrafo 1, lettera d), del RGPD.
[39] Cfr. il considerando 65.

Nello stabilire come utilizzare l'IA, il titolare dovrebbe disporre di dati esatti per ottenere risultati precisi. Pertanto, il titolare dovrebbe garantire che i dati utilizzati per addestrare l'IA siano esatti.

Presupponendo che la compagnia assicurativa abbia una base giuridica valida per addestrare l'IA utilizzando i dati personali tratti da un sottoinsieme consistente di clienti esistenti, il titolare sceglie una base di clienti che è rappresentativa della popolazione anche per evitare distorsioni sistematiche.

I dati dei clienti, tra cui quelli sul tipo di assicurazione (per esempio un'assicurazione sanitaria, per la casa, per un viaggio, ecc.), oltre ai dati provenienti da registri pubblici cui il titolare ha legittimamente accesso, vengono quindi raccolti dal rispettivo sistema di gestione dei dati. Tutti i dati sono pseudonimizzati prima di essere trasferiti al sistema dedicato all'addestramento del modello di IA.

Per garantire che i dati utilizzati per l'addestramento dell'IA siano il più esatti possibile, il titolare li raccoglie soltanto dalle fonti che contengono informazioni corrette e aggiornate.

La compagnia assicurativa verifica che l'IA sia attendibile e fornisca risultati non discriminatori durante il suo sviluppo e, infine, prima della distribuzione del prodotto. Quando l'IA è pienamente addestrata e operativa, la compagnia assicurativa utilizza i risultati a supporto delle valutazioni del rischio assicurativo, senza tuttavia affidarsi esclusivamente all'IA per decidere se concedere l'assicurazione, a meno che la decisione non venga adottata in conformità delle eccezioni di cui all'articolo 22, paragrafo 2, del RGPD.

La compagnia assicurativa verificherà inoltre periodicamente i risultati dell'IA per mantenerla affidabile e, ove necessario, adeguare l'algoritmo.

Esempio 2

Il titolare è una struttura sanitaria che ricerca metodi per garantire l'integrità e l'esattezza dei dati personali nei suoi registri clienti.

Qualora due diverse persone arrivino presso la struttura sanitaria alla medesima ora e ricevano lo stesso trattamento, si corre il rischio di confonderle se l'unico parametro che le distingue è il nome. Per garantire l'esattezza, il titolare ha bisogno di un identificativo unico per ciascuna persona e quindi di maggiori informazioni rispetto al solo nome del cliente.

La struttura utilizza diversi sistemi che contengono informazioni personali dei clienti e deve assicurare che tali informazioni sul cliente siano corrette, esatte e coerenti in tutti i sistemi in qualunque momento. La struttura ha individuato vari rischi che possono insorgere se le informazioni sono modificate in un sistema ma non negli altri.

Il titolare decide di mitigare il rischio utilizzando una tecnica di hashing che può servire per garantire l'integrità dei dati nel registro dei trattamenti sanitari. A tal fine crea marcature temporali immutabili e crittografiche per le voci del registro dei trattamenti sanitari a cui il cliente è associato, in modo da consentire il riconoscimento, la correlazione e l'eventuale tracciamento di ogni modifica.

3.7 Limitazione della conservazione

80. Il titolare deve garantire che i dati personali siano conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore a quello necessario per le finalità per le quali i dati personali sono trattati[40].
È fondamentale che il titolare sappia esattamente quali dati personali sono trattati e perché. La finalità del trattamento è il criterio principale per stabilire la durata della conservazione dei dati personali.

81. Le misure e le garanzie che attuano il principio della limitazione della conservazione integrano i diritti e le libertà degli interessati, in particolare il diritto alla cancellazione e il diritto di opposizione.

82. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi alla limitazione della conservazione, possono figurare:
- cancellazione e anonimizzazione – il titolare dovrebbe disporre di procedure interne e di funzionalità ben definite per la cancellazione e/o l'anonimizzazione dei dati;
- efficacia dell'anonimizzazione/cancellazione – il titolare si assicura che non sia possibile re-identificare i dati anonimizzati o recuperare quelli cancellati e dovrebbe verificare che tali misure funzionino;
- automatizzazione – la cancellazione di determinati dati personali dovrebbe essere automatizzata;
- criteri di conservazione – il titolare deve stabilire la durata della conservazione e quali dati sono necessari per la specifica finalità;
- giustificazione – il titolare deve essere in grado di motivare perché il periodo di conservazione sia necessario per la finalità e per i dati personali in questione, nonché di spiegare le ragioni e i fondamenti giuridici alla base del periodo di conservazione;
- applicazione delle politiche di conservazione – il titolare dovrebbe far valere determinate politiche di conservazione interne e verificare se l'organizzazione le mette in pratica;
- backup/registri di eventi – i titolari devono stabilire quali dati personali e quale periodo di conservazione siano necessari per i backup e i registri di eventi;
- flusso di dati – i titolari dovrebbero prestare attenzione al flusso di dati personali e alla conservazione delle loro copie, cercando di limitarne la conservazione «temporanea».

Esempio

Il titolare raccoglie dati personali e la finalità del trattamento è gestire le iscrizioni degli interessati. I dati personali vengono cancellati quando termina l'iscrizione e non sussiste una base giuridica che imponga l'ulteriore conservazione dei dati.

A tal fine, il titolare definisce innanzitutto una procedura interna per la conservazione e la cancellazione dei dati, in base alla quale i dipendenti cancellano manualmente i dati personali dopo la fine del periodo di conservazione. Il dipendente si attiene alla procedura di cancellare regolarmente e correggere i dati salvati in qualunque dispositivo, backup, registri, e-mail e altri dispositivi di memorizzazione pertinenti.

Per rendere la cancellazione più efficace e meno soggetta a errori, il titolare implementa un meccanismo automatico al fine di cancellare i dati automaticamente, in modo affidabile e più regolare. Il meccanismo è configurato per seguire una determinata procedura per la cancellazione dei dati che avviene poi a intervalli regolari e predefiniti, eliminando i dati personali da tutti i dispositivi di

[40] Articolo 5, paragrafo 1, lettera c) del RGPD.

memorizzazione dell'impresa. Il titolare esamina e verifica periodicamente la procedura di conservazione, garantendo che sia conforme alla politica di conservazione aggiornata.

3.8 Integrità e riservatezza

83. Il principio di integrità e riservatezza prevede la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. La sicurezza dei dati personali richiede misure appropriate concepite per prevenire e gestire incidenti di violazione dei dati, garantire la corretta esecuzione dei compiti di trattamento dei dati e la conformità agli altri principi, nonché facilitare l'esercizio effettivo dei diritti delle persone.

84. Il considerando 78 stabilisce che una delle misure della DPbDD potrebbe consistere nel consentire al titolare di *«di creare e migliorare caratteristiche di sicurezza»*. Parallelamente alle altre misure della DPbDD, il considerando 78 suggerisce una responsabilità dei titolari, ossia quella di valutare costantemente se stiano utilizzando, in qualunque momento, i mezzi appropriati di trattamento e se le misure scelte contrastino effettivamente le vulnerabilità esistenti. Inoltre, i titolari dovrebbero effettuare revisioni periodiche delle misure di sicurezza poste a presidio e tutela dei dati personali, nonché della procedura per la gestione delle violazioni dei dati.

85. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi all'integrità e alla riservatezza, possono figurare:
    - sistema di gestione della sicurezza delle informazioni – occorre disporre di uno strumento operativo per gestire le politiche e le procedure per la sicurezza delle informazioni;
    - analisi del rischio – valutare i rischi per la sicurezza dei dati personali, considerando l'impatto sui diritti delle persone, e contrastare quelli identificati, nonché, ai fini dell'utilizzo nella valutazione dei rischi, sviluppare e gestire una «modellizzazione delle minacce» esaustiva, sistematica e realistica e un'analisi della superficie di attacco riferita al software specifico così da ridurre i vettori di attacco e le opportunità di sfruttare eventuali punti deboli e vulnerabilità;
    - sicurezza fin dalla progettazione – tenere conto non appena possibile dei requisiti di sicurezza nella progettazione e nello sviluppo del sistema, integrando e svolgendo costantemente test pertinenti;
    - manutenzione – rivedere e verificare periodicamente il software, l'hardware, i sistemi e i servizi, ecc. per scoprire eventuali vulnerabilità dei sistemi di supporto del trattamento;
    - gestione del controllo degli accessi – solo il personale autorizzato che ne ha necessità dovrebbe avere accesso ai dati personali necessari ai loro compiti di trattamento. Inoltre, il titolare dovrebbe differenziare i privilegi di accesso del personale autorizzato;
        - limitazione dell'accesso (agenti) – definire il trattamento dei dati in modo tale che un numero minimo di persone abbia bisogno di accedere ai dati personali per svolgere le proprie funzioni, e limitare l'accesso di conseguenza;
        - limitazione dell'accesso (contenuto) – nel contesto di ciascuna operazione di trattamento, limitare l'accesso per ogni set di dati ai soli attributi che sono necessari allo svolgimento di tale operazione. Limitare inoltre l'accesso ai dati relativi agli interessati di competenza del rispettivo dipendente;
        - segregazione dell'accesso – definire il trattamento dei dati in modo tale che nessuno necessiti di accedere a tutti i dati raccolti sull'interessato, tanto meno a tutti i dati personali di una categoria specifica di interessati;
    - trasferimenti sicuri – i trasferimenti sono protetti da modifiche e accessi non autorizzati e accidentali;

- conservazione sicura – la conservazione dei dati è protetta da modifiche e accessi non autorizzati. Dovrebbero essere previste procedure per valutare il rischio di conservazione centralizzata o decentrata, e le categorie di dati personali cui si applicano. Alcuni dati potrebbero richiedere misure di sicurezza supplementari rispetto ad altri o l'isolamento da questi ultimi;
- pseudonimizzazione – i dati personali e i backup/registri di eventi dovrebbero essere pseudonimizzati come misura di sicurezza per ridurre al minimo i rischi di potenziali violazioni dei dati, ad esempio utilizzando l'hashing o la cifratura;
- backup/registri di eventi – conservare backup e registri di eventi nella misura necessaria per la sicurezza delle informazioni, utilizzare registri delle attività (*audit trails*) e il monitoraggio degli eventi come controlli di sicurezza su base routinaria, proteggendoli da modifiche e accessi non autorizzati e accidentali e rivedendoli periodicamente, oltre a gestire in modo tempestivo eventuali incidenti;
- ripristino in caso di disastro (*disaster recovery*)/continuità operativa – soddisfare i requisiti per il ripristino del sistema informativo in caso di disastro e per la continuità operativa, al fine di ripristinare la disponibilità dei dati personali a seguito di incidenti rilevanti;
- protezione in base al rischio – tutte le categorie di dati personali dovrebbero essere protette con misure adeguate contro il rischio di violazioni della sicurezza. I dati che comportano rischi particolari dovrebbero, ove possibile, essere tenuti separati dagli altri dati personali;
- gestione della risposta in caso di incidenti legati alla sicurezza – occorre disporre di metodologie, procedure e risorse per rilevare, limitare, gestire e segnalare le violazioni dei dati e trarne insegnamenti;
- gestione degli incidenti – al fine di rendere più solido il sistema di trattamento, il titolare deve disporre di procedure per gestire violazioni e incidenti, ivi comprese procedure di notifica quali la gestione delle notifiche (per l'autorità di controllo) e delle informazioni (per gli interessati).

Esempio

Un titolare vuole estrarre grandi quantità di dati personali da un database sanitario contenente cartelle cliniche elettroniche (dei pazienti) e trasferirli su un server dedicato aziendale per trattarli ai fini della garanzia della qualità. L'impresa ha valutato che il rischio legato all'instradamento dei dati estratti verso un server accessibile a tutti i dipendenti è probabilmente elevato per i diritti e le libertà degli interessati. Poiché nell'impresa c'è solo un reparto che deve trattare gli estratti dei dati relativi ai pazienti, il titolare decide di limitare ai dipendenti di quel reparto l'accesso al server dedicato. Inoltre, per ridurre ulteriormente i rischi, i dati saranno pseudonimizzati prima del trasferimento.

