



17/IT

WP 259 rev.01

Gruppo di lavoro Articolo 29
Linee guida sul consenso ai sensi del regolamento (UE) 2016/679

adottate il 28 novembre 2017
come modificate e adottate da ultimo il 10 aprile 2018

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL
TRATTAMENTO DEI DATI PERSONALI

istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 della stessa,

visto il suo regolamento interno,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della Commissione europea, direzione generale Giustizia e consumatori, B -1049 Bruxelles, Belgio, ufficio MO-59 05/35.

Sito internet: http://ec.europa.eu/justice/data-protection/index_en.htm

Indice

1.	Introduzione	3
2.	Consenso di cui all'articolo 4, punto 11, del regolamento generale sulla protezione dei dati	4
3.	Elementi del consenso valido	5
3.1.	Consenso libero/manifestazione di volontà libera	6
3.1.1.	Squilibrio di potere	6
3.1.2.	Condizionalità	8
3.1.3.	Granularità	11
3.1.4.	Pregiudizio	11
3.2.	Specifico	12
3.3.	Informato	14
3.3.1.	Requisiti minimi di contenuto del consenso "informato"	14
3.3.2.	Come fornire le informazioni	15
3.4.	Manifestazione di volontà inequivocabile	17
4.	Ottenimento del consenso esplicito	20
5.	Condizioni aggiuntive per l'ottenimento di un consenso valido	22
5.1.	Dimostrazione del consenso	22
5.2.	Revoca del consenso	24
6.	Interazione tra il consenso e altre basi legittime di cui all'articolo 6 del regolamento generale sulla protezione dei dati	26
7.	Settori specifici di interesse nel regolamento generale sulla protezione dei dati	26
7.1.	Minori (articolo 8)	26
7.1.1.	Servizio della società dell'informazione	27
7.1.2.	Forniti direttamente a un minore	28
7.1.3.	Età	28
7.1.4.	Consenso del minore e responsabilità genitoriale	29
7.2.	Ricerca scientifica	31
7.3.	Diritti dell'interessato	33
8.	Consenso ottenuto a norma della direttiva 95/46/CE	34

1. Introduzione

Le presenti linee guida forniscono un'analisi approfondita della nozione di consenso di cui al regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati). Il concetto di consenso di cui alla direttiva sulla protezione dei dati (direttiva 95/46/CE) e alla direttiva relativa alla vita privata e alle comunicazioni elettroniche (direttiva 2002/58/CE) si è evoluto. Il regolamento generale sulla protezione dei dati fornisce ulteriori chiarimenti e specifiche sui requisiti per ottenere e dimostrare un consenso valido. Prendendo le mosse dal parere 15/2011 sul consenso, le presenti linee guida si concentrano sui cambiamenti introdotti, fornendo orientamenti pratici per garantire il rispetto del regolamento. Il titolare del trattamento è tenuto a innovare per trovare soluzioni che siano conformi ai requisiti di legge e sostengano meglio la protezione dei dati personali e gli interessi degli interessati.

Il consenso rimane una delle sei basi legittime per trattare i dati personali, come disposto dall'articolo 6 del regolamento¹. Prima di avviare attività che implicano il trattamento di dati personali, il titolare del trattamento deve sempre valutare con attenzione la base legittima appropriata per il trattamento.

Di norma, il consenso può costituire la base legittima appropriata solo se all'interessato vengono offerti il controllo e l'effettiva possibilità di scegliere se accettare o meno i termini proposti o rifiutarli senza subire pregiudizio. Quando richiede il consenso, il titolare del trattamento deve valutare se soddisferà tutti i requisiti per essere valido. Se ottenuto nel pieno rispetto del regolamento, il consenso è uno strumento che fornisce all'interessato il controllo sul trattamento dei dati personali che lo riguardano. In caso contrario, il controllo diventa illusorio e il consenso non costituirà una base valida per il trattamento, rendendo illecita l'attività di trattamento².

Ove coerenti con il nuovo quadro giuridico, i pareri che il Gruppo di lavoro Articolo 29 (in appresso: Gruppo di lavoro) ha formulato in materia di consenso³ rimangono pertinenti, in quanto il regolamento generale sulla protezione dei dati codifica gli orientamenti e le buone prassi generali del Gruppo di lavoro e lascia immutata la maggior parte degli aspetti essenziali del consenso. Di conseguenza, il presente documento amplia e completa pareri precedenti del Gruppo di lavoro su argomenti specifici che fanno riferimento al consenso ai sensi della direttiva 95/46/CE, senza sostituirli.

Come affermato nel parere 15/2011 sulla definizione di consenso, l'invito ad accettare il trattamento dei dati dovrebbe essere soggetto a criteri rigorosi, poiché sono in gioco i diritti fondamentali dell'interessato e il titolare del trattamento intende svolgere un trattamento che senza il consenso

¹ L'articolo 9 del regolamento generale sulla protezione dei dati fornisce un elenco di possibili esenzioni al divieto di trattamento di categorie particolari di dati. Una delle esenzioni elencate è il consenso esplicito dell'interessato all'uso di tali dati.

² Cfr. anche il parere 15/2011 sulla definizione di consenso (WP 187), pagine 6-8 e/o il parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE (WP 217), pagg. 9, 10, 13 e 14.

³ In particolare il parere 15/2011 sulla definizione di consenso (WP 187).

sarebbe illecito⁴. Il ruolo cruciale del consenso è sottolineato dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Inoltre, l'ottenimento del consenso non fa venir meno né diminuisce in alcun modo l'obbligo del titolare del trattamento di rispettare i principi applicabili al trattamento sanciti nel regolamento generale sulla protezione dei dati, in particolare all'articolo 5, per quanto concerne la correttezza, la necessità e la proporzionalità, nonché la qualità dei dati. Il fatto che il trattamento dei dati personali si basi sul consenso dell'interessato non legittima la raccolta di dati non necessari a una finalità specifica di trattamento, che sarebbe fundamentalmente iniqua⁵.

Parallelamente, il Gruppo di lavoro è a conoscenza della revisione della direttiva relativa alla vita privata e alle comunicazioni elettroniche. La nozione di consenso nel progetto di regolamento sulla vita privata e le comunicazioni elettroniche rimane legata a quella del regolamento generale sulla protezione dei dati⁶. È probabile che ai sensi del futuro strumento le organizzazioni necessitino del consenso per la maggior parte dei messaggi di marketing online, per le chiamate di marketing e per i metodi di tracciamento online, compreso tramite l'uso di cookie, applicazioni o altri software. Il Gruppo di lavoro ha già fornito raccomandazioni e orientamenti al legislatore europeo in merito alla proposta di regolamento sulla vita privata e le comunicazioni elettroniche⁷.

Per quanto riguarda l'attuale direttiva relativa alla vita privata e alle comunicazioni elettroniche, il Gruppo di lavoro rileva che i riferimenti alla direttiva 95/46/CE abrogata si intendono fatti al regolamento generale sulla protezione dei dati⁸. Ciò vale anche per i riferimenti riguardanti il consenso, poiché il regolamento sulla vita privata e le comunicazioni elettroniche non sarà (ancora) entrato in vigore il 25 maggio 2018. Ai sensi dell'articolo 95 del regolamento generale sulla protezione dei dati, non sono imposti obblighi supplementari in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione, nella misura in cui la direttiva relativa alla vita privata e alle comunicazioni elettroniche impone obblighi specifici aventi il medesimo obiettivo. Il Gruppo di lavoro rileva che i requisiti per il consenso ai sensi del regolamento generale sulla protezione dei dati non sono considerati un "obbligo supplementare", bensì condizioni preliminari per la liceità del trattamento. Pertanto, tali requisiti sono applicabili alle situazioni che rientrano nel campo di applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

2. Consenso di cui all'articolo 4, punto 11, del regolamento generale sulla protezione dei dati

L'articolo 4, punto 11, del regolamento generale sulla protezione dei dati definisce il consenso dell'interessato come: *“qualsiasi manifestazione di volontà libera, specifica, informata e*

⁴ Parere 15/2011 sulla definizione di consenso (WP 187), pag. 9.

⁵ Cfr. anche il parere 15/2011 sulla definizione di consenso (WP 187) e l'articolo 5 del regolamento generale sulla protezione dei dati.

⁶ Ai sensi dell'articolo 9 della proposta di regolamento sulla vita privata e le comunicazioni elettroniche, si applicano la definizione e le condizioni per il consenso di cui all'articolo 4, punto 11, e all'articolo 7, del regolamento generale sulla protezione dei dati.

⁷ Cfr. *“Opinion 03/2016 on the evaluation and review of the ePrivacy Directive”* [Parere 03/2016 sulla valutazione e la revisione della direttiva relativa alla vita privata e alle comunicazioni elettroniche] (WP 240).

⁸ Cfr. articolo 94 del regolamento generale sulla protezione dei dati.

inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento”.

La nozione di consenso rimane sostanzialmente simile a quella della direttiva 95/46/CE, e il consenso rimane uno dei presupposti per il trattamento dei dati personali, ai sensi dell'articolo 6 del regolamento generale sulla protezione dei dati⁹. Oltre alla definizione modificata di cui all'articolo 4, punto 11, il regolamento fornisce ulteriori indicazioni, all'articolo 7 e ai considerando 32, 33, 42 e 43, su come il titolare del trattamento deve agire per rispettare gli elementi principali del requisito del consenso.

L'inclusione, nel regolamento, di disposizioni e considerando specifici sulla revoca del consenso conferma che quest'ultimo dovrebbe essere una decisione reversibile e che l'interessato mantiene un certo grado di controllo.

3. Elementi del consenso valido

L'articolo 4, punto 11, del regolamento generale sulla protezione dei dati stabilisce che il consenso dell'interessato è qualsiasi:

- manifestazione di volontà libera,
- specifica,
- informata e
- inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Le sezioni che seguono analizzano la misura in cui la formulazione dell'articolo 4, punto 11, richiede al titolare del trattamento di modificare le sue richieste/i suoi moduli di consenso affinché siano conformi al regolamento generale sulla protezione dei dati¹⁰.

⁹ Il consenso, definito nella direttiva 95/46/CE come “*qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento*”, deve essere “manifestato in maniera inequivocabile” in maniera da rendere legittimo il trattamento dei dati personali (articolo 7, lettera a), della direttiva 95/46/CE). Cfr. Gruppo di lavoro Articolo 29, Parere 15/2011 sulla definizione di consenso (WP 187), per esempi sull'adeguatezza del consenso come base legittima. In tale parere, il Gruppo di lavoro ha fornito linee guida atte a distinguere il caso in cui il consenso costituisca una base lecita appropriata rispetto ai casi in cui è sufficiente fare affidamento su motivi di interesse legittimo (magari offrendo un'opportunità di rinuncia, “*opt-out*”) o sarebbe raccomandabile fondare il trattamento su un rapporto contrattuale. Cfr. anche il parere 06/2014 del Gruppo di lavoro, sezione III.1.2, pag. 17 e successive. Il consenso esplicito è anche una delle esenzioni al divieto di trattamento di categorie particolari di dati: cfr. articolo 9 del regolamento generale sulla protezione dei dati.

¹⁰ Per orientamenti in merito alle attività di trattamento in corso basate sul consenso di cui alla direttiva 95/46, cfr. il capitolo 7 del presente documento e il considerando 171 del regolamento generale sulla protezione dei dati.

3.1. Consenso libero/manifestazione di volontà libera¹¹

L'elemento della manifestazione di volontà "libera" implica che l'interessato abbia una scelta effettiva e il controllo sui propri dati. Come regola generale, il regolamento stabilisce che se l'interessato non dispone di una scelta effettiva, si sente obbligato ad acconsentire o subirà conseguenze negative se non acconsente, il consenso non sarà valido¹². Se il consenso è parte non negoziabile delle condizioni generali di contratto/servizio, si presume che non sia stato prestato liberamente. Di conseguenza, il consenso non sarà considerato libero se l'interessato non può rifiutarlo o revocarlo senza subire pregiudizio¹³. Il regolamento generale sulla protezione dei dati ha preso in considerazione anche la nozione di squilibrio tra il titolare del trattamento e l'interessato.

Nel valutare se il consenso sia stato prestato liberamente, si deve anche tener conto dell'eventualità che il consenso sia collegato all'esecuzione di un contratto o alla prestazione di un servizio come descritto all'articolo 7, paragrafo 4. L'articolo 7, paragrafo 4, contenendo l'inciso "tra le altre", non è esaustivo e può quindi comprendere altre eventualità. In termini generali, qualsiasi azione di pressione o influenza inappropriata sull'interessato (che si può manifestare in svariati modi) che impedisca a quest'ultimo di esercitare il suo libero arbitrio, rende il consenso invalido.

[Esempio 1]

Un'applicazione mobile per il fotoritocco chiede agli utenti di attivare la localizzazione GPS per l'utilizzo dei suoi servizi. L'applicazione comunica agli utenti che utilizzerà i dati raccolti per finalità di pubblicità comportamentale. Né la geolocalizzazione né la pubblicità comportamentale online sono necessarie per la prestazione del servizio di fotoritocco e vanno oltre la fornitura del servizio principale. Poiché gli utenti non possono utilizzare l'applicazione senza acconsentire a tali finalità, il consenso non può essere considerato liberamente espresso.

3.1.1. Squilibrio di potere

Il considerando 43¹⁴ indica chiaramente che è improbabile che le **autorità pubbliche** possano basarsi sul consenso per effettuare il trattamento, poiché quando il titolare del trattamento è un'autorità pubblica sussiste spesso un evidente squilibrio di potere nella relazione tra il titolare del trattamento e l'interessato. In molti di questi casi è inoltre evidente che l'interessato non dispone di

¹¹ In svariati pareri il Gruppo di lavoro Articolo 29 ha esaminato i limiti del consenso in situazioni in cui non sia possibile esprimerlo liberamente. Ciò è avvenuto in particolare nei seguenti documenti del Gruppo: parere 15/2011 sulla definizione di consenso (WP 187), documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (WP 131), parere 8/2001 sul trattamento dei dati personali nel contesto lavorativo (WP 48) e "Second opinion 4/2009 on processing of data by the World Anti-Doping Agency (WADA) (International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations" [Secondo parere 4/2009 sul trattamento dei dati da parte dell'Agenzia mondiale antidoping (AMA) - norma internazionale per la tutela della vita privata e delle informazioni personali, sulle relative disposizioni del codice AMA e sulla altre questioni relative alla tutela della vita privata nel contesto della lotta contro il doping nello sport da parte dell'AMA e delle organizzazioni (nazionali) antidoping] (WP 162).

¹² Cfr. parere 15/2011 sulla definizione di consenso (WP 187), pag. 13.

¹³ Cfr. considerando 42 e 43 del regolamento generale sulla protezione dei dati e il parere del Gruppo di lavoro 15/2011 sulla definizione di consenso, adottato il 13 luglio 2011 (WP 187), pag. 13.

¹⁴ Il considerando 43 del regolamento generale sulla protezione dei dati afferma: "Per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica. (...)".

alternative realistiche all'accettazione (dei termini) del trattamento. Il Gruppo di lavoro ritiene che esistano altre basi legittime, in linea di principio più appropriate, per il trattamento da parte delle autorità pubbliche¹⁵.

Fatte salve queste considerazioni generali, il regolamento non esclude completamente il ricorso al consenso come base legittima per il trattamento dei dati da parte delle autorità pubbliche. I seguenti esempi mostrano infatti che l'uso del consenso può essere appropriato in determinate circostanze.

[Esempio 2]

Un comune sta pianificando l'esecuzione di lavori di manutenzione stradale. Poiché i lavori possono perturbare il traffico per parecchio tempo, il comune offre ai cittadini la possibilità di iscriversi a una mailing list per ricevere aggiornamenti sull'avanzamento dei lavori e sui ritardi previsti. Il comune chiarisce che la partecipazione non è obbligatoria e chiede il consenso a utilizzare gli indirizzi di posta elettronica per questa finalità (esclusiva). I cittadini che non acconsentono non perderanno l'accesso ad alcun servizio fondamentale del comune né alcun diritto, di conseguenza possono esprimere o rifiutare liberamente il loro consenso a questo uso dei dati. Tutte le informazioni sui lavori stradali saranno disponibili anche sul sito web del comune.