Per disciplinare l'accesso e attenuare i possibili danni derivanti da malware, l'impresa decide di segregare la rete e stabilire controlli di accesso al server. Inoltre, istituisce un monitoraggio della sicurezza e sistemi di rilevamento e prevenzione delle intrusioni, inibendoli all'utilizzo abituale. È istituito un sistema di controllo automatizzato per monitorare gli accessi e le modifiche che genera segnalazioni e avvisi automatici quando si configurano determinati eventi riguardanti l'uso. Il titolare garantirà che gli utenti abbiano accesso esclusivamente sulla base del principio 'need to know' (cioè di effettive esigenze informative) e purché siano provvisti di adeguati privilegi di accesso. Ogni utilizzo improprio può essere rilevato facilmente e rapidamente.

Alcuni dei dati estratti devono essere confrontati con quelli nuovi e devono pertanto essere conservati per tre mesi. Il titolare decide di inserirli in banche dati separate sullo stesso server e di utilizzare una cifratura trasparente e con chiave a livello di colonna per conservarli. Le chiavi per la decifratura dei dati nelle colonne sono conservate in appositi moduli di sicurezza che possono essere utilizzati, ma non estratti, solo da personale autorizzato.

La presenza di meccanismi per la gestione degli incidenti futuri rende il sistema più solido e affidabile. Il titolare del trattamento è consapevole della necessità di integrare garanzie e misure efficaci e preventive in tutti i trattamenti di dati personali, sia correnti sia futuri, e che così facendo si possono prevenire future violazioni dei dati.

Il titolare stabilisce queste misure di sicurezza per garantire l'esattezza, l'integrità e la riservatezza, ma anche per prevenire la diffusione di malware attraverso attacchi informatici e ottenere una soluzione robusta. Disporre di solide misure di sicurezza contribuisce a instaurare un clima di fiducia con gli interessati.

3.9 Responsabilizzazione[41]

86. Il principio di responsabilizzazione prevede che il titolare sia responsabile della conformità a tutti i principi summenzionati e sia in grado di dimostrarla.

87. Il titolare deve essere in grado di dimostrare la conformità ai principi; in tal modo può comprovare gli effetti delle misure adottate per tutelare i diritti degli interessati e i motivi per cui tali misure sono considerate adeguate ed efficaci, dimostrando ad esempio in che modo una determinata misura sia adeguata a garantire efficacemente il principio di limitazione della conservazione.

88. Per poter trattare i dati responsabilmente, il titolare dovrebbe sia conoscere le norme in materia di protezione dei dati sia essere in grado di darvi attuazione . Ciò comporta che egli comprenda gli obblighi in materia di protezione dei dati imposti nei suoi riguardi dal RGPD e sia in grado di adempiere a tali obblighi.

4 ARTICOLO 25, PARAGRAFO 3: CERTIFICAZIONE

89. Ai sensi dell'articolo 25, paragrafo 3, la certificazione di cui all'articolo 42 può essere utilizzata come un elemento per dimostrare la conformità con la DPbDD. Parimenti, i documenti che attestano la conformità con la DPbDD potrebbero risultare utili durante una procedura di certificazione. Ciò significa che laddove un trattamento svolto da un titolare o un responsabile sia stato certificato ai sensi dell'articolo 42, le autorità di controllo ne tengono conto nella loro valutazione della conformità con il RGPD, in particolare con la DPbDD.

90. Quando un trattamento è certificato a norma dell'articolo 42, gli elementi che contribuiscono ad attestare la conformità all'articolo 25, paragrafi 1 e 2 sono le procedure di progettazione, ossia la procedura per determinare i mezzi di trattamento, la governance nonché le misure tecniche e organizzative finalizzate ad attuare i principi di protezione dei dati. I criteri di una certificazione in materia di protezione dei dati sono definiti dagli organismi di certificazione o dai titolari dello schema di certificazione e poi approvati dall'autorità di controllo competente o dall'EDPB. Per ulteriori informazioni sui meccanismi di certificazione, rinviamo il lettore alle Linee guida dell'EDPB relative alla certificazione[42] e ad altri orientamenti pertinenti pubblicati sul sito web dell'EDPB.