[Esempio 3]

Un proprietario terriero necessita di alcuni permessi tanto dal comune quanto dalla provincia. Entrambi gli enti pubblici richiedono le stesse informazioni per il rilascio dei permessi, ma non hanno accesso alle rispettive banche dati. Di conseguenza entrambi chiedono le stesse informazioni e il proprietario terriero invia i dati ad entrambi. Il comune e la provincia chiedono il consenso dell'interessato per riunire i fascicoli al fine di evitare duplicazioni di procedure e corrispondenza. Entrambi gli enti pubblici assicurano che ciò è facoltativo e che le richieste di permesso verranno comunque trattate separatamente qualora l'interessato decida di non acconsentire alla riunione dei fascicoli. Il proprietario terriero può quindi esprimere liberamente il consenso alle autorità per la finalità di riunione dei fascicoli.

[Esempio 4]

Una scuola pubblica chiede agli studenti il consenso ad utilizzare le loro fotografie in una rivista studentesca in formato cartaceo. In questo caso il consenso costituisce una scelta vera e propria a condizione che agli studenti non vengano negati l'istruzione o altri servizi e che gli studenti possano rifiutare il consenso senza subire pregiudizio¹⁶.

Lo squilibrio di potere sussiste anche nel contesto dell'**occupazione**¹⁷. Data la dipendenza risultante dal rapporto datore di lavoro/dipendente, è improbabile che l'interessato sia in grado di negare al datore di lavoro il consenso al trattamento dei dati senza temere o rischiare di subire ripercussioni negative come conseguenza del rifiuto. È improbabile che il dipendente sia in grado di rispondere liberamente, senza percepire pressioni, alla richiesta del datore di lavoro di acconsentire, ad esempio, all'attivazione di sistemi di monitoraggio, quali la sorveglianza con telecamere sul posto di lavoro, o alla compilazione di moduli di valutazione¹⁸. Di conseguenza il Gruppo di lavoro

¹⁵ Cfr. articolo 6 del regolamento generale sulla protezione dei dati, in particolare il paragrafo 1 lettera c) e lettera e).

¹⁶ Ai fini di questo esempio, con "scuola pubblica" si intende una scuola finanziata con fondi pubblici o qualsiasi struttura educativa che si qualifica come un'autorità pubblica o un ente pubblico ai sensi della legislazione nazionale.

¹⁷ Cfr. anche l'articolo 88 del regolamento generale sulla protezione dei dati, nel quale si sottolinea la necessità di tutelare gli interessi specifici dei dipendenti e si crea una possibilità di deroga nel diritto degli Stati membri. Cfr. anche il considerando 155.

¹⁸ Cfr. parere 15/2011 sulla definizione di consenso (WP 187), pagg. 13-15; parere 8/2001 sul trattamento dei dati personali nel contesto lavorativo (WP 48), capitolo 10; documento di lavoro riguardante la vigilanza sulle

ritiene problematico per il datore di lavoro trattare i dati personali dei dipendenti attuali o futuri sulla base del consenso, in quanto è improbabile che questo venga prestato liberamente. Per la maggior parte delle attività di trattamento svolte sul posto di lavoro, la base legittima non può e non dovrebbe essere il consenso del dipendente (articolo 6, paragrafo 1, lettera a)) in considerazione della natura del rapporto tra datore di lavoro e dipendente¹⁹.

Tuttavia, ciò non significa che il datore di lavoro non possa mai basarsi sul consenso come base legittima per il trattamento. In alcune situazioni il datore di lavoro è in grado di dimostrare che il consenso è stato effettivamente espresso liberamente. Dato lo squilibrio di potere tra il datore di lavoro e il suo personale, i dipendenti possono manifestare il loro consenso liberamente soltanto in casi eccezionali, quando non subiranno alcuna ripercussione negativa per il fatto che esprimano il loro consenso o meno²⁰.

[Esempio 5]

Una troupe cinematografica filmerà una determinata area di un ufficio. Il datore di lavoro chiede a tutti i dipendenti che hanno la scrivania in quella zona il consenso a essere ripresi, in quanto potrebbero apparire sullo sfondo del video. Chi non vuole essere filmato non viene penalizzato in alcun modo e ottiene invece una scrivania altrove nell'edificio per l'intera durata delle riprese.

Gli squilibri di potere non sono limitati alle autorità pubbliche e ai datori di lavoro, potendo verificarsi anche in altre situazioni. Come evidenziato dal Gruppo di lavoro in diversi pareri, il consenso è valido soltanto se l'interessato è in grado di operare realmente una scelta e non c'è il rischio di raggiri, intimidazioni, coercizioni o conseguenze negative significative (ad es. costi aggiuntivi sostanziali) in caso di rifiuto a prestare il consenso. Il consenso non sarà considerato liberamente espresso qualora vi sia qualsiasi elemento di costrizione, pressione o incapacità di esercitare il libero arbitrio.

3.1.2. Condizionalità

Per valutare se il consenso sia stato prestato liberamente è di rilievo l'articolo 7, paragrafo 4, del regolamento²¹.

L'articolo 7, paragrafo 4, indica, tra l'altro, che è altamente inopportuno "accorpare" il consenso all'accettazione delle condizioni generali di contratto/servizio o "subordinare" la fornitura di un contratto o servizio a una richiesta di consenso al trattamento di dati personali che non sono necessari per l'esecuzione del contratto o servizio. Si presume che il consenso prestato in una tale

comunicazioni elettroniche sul posto di lavoro (WP 55), punto 4.2; e parere 2/2017 sul trattamento dei dati sul posto di lavoro (WP 249), punto 6.2.

¹⁹ Cfr. parere 2/2017 sul trattamento dei dati sul posto di lavoro, pagg. 6-7.

²⁰ Cfr. anche il parere 2/2017 sul trattamento dei dati sul lavoro (WP 249), punto 6.2.

²¹ L'articolo 7, paragrafo 4, del regolamento generale sulla protezione dei dati recita: "*Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto*". Cfr. anche il considerando 43 del regolamento, che afferma: "*[...] Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione*".

situazione non sia stato espresso liberamente (considerando 43). L'articolo 7, paragrafo 4, mira a garantire che la finalità del trattamento dei dati personali non sia mascherata né accorpata all'esecuzione di un contratto o alla prestazione di un servizio per il quale i dati personali non sono necessari. In tal modo, il regolamento assicura che il trattamento dei dati personali per cui viene richiesto il consenso non possa trasformarsi direttamente o indirettamente in una controprestazione contrattuale. Le due basi legittime per la liceità del trattamento dei dati personali, ossia il consenso e l'esecuzione di un contratto, non possono essere riunite e rese indistinte.

L'obbligo di acconsentire all'uso di dati personali aggiuntivi rispetto a quelli strettamente necessari limita la scelta dell'interessato e ostacola l'espressione del libero consenso. Poiché la legislazione in materia di protezione dei dati mira a tutelare i diritti fondamentali, è essenziale che l'interessato abbia il controllo sui propri dati personali; inoltre sussiste una presunzione forte secondo cui il consenso a un trattamento di dati personali non necessario non può essere considerato un corrispettivo obbligatorio dell'esecuzione di un contratto o della prestazione di un servizio.

Pertanto, ogni volta che una richiesta di consenso è legata all'esecuzione di un contratto da parte del titolare del trattamento, l'interessato che non desidera mettere a disposizione i propri dati personali per il trattamento da parte del titolare corre il rischio di vedersi negare l'erogazione dei servizi richiesti.

Per valutare se si verifica una situazione di accorpamento o subordinazione è importante determinare qual è la portata del contratto e quali dati sono necessari per la sua esecuzione.

Secondo il parere 06/2014 del Gruppo di lavoro, l'espressione "necessario per l'esecuzione di un contratto" deve essere interpretata in maniera rigorosa. Il trattamento deve essere necessario per adempiere il contratto con ciascun interessato. In quest'ambito possono rientrare, per esempio, il trattamento dell'indirizzo dell'interessato ai fini della consegna delle merci acquistate online o il trattamento degli estremi della carta di credito per facilitare il pagamento. Nel contesto occupazionale, questo presupposto potrebbe permettere, per esempio, il trattamento di informazioni riguardanti lo stipendio e le coordinate bancarie per consentire il pagamento degli stipendi²². È necessario che vi sia un collegamento diretto e obiettivo tra il trattamento dei dati e la finalità dell'esecuzione del contratto.

Quando il titolare del trattamento intende trattare dati personali che sono effettivamente necessari per l'esecuzione di un contratto il consenso non è la base legittima appropriata²³.

L'articolo 7, paragrafo 4, è pertinente soltanto laddove i dati richiesti **non** sono necessari per l'esecuzione del contratto (ivi compreso per la prestazione di un servizio) e l'esecuzione del contratto è subordinata all'ottenimento di tali dati in base al presupposto del consenso. Al contrario, qualora il trattamento **sia** necessario per eseguire il contratto (ivi incluso per la prestazione di un servizio), l'articolo 7, paragrafo 4, non si applica.

²² Per maggiori informazioni ed esempi, cfr. parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE, adottato dal Gruppo di lavoro, il 9 aprile 2014, pagg. 19-20. (WP 217).

²³ La base legittima appropriata in tal caso potrebbe infatti essere l'articolo 6, paragrafo 1, lettera b) (contratto).

[Esempio 6]

Una banca chiede ai clienti il consenso per consentire a terzi di utilizzare i dettagli di pagamento per finalità di marketing diretto. Questa attività di trattamento non è necessaria per l'esecuzione del contratto stipulato con il cliente e la prestazione di servizi ordinari di conto bancario. Qualora il rifiuto del cliente a prestare il consenso per tale finalità di trattamento porti alla negazione di servizi bancari, alla chiusura del conto bancario o, a seconda dei casi, a un aumento della commissione, il consenso non può considerarsi espresso liberamente.

La scelta del legislatore di evidenziare la condizionalità, tra l'altro, come presunzione di mancanza di libertà di esprimere il consenso dimostra che il verificarsi della condizionalità deve essere attentamente esaminato. L'espressione "nella massima considerazione" di cui all'articolo 7, paragrafo 4, suggerisce che il titolare del trattamento deve prestare particolare attenzione qualora il contratto (che potrebbe includere la prestazione di un servizio) sia collegato a una richiesta di consenso al trattamento di dati personali.

Poiché l'articolo 7, paragrafo 4, non è formulato in maniera assoluta, in un numero molto ristretto di casi tale condizionalità potrebbe non rendere invalido il consenso. Tuttavia, il verbo "si presume" al considerando 43 indica chiaramente che tali casi saranno estremamente eccezionali.

Ad ogni modo, l'onere della prova riguardo all'articolo 7, paragrafo 4, incombe al titolare del trattamento²⁴. Questa norma specifica riflette il principio generale di responsabilizzazione che permea l'intero regolamento generale sulla protezione dei dati. Tuttavia, quando si applica l'articolo 7, paragrafo 4, risulta più difficile per il titolare del trattamento dimostrare che l'interessato ha prestato liberamente il consenso²⁵.

Il titolare del trattamento potrebbe sostenere che la sua organizzazione offre all'interessato una scelta reale mettendolo in grado di scegliere tra un servizio che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, e un servizio equivalente che non implica un siffatto consenso, dall'altro. Finché esiste la possibilità che il contratto venga eseguito o che il servizio oggetto del contratto venga prestato dal titolare del trattamento senza necessità di acconsentire ad usi ulteriori o supplementari dei dati in questione non si è in presenza di un servizio condizionato. Tuttavia, i due servizi devono essere effettivamente equivalenti.

Il Gruppo di lavoro ritiene che il consenso non possa considerarsi prestato liberamente se il titolare del trattamento sostiene che esiste una scelta tra il suo servizio che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, e un servizio equivalente offerto da un altro titolare del trattamento, dall'altro. In tal caso la libertà di scelta dipenderebbe dagli altri operatori

²⁴ Cfr. anche l'articolo 7, paragrafo 1, del regolamento generale sulla protezione dei dati, il quale stabilisce che il titolare del trattamento deve dimostrare che il consenso dell'interessato è stato liberamente manifestato.

²⁵ In una certa misura, l'introduzione di questo paragrafo è una codifica delle linee guida esistenti formulate dal Gruppo di lavoro. Come descritto nel parere 15/2011, quando un interessato si trova in una situazione di dipendenza rispetto al titolare del trattamento dei dati, in ragione della natura della relazione o di circostanze speciali, potrebbe sussistere una marcata presunzione che la libera manifestazione del consenso sia limitata in tali contesti (ad esempio in un rapporto di lavoro o se la raccolta dei dati è effettuata da un'autorità pubblica). Con l'entrata in vigore dell'articolo 7, paragrafo 4, sarà più difficile per il titolare del trattamento dimostrare che l'interessato ha prestato liberamente il consenso. Cfr.: parere 15/2011 sulla definizione di consenso (WP 187), pp. 14-19.

del mercato e dal fatto che l'interessato ritenga che i servizi offerti dall'altro titolare del trattamento siano effettivamente equivalenti. Ciò implicherebbe inoltre l'obbligo per il titolare del trattamento di monitorare gli sviluppi del mercato per garantire la continuità della validità del consenso per le sue attività di trattamento dei dati, in quanto un concorrente potrebbe modificare il suo servizio in un momento successivo. Di conseguenza il consenso ottenuto con questa argomentazione non rispetta il regolamento generale sulla protezione dei dati.

3.1.3. Granularità

Un servizio può comportare trattamenti multipli per più finalità. In tal caso, l'interessato dovrebbe essere libero di scegliere quale finalità accettare anziché dover acconsentire a un insieme di finalità. Ai sensi del regolamento generale sulla protezione dei dati, in un determinato caso possono essere giustificati più consensi per iniziare a offrire un servizio.

Il considerando 43 chiarisce che si presume che il consenso non sia stato espresso liberamente se il processo o la procedura seguiti per ottenerlo non permettono all'interessato di esprimere un consenso separato ai distinti trattamenti dei dati personali (ad esempio solo ad alcuni trattamenti e non ad altri) nonostante ciò sia appropriato nel singolo caso. Il considerando 32 afferma: *“Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste”*.

Se il titolare del trattamento ha riunito diverse finalità di trattamento e non ha chiesto il consenso separato per ciascuna di esse non c'è libertà. La granularità è strettamente correlata alla necessità che il consenso sia specifico, come analizzato nella sezione 3.2. Quando il trattamento di dati mira a perseguire finalità diverse, la soluzione per soddisfare le condizioni per la validità del consenso risiede nella granularità, ossia nella separazione delle finalità e nell'ottenimento del consenso per ciascuna di esse.

[Esempio 7]

Nel contesto della medesima richiesta di consenso, un rivenditore chiede ai propri clienti il consenso a utilizzare i loro dati per inviare comunicazioni di marketing tramite posta elettronica e per condividere i dati con altre società del gruppo. Tale consenso non è granulare in quanto non è distinto per queste due finalità, pertanto non sarà valido. In questo caso è necessario un consenso specifico all'invio dei dati di contatto ai partner commerciali. Tale consenso specifico sarà ritenuto valido per ciascun partner (cfr. anche la sezione 3.3.1) la cui identità è stata fornita all'interessato al momento dell'ottenimento del consenso, nella misura in cui i dati vengano inviati per la medesima finalità (nell'esempio, finalità di marketing).

3.1.4. Pregiudizio

Il titolare del trattamento deve dimostrare che è possibile rifiutare il consenso oppure revocarlo senza subire pregiudizio (considerando 42), ad esempio dimostrando che la revoca del consenso non comporta alcun costo per l'interessato e quindi nessuno svantaggio evidente in caso di revoca.

Altri esempi di pregiudizio sono l'inganno, l'intimidazione, la coercizione o conseguenze negative significative in caso di mancato consenso. Il titolare del trattamento dovrebbe essere in grado di

dimostrare che l'interessato ha potuto scegliere liberamente o realmente se acconsentire o meno e che poteva revocare il consenso senza pregiudizio.

Se il titolare del trattamento può dimostrare che il servizio consente di revocare il consenso senza conseguenze negative, ad esempio senza che il livello della prestazione del servizio venga diminuito a scapito dell'utente, allora può dimostrare che il consenso è stato conferito liberamente. Il regolamento generale sulla protezione dei dati non esclude tutti gli incentivi, tuttavia spetta al titolare del trattamento dimostrare che il consenso è stato prestato liberamente in tutte le circostanze.