[41] Cfr. il considerando 74, in base a cui i titolari sono tenuti a dimostrare l'efficacia delle loro misure.

[42] EDPB, «Linee guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento», versione 3.0, 4 giugno 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_it.pdf

91. Anche qualora un trattamento sia certificato ai sensi dell'articolo 42, il titolare è comunque tenuto a garantire il monitoraggio costante e il miglioramento della conformità ai criteri della DPbDD di cui all'articolo 25.

5 MISURE PRESE IN ATTUAZIONE DELL'ARTICOLO 25 E RELATIVE CONSEGUENZE

92. Le autorità di controllo possono valutare la conformità con l'articolo 25 secondo le procedure indicate all'articolo 58. I poteri correttivi sono evidenziati all'articolo 58, paragrafo 2, e comprendono avvertimenti, ammonimenti, ingiunzioni di conformarsi ai diritti degli interessati, limitazioni o divieti di trattamento, sanzioni amministrative pecuniarie, ecc.

93. La DPbDD costituisce, inoltre, un elemento preso in considerazione al fine di stabilire l'entità delle sanzioni pecuniarie per le violazioni del RGPD, cfr. articolo 83, paragrafo 4[43] [44].

6 RACCOMANDAZIONI

94. Benché non siano direttamente destinatari delle disposizioni di cui all'articolo 25, anche i responsabili del trattamento e i produttori rappresentano figure essenziali ai fini della DPbDD e dovrebbero essere consapevoli del fatto che i titolari sono tenuti a trattare i dati personali solo utilizzando sistemi e tecnologie che integrano i principi di protezione dei dati.

95. Nel trattare i dati per conto dei titolari, o nel fornire ai titolari soluzioni di trattamento, responsabili e produttori dovrebbero utilizzare le loro competenze per instaurare un clima di fiducia e orientare i loro clienti, PMI comprese, verso soluzioni di progettazione che integrano la protezione dei dati nel trattamento. Ciò significa a sua volta che la progettazione di prodotti e servizi dovrebbe semplificare le esigenze dei titolari.

96. Nell'applicare l'articolo 25 si dovrebbe tener presente che il principale obiettivo di progettazione è costituito dall' integrare nelle misure adeguate per lo specifico trattamento l'*efficace attuazione* dei principi e la *tutela* dei diritti degli interessati. Al fine di agevolare e potenziare l'adozione della DPbDD, formuliamo le seguenti raccomandazioni per i titolari, i produttori e i responsabili del trattamento:
    - i titolari dovrebbero pensare alla protezione dei dati sin dalle *fasi iniziali* della pianificazione di un trattamento e ancor prima di definirne i mezzi;
    - se un titolare è coadiuvato da un responsabile della protezione dei dati (RPD), l'EDPB incoraggia il coinvolgimento attivo dell'RDP per integrare la DPbDD nelle procedure di acquisizione e sviluppo, nonché lungo l'intero ciclo di vita del trattamento;
    - un trattamento può essere *certificato*. La capacità di ottenere una certificazione per il trattamento rappresenta un valore aggiunto per il titolare al momento di scegliere tra i diversi software, hardware, servizi e/o sistemi di trattamento forniti dai produttori o dai responsabili del trattamento. Pertanto, i produttori dovrebbero sforzarsi di dimostrare che la DPbDD è

[43] Ai sensi dell'articolo 83, paragrafo 2, lettera d), del RGPD, nel determinare l'imposizione delle sanzioni per violazione dello stesso RGPD *«si tiene debito conto» del «grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32».*

[44] Sono disponibili maggiori informazioni sulle sanzioni nel documento del Gruppo di lavoro dell'articolo 29, «Guidelines on application and setting of administrative fines for the purposes of the Regulation 2016/679», WP 253, 3 ottobre 2017, ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 - approvate dall'EDPB.

parte integrante del ciclo di vita dello sviluppo della loro soluzione per il trattamento; una certificazione può inoltre orientare gli interessati nella loro scelta tra i diversi prodotti e servizi: avere la possibilità di far certificare un trattamento può costituire da vantaggio competitivo per i produttori, i responsabili e i titolari e può persino accrescere la fiducia degli interessati nel trattamento dei loro dati personali. In assenza di certificazione, i titolari dovrebbero cercare di avere altre *garanzie* in merito alla conformità ai requisiti della DPbDD da parte dei produttori o dei responsabili del trattamento;