[Esempio 8]

Un'applicazione mobile dedicata allo stile di vita richiede, all'atto dello scaricamento, il consenso all'accesso all'accelerometro del telefono. Tale accesso non è necessario per il funzionamento dell'applicazione, ma è utile al titolare del trattamento per saperne di più sui movimenti e sui livelli di attività degli utenti. Un utente revoca il consenso e scopre che dopo la revoca l'applicazione funziona solo in misura limitata. Questo è un esempio di pregiudizio ai sensi del considerando 42, il che significa che il consenso non è mai stato ottenuto in maniera valida (e quindi il titolare del trattamento deve cancellare tutti i dati personali sui movimenti degli utenti raccolti in tale modo).

[Esempio 9]

Un interessato si iscrive alla newsletter di un rivenditore del settore della moda che offre sconti generali. Il rivenditore chiede all'interessato il consenso per raccogliere ulteriori dati sulle preferenze di acquisto in maniera da personalizzare le offerte in base alle preferenze dell'interessato secondo la cronologia degli acquisti o un questionario facoltativo. Quando l'interessato successivamente revoca il consenso, riceve nuovamente sconti per articoli di moda non personalizzati. Ciò non equivale a un pregiudizio in quanto l'interessato ha perso soltanto l'incentivo ammissibile.

[Esempio 10]

Una rivista di moda offre ai lettori la possibilità di acquistare nuovi prodotti per il trucco prima del loro lancio ufficiale.

I prodotti saranno presto disponibili per la vendita, ma i lettori della rivista ne riceveranno un'anteprima esclusiva. Per godere di tale vantaggio i lettori devono fornire l'indirizzo postale e accettare l'iscrizione alla mailing list della rivista. L'indirizzo postale è necessario per la spedizione e la mailing list viene utilizzata per l'invio di offerte commerciali per prodotti quali cosmetici o t-shirt nel corso dell'anno.

L'azienda spiega che i dati relativi alla mailing list saranno utilizzati esclusivamente per l'invio di prodotti e pubblicità cartacea da parte della rivista stessa e non saranno condivisi con altre organizzazioni.

Qualora non voglia comunicare il proprio indirizzo per tale finalità, il lettore non subisce alcun pregiudizio in quanto i prodotti saranno comunque a sua disposizione.

3.2. Specifico

L'articolo 6, paragrafo 1, lettera a), conferma che il consenso dell'interessato deve essere espresso in relazione a "una o più specifiche" finalità e che l'interessato deve poter scegliere in relazione a ciascuna di esse²⁶. Il requisito secondo il quale il consenso deve essere "*specifico*" mira a garantire un certo grado di controllo da parte dell'utente e trasparenza per l'interessato. Tale requisito non è stato modificato dal regolamento e rimane strettamente legato al requisito del consenso "informato". Allo stesso tempo, deve essere interpretato in linea con il requisito della "granularità",

²⁶ Ulteriori indicazioni sulla determinazione delle "finalità" sono riportate nel documento *Opinion 3/2013 on purpose limitation* [parere 3/2013 sulla limitazione della finalità] (WP 203).

affinché il consenso sia “libero”²⁷. In sintesi, per rispettare l’elemento della specificità (“specifico”), il titolare del trattamento deve applicare:

- (i) la specificazione delle finalità come garanzia contro la “*function creep*”, ossia l’estensione indebita delle funzionalità;
- (ii) la granularità nelle richieste di consenso, e
- (iii) una chiara separazione delle informazioni sull’ottenimento del consenso per le attività di trattamento dei dati rispetto alle informazioni su altre questioni.

Sul punto i): ai sensi dell’articolo 5, paragrafo 1, lettera b), del regolamento, per ottenere un consenso valido occorre sempre prima determinare la finalità specifica, esplicita e legittima dell’attività di trattamento prevista²⁸. La necessità di un consenso specifico associata alla nozione di limitazione delle finalità di cui all’articolo 5, paragrafo 1, lettera b), funge da garanzia contro l’ampliamento progressivo, o la commistione, delle finalità di trattamento dei dati dopo che l’interessato ha acconsentito alla loro raccolta iniziale. Questo fenomeno, noto anche come “*function creep*”, rappresenta un rischio per l’interessato, in quanto può comportare l’uso non previsto di dati personali da parte del titolare del trattamento o di terzi e la perdita del controllo da parte dell’interessato.

Se il titolare del trattamento si basa sull’articolo 6, paragrafo 1, lettera a), l’interessato deve sempre fornire il consenso per una finalità di trattamento specifica²⁹. In linea con il concetto di *limitazione delle finalità* e con l’articolo 5, paragrafo 1, lettera b), e il considerando 32 del regolamento, il consenso può coprire trattamenti distinti, purché abbiano la medesima finalità. Chiaramente il consenso specifico può essere ottenuto soltanto quando l’interessato è specificamente informato delle finalità previste dell’uso dei dati che lo riguardano.

Nonostante le disposizioni in materia di compatibilità delle finalità, il consenso deve essere specifico per finalità. L’interessato presterà il consenso nella convinzione di avere il controllo sui suoi dati e nella convinzione che questi saranno trattati esclusivamente per le finalità specificate. Se tratta i dati basandosi sul presupposto del consenso e intende trattarli per un’altra finalità, il titolare del trattamento deve richiedere un ulteriore consenso per tale finalità a meno che non possa basarsi su un’altra base legittima che risponda meglio alla situazione.

[Esempio 11]

Una rete TV via cavo raccoglie i dati personali degli abbonati, sulla base del loro consenso, per fornire suggerimenti personali su nuovi film che, stando alle abitudini di visualizzazione, potrebbero interessare loro. Dopo un po’, la rete TV vorrebbe consentire a terzi di inviare (o mostrare) pubblicità mirata sulla base delle

²⁷ Il considerando 43 del regolamento generale sulla protezione dei dati afferma che, se del caso, sarà necessario un consenso separato per trattamenti distinti. Dovrebbero essere messe a disposizione opzioni di consenso granulare in maniera da consentire agli interessati di acconsentire separatamente a finalità distinte.

²⁸ Cfr. parere del Gruppo di lavoro 3/2013 sulla limitazione della finalità (WP 203), pag. 16: “*Per questi motivi, una finalità che sia vaga o generica, come ad esempio ‘migliorare l’esperienza degli utenti’, ‘finalità di marketing’, ‘finalità di sicurezza informatica’ o ‘ricerca futura’, senza ulteriori dettagli, di solito non soddisfa i criteri per essere ‘specificata’*”.

²⁹ Ciò è coerente con il parere del Gruppo di lavoro 15/2011 sulla definizione di consenso (WP 187), ad esempio a pag. 19.

abitudini di visualizzazione degli abbonati. Data questa nuova finalità, è necessario ottenere un nuovo consenso.

Sul punto ii): i meccanismi di consenso devono essere granulari non solo per soddisfare il requisito del consenso “libero”, ma anche per soddisfare quello del consenso “specifico”. Ciò significa che il titolare del trattamento che richiede il consenso per finalità diverse dovrebbe prevedere una possibilità di adesione distinta per ciascuna finalità, in modo da consentire all’utente di esprimere un consenso specifico per le finalità specifiche.

Sul punto iii): il titolare del trattamento dovrebbe fornire informazioni specifiche, in relazione a ciascuna richiesta di consenso distinta, sui dati che vengono trattati per ciascuna finalità, al fine di rendere noto all’interessato l’impatto delle diverse scelte a sua disposizione. In questo modo l’interessato può esprimere un consenso specifico. Questo aspetto si sovrappone al requisito che impone al titolare del trattamento di fornire informazioni chiare, come analizzato al punto 3.3.

3.3. Informato

Il regolamento generale sulla protezione dei dati rafforza il requisito secondo cui il consenso deve essere informato. Ai sensi dell’articolo 5 del regolamento, il requisito della trasparenza è uno dei principi fondamentali, strettamente legato ai principi di correttezza e liceità. Fornire informazioni agli interessati prima di ottenerne il consenso è fondamentale per consentire loro di prendere decisioni informate, capire a cosa stanno acconsentendo e, ad esempio, esercitare il diritto di revocare il consenso. Se il titolare del trattamento non fornisce informazioni accessibili, il controllo dell’utente diventa illusorio e il consenso non costituirà una base valida per il trattamento.

Se i requisiti per il consenso informato non sono rispettati il consenso non sarà valido e il titolare del trattamento potrebbe essere in violazione dell’articolo 6 del regolamento.

3.3.1. Requisiti minimi di contenuto del consenso “informato”

Affinché il consenso sia informato è necessario informare l’interessato su determinati elementi che sono fondamentali per effettuare una scelta. Di conseguenza, il Gruppo di lavoro ritiene che per ottenere un consenso valido siano necessarie almeno le seguenti informazioni:

- (i) l’identità del titolare del trattamento³⁰;
- (ii) la finalità di ciascuno dei trattamenti per i quali è richiesto il consenso³¹;
- (iii) quali (tipi di) dati saranno raccolti e utilizzati³²;
- (iv) l’esistenza del diritto di revocare il consenso³³;
- (v) informazioni sull’uso dei dati per un processo decisionale automatizzato ai sensi dell’articolo 22, paragrafo 2, lettera c)³⁴, se del caso; e

³⁰ Cfr. anche considerando 42 del regolamento generale sulla protezione dei dati: “[...] Ai fini di un consenso informato, l’interessato dovrebbe essere posto a conoscenza almeno dell’identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali. [...]”.

³¹ Ancora una volta, cfr. considerando 42 del regolamento generale sulla protezione dei dati.

³² Cfr. anche Gruppo di lavoro Articolo 29, Parere 15/2011 sulla definizione di consenso (WP 187), pagg. 22-23.

³³ Cfr. articolo 7, paragrafo 3, del regolamento generale sulla protezione dei dati.

- (vi) informazioni sui possibili rischi di trasferimenti di dati dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate come descritto nell'articolo 46³⁵.

Per quanto riguarda i punti i) e iii), il Gruppo di lavoro osserva che qualora più titolari del trattamento (congiunti) intendano basarsi sul medesimo consenso oppure qualora i dati debbano essere trasferiti o trattati da altri titolari del trattamento che intendono basarsi sul consenso iniziale, tutti questi titolari del trattamento devono essere indicati. Non è necessario fornire i nomi dei responsabili del trattamento, sebbene per rispettare gli articoli 13 e 14 del regolamento il titolare del trattamento dovrà fornire un elenco completo dei destinatari o delle categorie di destinatari, inclusi i responsabili del trattamento. Per concludere, il Gruppo di lavoro rileva che, a seconda delle circostanze e del contesto della fattispecie, potrebbero essere necessarie più informazioni per consentire all'interessato di comprendere veramente i trattamenti in corso.

3.3.2. Come fornire le informazioni

Il regolamento generale sulla protezione dei dati non prescrive la forma o il formato in cui è necessario fornire le informazioni affinché sia soddisfatto il requisito del consenso informato. Le informazioni valide possono quindi essere presentate in vari modi, ad esempio sotto forma di dichiarazioni scritte o verbali oppure di messaggi audio o video. Tuttavia, il regolamento prevede varie prescrizioni in merito al consenso informato, in particolare all'articolo 7, paragrafo 2, e al considerando 32. Ciò assicura un maggiore livello di chiarezza e accessibilità delle informazioni.

Quando richiede il consenso, il titolare del trattamento dovrebbe assicurarsi di usare sempre un linguaggio chiaro e semplice. Ciò significa che il messaggio dovrebbe essere facilmente comprensibile per una persona media, non solo per un avvocato. Il titolare del trattamento non può usare lunghe politiche sulla tutela della vita privata difficili da comprendere oppure informative piene di gergo giuridico. Il consenso deve essere chiaro e distinguibile dalle altre questioni, e deve essere presentato in una forma intelligibile e facilmente accessibile. Ciò significa, in sostanza, che le informazioni pertinenti per prendere una decisione informata sul consenso non possono essere nascoste all'interno delle condizioni generali di contratto/servizio³⁶.

Il titolare del trattamento deve garantire che il consenso sia fornito sulla base di informazioni che consentono all'interessato di identificare facilmente chi è il titolare del trattamento e di capire a cosa sta acconsentendo. Il titolare del trattamento deve descrivere chiaramente la finalità del trattamento dei dati per la quale richiede il consenso³⁷.

Ulteriori orientamenti specifici in materia di accessibilità sono stati forniti dal Gruppo di lavoro nelle linee guida sulla trasparenza. Quando il consenso deve essere prestato per via elettronica, la

³⁴ Cfr. anche le linee guida del Gruppo di lavoro sul processo decisionale automatizzato e la profilazione ai fini del regolamento 2016/679 (WP 251), punto IV.B, pag. 20 e successive.

³⁵ Ai sensi dell'articolo 49, paragrafo 1, lettera a), sono richieste informazioni specifiche sull'assenza delle garanzie di cui all'articolo 46, quando si richiede il consenso esplicito. Cfr. anche Gruppo di lavoro Articolo 29, Parere 15/2011 sulla definizione di consenso (WP 187), pag. 20.

³⁶ La dichiarazione di consenso deve essere designata come tale. Scrivere formulazioni del tipo "So che..." non soddisfa il requisito di un linguaggio chiaro.

³⁷ Cfr. articolo 4, punto 11 e articolo 7, paragrafo 2, del regolamento generale sulla protezione dei dati.

richiesta deve essere chiara e concisa. La messa a disposizione di informazioni “a livelli” e granulari può essere un modo appropriato per soddisfare il duplice obbligo di essere precisi e completi, da un lato, e comprensibili, dall’altro.

Il titolare del trattamento deve valutare il tipo di pubblico che fornisce dati personali alla sua organizzazione. Ad esempio, se il pubblico di destinazione include interessati minorenni, il titolare del trattamento deve assicurarsi che le informazioni siano comprensibili per i minori³⁸. Dopo aver individuato il pubblico, il titolare del trattamento deve stabilire le informazioni da fornire e, successivamente, il modo in cui fornirle.

L’articolo 7, paragrafo 2, concerne le dichiarazioni scritte di consenso preformulate che riguardano anche altre questioni. Quando il consenso viene richiesto nell’ambito di un contratto (cartaceo), la richiesta di consenso deve essere chiaramente distinguibile dal resto. Se il contratto cartaceo tratta numerosi aspetti che non sono collegati al consenso all’uso dei dati personali, quest’ultimo deve essere trattato in modo da distinguersi chiaramente oppure in un documento distinto. Analogamente, ai sensi del considerando 32³⁹, se il consenso viene richiesto per via elettronica, la richiesta di consenso deve essere separata e distinta, e non può semplicemente figurare in un paragrafo all’interno delle condizioni generali di contratto/servizio. Per tener conto degli schermi di piccole dimensioni o degli spazi ristretti per le informazioni, può essere appropriata, se del caso, una modalità di visualizzazione delle informazioni “a livelli” per evitare eccessivi disturbi all’esperienza dell’utente o alla progettazione del prodotto.

Per rispettare il regolamento il titolare del trattamento che si basa sul consenso dell’interessato deve adempiere anche gli obblighi di informazione separati di cui agli articoli 13 e 14. Nella pratica il rispetto degli obblighi di informazione e del requisito del consenso informato possono portare in molti casi a un approccio integrato. Tuttavia la presente sezione è scritta nella consapevolezza che possa sussistere un consenso “informato” valido anche quando non tutti gli aspetti di cui agli articoli 13 e/o 14 sono menzionati nel processo di ottenimento del consenso (questi punti dovrebbero ovviamente essere menzionati altrove, come ad esempio nell’informativa sulla protezione dei dati personali dell’azienda). Il Gruppo di lavoro ha emanato linee guida separate sul requisito della trasparenza.