- titolari, responsabili e produttori dovrebbero tenere conto degli obblighi di fornire una tutela specifica ai minori e ad altri gruppi vulnerabili, nel rispetto della DPbDD;
- produttori e responsabili dovrebbero cercare di agevolare l'attuazione della DPbDD al fine di supportare il titolare nell'adempimento degli obblighi previsti dall'articolo 25. I titolari, d'altro canto, non dovrebbero scegliere produttori o responsabili che non offrono sistemi in grado di consentire o facilitare l'adempimento degli obblighi di cui all'articolo 25 in capo ai titolari stessi, poiché saranno questi ultimi a rispondere dell'eventuale mancata attuazione;
- i produttori e i responsabili dovrebbero svolgere un ruolo attivo nel garantire che siano soddisfatti i criteri relativi allo «stato dell'arte» e notificare ai titolari del trattamento qualunque modifica a tale «stato dell'arte» che possa compromettere l'efficacia delle misure adottate. I titolari dovrebbero inserire questo requisito fra le clausole contrattuali per assicurarsi un tempestivo aggiornamento;
- l'EDPB raccomanda ai titolari di richiedere che i produttori e i responsabili del trattamento dimostrino in che modo i loro hardware, software, servizi o sistemi permettano al titolare di soddisfare i requisiti in materia di responsabilizzazione in conformità della DPbDD, per esempio utilizzando indicatori chiave di prestazione (KPI) per dimostrare l'efficacia delle misure e delle garanzie nell'attuazione dei principi e dei diritti;
- l'EDPB sottolinea la necessità di un approccio armonizzato per attuare i principi e i diritti in modo efficace e invita anche le associazioni o gli organismi che elaborano codici di condotta a norma dell'articolo 40 a incorporarvi orientamenti in materia di DPbDD specifici per il singolo settore;
- i titolari dovrebbero essere corretti e trasparenti nei confronti degli interessati per quanto concerne la valutazione e dimostrazione dell'effettiva attuazione della DPbDD, analogamente a quanto si verifica nella dimostrazione della loro conformità con il RGPD in base al principio di responsabilizzazione;
- le tecnologie di rafforzamento della privacy (PET, privacy-enhancing technologies) che hanno raggiunto lo stato dell'arte possono essere utilizzate fra le misure da adottare in conformità dei requisiti della DPbDD, se del caso, secondo un approccio basato sul rischio. Di per sé, le PET non coprono necessariamente gli obblighi di cui all'articolo 25. I titolari devono valutare se la specifica misura sia adeguata ed efficace ai fini dell'attuazione dei principi di protezione dei dati e dei diritti degli interessati;
- i sistemi preesistenti sono soggetti agli stessi obblighi in materia di DPbDD ai quali soggiacciono i sistemi nuovi, cosicché, ove non siano già conformi ai principi della DPbDD e non sia possibile effettuare modifiche per adempiere ai relativi obblighi, i sistemi preesistenti non sono conformi agli obblighi del RGPD e non possono essere utilizzati per trattare dati personali;
- l'articolo 25 non prevede requisiti meno stringenti per le PMI. Le indicazioni fornite di seguito possono facilitare le PMI nel garantire la conformità all'articolo 25 :

1. eseguire una valutazione dei rischi in fase precoce;
2. cominciare dal trattamento di piccole quantità di dati, passando poi gradatamente a trattamenti di maggiore portata e complessità;
3. cercare di ottenere garanzie in materia di DPbDD da parte dei produttori e dei responsabili del trattamento, quali ad esempio la certificazione e l'adesione a codici di condotta;
4. avvalersi di partner di provata affidabilità;
5. rivolgersi alle autorità di protezione dei dati;
6. leggere gli orientamenti delle suddette autorità e dell'EDPB;
7. attenersi ai codici di condotta, ove disponibili;
8. richiedere assistenza e consulenza professionali.

Per il comitato europeo per la protezione dei dati

La presidente

(Andrea Jelinek)