[Esempio 12]

L’azienda X è un titolare del trattamento che ha ricevuto reclami per il fatto che agli interessati non è chiaro l’uso dei dati per il quale si chiede loro il consenso. L’azienda ritiene quindi sia necessario verificare se le informazioni contenute nella sua richiesta di consenso sono comprensibili per gli interessati. X organizza gruppi di prova volontari di categorie specifiche dei propri clienti e presenta loro nuovi aggiornamenti delle informazioni di consenso prima di comunicarle esternamente. La selezione di tale gruppo rispetta il principio di indipendenza ed avviene sulla base di norme che garantiscono un risultato rappresentativo e non distorto. Il gruppo riceve un questionario e indica cosa ha capito delle informazioni e quale valutazione darebbe sulla

³⁸ Cfr. anche il considerando 58 relativo a informazioni comprensibili per i minori.

³⁹ Cfr. anche il considerando 42 e la direttiva 93/13/CE, in particolare l’articolo 5 (linguaggio comprensibile e, in caso di dubbio, prevale l’interpretazione più favorevole al consumatore) e l’articolo 6 (invalidità di clausole abusive, il contratto continua a sussistere senza tali clausole abusive soltanto qualora sia ancora ragionevole, altrimenti l’intero contratto non è valido).

comprensibilità e pertinenza delle informazioni. Il titolare del trattamento continua a eseguire prove fino a quando i gruppi di prova non indicano che le informazioni sono comprensibili. X redige una relazione della prova e la tiene disponibile per riferimento futuro. Questo esempio mostra un modo con cui X può dimostrare che gli interessati hanno ricevuto informazioni chiare prima di acconsentire al trattamento dei loro dati personali da parte di X.

[Esempio 13]

Un'azienda effettua un trattamento di dati basandosi sul presupposto del consenso. L'azienda utilizza un'informativa sulla protezione dei dati a più livelli che include una richiesta di consenso. L'azienda comunica tutti i dettagli di base del titolare del trattamento e le attività di trattamento dei dati previste⁴⁰. Tuttavia, l'azienda non indica in che modo sia possibile contattare il responsabile della protezione dei dati nel primo livello di informazioni dell'informativa. Ai fini della base legittima e valida per il trattamento ai sensi dell'articolo 6, questo titolare del trattamento ha ottenuto un consenso "informato" valido, anche se i dati di contatto del responsabile della protezione dei dati non sono stati comunicati all'interessato (nel primo livello di informazioni), a norma dell'articolo 13, paragrafo 1, lettera b) o dell'articolo 14, paragrafo 1, lettera b).

3.4. Manifestazione di volontà inequivocabile

Il regolamento generale sulla protezione dei dati afferma chiaramente che il consenso richiede una dichiarazione o un'azione positiva inequivocabile da parte dell'interessato, il che significa che il consenso deve sempre essere espresso attraverso una dichiarazione o in modo attivo. Deve essere ovvio che l'interessato ha acconsentito al particolare trattamento.

L'articolo 2, lettera h), della direttiva 95/46/CE definisce il consenso come una "manifestazione di volontà con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento". L'articolo 4, punto 11, del regolamento generale sulla protezione dei dati si basa su tale definizione, chiarendo che il consenso, per essere valido, richiede una manifestazione *inequivocabile* mediante una *dichiarazione o azione positiva inequivocabile*, in conformità alle precedenti linee guida del Gruppo di lavoro.

Con "azione positiva inequivocabile" si intende che l'interessato deve aver intrapreso un'azione deliberata per acconsentire al trattamento specifico⁴¹. Il considerando 32 stabilisce ulteriori

⁴⁰ Si noti che quando l'identità del titolare del trattamento o la finalità del trattamento non è evidente dal primo livello di informazioni dell'informativa sulla protezione dei dati a più livelli (e si trovano in ulteriori sottolivelli), sarà difficile per il titolare del trattamento dimostrare che l'interessato ha espresso il proprio consenso informato, a meno che il titolare del trattamento non possa dimostrare che l'interessato in questione ha avuto accesso a tali informazioni prima di manifestare il proprio consenso.

⁴¹ Cfr. Documento di lavoro dei servizi della Commissione, Valutazione d'impatto, allegato 2, pag. 20 e anche pagg. 105-106 (in inglese): "Come sottolineato anche nel parere adottato dal Gruppo di lavoro Articolo 29 in materia di consenso, sembra fondamentale chiarire che affinché un consenso sia valido è necessario ricorrere a meccanismi che non lascino dubbi circa l'intenzione dell'interessato di acconsentire, pur chiarendo che, nel contesto dell'ambiente online, l'uso di opzioni predefinite che l'interessato è tenuto a modificare per rifiutare il trattamento ('consenso basato sul silenzio') non costituisce di per sé un consenso inequivocabile. Ciò darebbe alle persone un controllo maggiore sui propri dati, qualora il trattamento si basi sul loro consenso. Per quanto riguarda l'impatto sui titolari del trattamento dei dati, ciò non avrebbe un impatto rilevante poiché chiarisce e specifica meglio le implicazioni della direttiva attuale in relazione alle condizioni per ottenere un consenso valido e significativo da parte dell'interessato. In particolare, nella misura in cui il consenso 'esplicito' chiarisca (sostituendo 'inequivocabile') le modalità e la qualità del consenso e che non è inteso a estendere i casi e le situazioni in cui il consenso (esplicito) verrebbe utilizzato come base giuridica per il trattamento, l'impatto di tale misura sui titolari del trattamento non dovrebbe essere rilevante".

orientamenti al riguardo. Il consenso può essere raccolto attraverso una dichiarazione scritta o verbale (registrata), anche tramite mezzi elettronici.

Probabilmente il modo più rigoroso per soddisfare il criterio della “dichiarazione scritta” consiste nell’assicurarsi che l’interessato scriva una lettera o un messaggio di posta elettronica al titolare del trattamento spiegando ciò a cui acconsente esattamente. Tuttavia, spesso ciò non è realistico. Le dichiarazioni scritte possono avere forme e formati diversi che potrebbero essere conformi al regolamento generale sulla protezione dei dati.

Fatto salvo il diritto contrattuale (nazionale) in vigore, il consenso può essere ottenuto attraverso una dichiarazione verbale registrata, sebbene sia necessario prendere debita nota delle informazioni rese disponibili all’interessato prima dell’espressione del consenso. L’uso di caselle di adesione preselezionate non è valido ai sensi del regolamento. Il silenzio o l’inattività da parte dell’interessato, così come il semplice procedere all’uso di un servizio, non possono essere considerati una manifestazione attiva di scelta.

[Esempio 14]

Durante l’installazione di un software, l’applicazione richiede all’interessato di acconsentire a utilizzare segnalazioni di arresto anomalo non anonimizzate per migliorare il software. La richiesta di consenso è accompagnata da una informativa sulla protezione dei dati a più livelli che fornisce le necessarie informazioni. Selezionando attivamente la casella facoltativa “Acconsento”, l’utente è in grado di eseguire validamente una “azione positiva inequivocabile” per acconsentire al trattamento.

Il titolare del trattamento deve inoltre fare attenzione al fatto che il consenso non può essere ottenuto tramite la stessa azione con cui si accetta un contratto o le condizioni generali di servizio. L’accettazione globale delle condizioni generali di contratto/servizio non può essere considerata come un’azione positiva inequivocabile ai fini del consenso all’uso dei dati personali. Il regolamento generale sulla protezione dei dati non consente al titolare del trattamento di mettere a disposizione caselle preselezionate o procedure di rinuncia (*opt-out*) che richiedono un intervento dell’interessato per rifiutare il consenso (ad esempio “caselle di rinuncia”)⁴².

Quando il consenso deve essere prestato a fronte di una richiesta elettronica, quest’ultima non deve interferire *inutilmente* con l’utilizzo del servizio per il quale viene fornito il consenso⁴³. Un’azione positiva con cui l’interessato manifesta il proprio consenso può essere necessaria quando una modalità di espressione del consenso meno in violazione e meno invasiva potrebbe determinare ambiguità. Di conseguenza potrebbe essere necessario che, per essere efficace, la richiesta di consenso interrompa in una certa misura l’esperienza d’uso.

Tuttavia, nel contesto dei requisiti di cui al regolamento generale sulla protezione dei dati, il titolare del trattamento è libero di sviluppare un flusso di consenso adatto alla propria organizzazione. A

⁴² Cfr. articolo 7, paragrafo 2. Cfr. Documento di lavoro 02/2013 sull’ottenimento del consenso per i cookie (WP 208), pagg. 3-6.

⁴³ Cfr. considerando 32 del regolamento generale sulla protezione dei dati.

questo proposito, le azioni fisiche possono qualificarsi come un'azione positiva inequivocabile in conformità con il regolamento.

Il titolare del trattamento dovrebbe progettare meccanismi di consenso che operano in maniera chiara per gli interessati. Il titolare del trattamento deve evitare ambiguità e garantire che l'azione con cui viene espresso il consenso possa essere distinta da altre azioni. La semplice prosecuzione dell'uso normale di un sito web non è pertanto un comportamento dal quale si può dedurre una manifestazione di volontà dell'interessato a prestare il consenso a un trattamento proposto.

[Esempio 15]

Far scorrere una barra su uno schermo, muovere la mano davanti a una telecamera intelligente, ruotare lo smartphone in senso orario o fargli compiere un movimento a otto potrebbero essere opzioni per indicare un consenso a patto che siano fornite informazioni chiare e sia inequivocabile che l'azione richiesta implica un consenso a una richiesta specifica (istruzione esemplificativa: se fai scorrere questa barra verso sinistra, acconsenti all'uso delle informazioni X per la finalità Y. Ripeti il movimento per confermare). Il titolare del trattamento deve essere in grado di dimostrare che il consenso è stato ottenuto in questo modo e l'interessato deve poter revocare il consenso con la stessa facilità con cui lo ha espresso.

[Esempio 16]

Scorrere un sito verso il basso o sfogliarne le pagine non sono azioni chiare e positive, poiché l'avviso che continuare a scorrere il sito costituirà un'espressione di consenso può essere difficile da distinguere e/o può essere trascurato inavvertitamente quando l'interessato scorre rapidamente grandi quantità di testo; inoltre tali azioni non sono sufficientemente inequivocabili.

Nel contesto digitale molti servizi necessitano di dati personali per funzionare, quindi gli interessati ricevono quotidianamente molteplici richieste di consenso che implicano risposte tramite clic e scorrimenti. Ne può derivare un certo grado di stanchezza a cliccare: se occorre farlo troppe volte, l'effettivo effetto di avvertimento dei meccanismi di consenso diminuisce.

Si può quindi verificare la situazione in cui le domande di consenso non vengono più lette, con un conseguente rischio specifico per l'interessato, in quanto in genere viene richiesto il consenso per azioni che in linea di principio sono illecite in assenza di consenso. Il regolamento generale sulla protezione dei dati impone al titolare del trattamento l'obbligo di sviluppare soluzioni per affrontare questo problema.

Un esempio spesso citato nel contesto online è l'ottenimento del consenso dell'utente di Internet tramite le impostazioni del browser. Tali impostazioni dovrebbero essere sviluppate in linea con le condizioni per la validità del consenso previste dal regolamento, come ad esempio il fatto che il consenso deve essere granulare per ciascuna delle finalità previste e che le informazioni da fornire per ottenere il consenso devono indicare i titolari del trattamento.

In ogni caso, il consenso deve sempre essere ottenuto prima che il titolare del trattamento inizi a trattare i dati personali per i quali è necessario il consenso. Il Gruppo di lavoro ha costantemente affermato nei precedenti pareri che il consenso dovrebbe essere espresso prima dell'avvio

dell'attività di trattamento⁴⁴. Sebbene il regolamento non prescriva esplicitamente all'articolo 4, punto 11, che il consenso debba essere manifestato prima dell'attività di trattamento, ciò è chiaramente implicito. La rubrica dell'articolo 6 e il verbo "ha espresso" di cui all'articolo 6, paragrafo 1, lettera a), confermano tale interpretazione. Conseguentemente dall'articolo 6 e dal considerando 40 che prima di iniziare un trattamento dei dati deve sussistere una base legittima e valida. Pertanto, il consenso dovrebbe essere espresso prima che abbia luogo l'attività di trattamento. In linea di principio può essere sufficiente chiedere il consenso dell'interessato una sola volta. Tuttavia, il titolare del trattamento deve ottenere un nuovo consenso specifico qualora le finalità del trattamento dei dati cambino dopo che è stato ottenuto il consenso o qualora sia prevista una finalità aggiuntiva.

4. Ottenimento del consenso esplicito

Il consenso esplicito è richiesto in talune circostanze nelle quali emergono gravi rischi per la protezione dei dati e in cui si ritiene quindi appropriato un livello elevato di controllo individuale sui dati personali. Il regolamento generale sulla protezione dei dati richiede il consenso esplicito all'articolo 9 per il trattamento di categorie particolari di dati, all'articolo 49⁴⁵ per i trasferimenti di dati verso paesi terzi od organizzazioni internazionali in assenza di garanzie adeguate, e all'articolo 22 per i processi decisionali automatizzati relativi alle persone fisiche, compresa la profilazione⁴⁶.

In base al regolamento, prerequisito per l'ottenimento di un consenso "conforme" è una "dichiarazione o un'azione positiva inequivocabile". Poiché il requisito del consenso "conforme" nel regolamento è già elevato a un livello superiore rispetto al requisito del consenso di cui alla direttiva 95/46/CE, è necessario chiarire quali sforzi supplementari debba attuare il titolare del trattamento per ottenere il consenso *esplicito* dell'interessato in linea con il regolamento.

Il termine *esplicito* si riferisce al modo in cui il consenso è espresso dall'interessato e significa che l'interessato deve fornire una dichiarazione esplicita di consenso. Un modo ovvio per assicurarsi che il consenso sia esplicito consisterebbe nel confermare espressamente il consenso in una dichiarazione scritta. Se del caso, il titolare del trattamento potrebbe assicurarsi che la dichiarazione

⁴⁴ Il Gruppo di lavoro ha sostenuto questa posizione in maniera coerente fin dal parere 15/2011 sulla definizione di consenso (WP 187), pagg. 35-37.

⁴⁵ Ai sensi dell'articolo 49, paragrafo 1, lettera a), del regolamento generale sulla protezione dei dati, il consenso esplicito può revocare il divieto di trasferimenti di dati verso paesi che non dispongono di livelli adeguati di protezione dei dati a norma di legge. Si consulti anche il documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1 della direttiva

95/46/CE del 24 ottobre 1995 (WP 114), pag. 11, nell'ambito del quale il Gruppo di lavoro ha indicato che il consenso per i trasferimenti di dati che si verificano periodicamente o su base continuativa è inappropriato.

⁴⁶ All'articolo 22 il regolamento generale sulla protezione dei dati introduce disposizioni destinate a proteggere gli interessati da un processo decisionale basato esclusivamente sul trattamento automatizzato, nonché dalla profilazione. Le decisioni adottate su tale base sono consentite nel rispetto di determinate condizioni legali. Il consenso svolge un ruolo chiave in questo meccanismo di protezione, in quanto l'articolo 22, paragrafo 2, lettera c), del regolamento generale sulla protezione dei dati, chiarisce che un titolare del trattamento può svolgere un processo decisionale automatizzato, compresa la profilazione, che può influire in maniera significativa sulle persone fisiche, con il consenso esplicito dell'interessato. Il Gruppo di lavoro ha prodotto linee guida distinte su questo tema: Gruppo di lavoro Articolo 29, *Guidelines on Automated decision-making and Profiling for the purposes of Regulation 2016/679* [Linee guida sul processo decisionale automatizzato e la profilazione ai fini del regolamento 2016/679], 3 ottobre 2017 (WP 251).

scritta sia firmata dall'interessato, al fine di dissipare tutti i possibili dubbi e la potenziale mancanza di prove in futuro⁴⁷.

Tuttavia la dichiarazione firmata non è l'unico modo per ottenere il consenso esplicito e non si può affermare che il regolamento prescriva dichiarazioni scritte e firmate in tutte le circostanze che richiedono un consenso esplicito valido. Ad esempio, nel contesto digitale od online, l'interessato può emettere la dichiarazione richiesta compilando un modulo elettronico, inviando un'e-mail, caricando un documento scansionato con la propria firma oppure utilizzando una firma elettronica. In teoria, anche l'uso di dichiarazioni verbali può essere sufficientemente specifico per ottenere un consenso esplicito valido, tuttavia può essere difficile per il titolare del trattamento dimostrare che tutte le condizioni per la validità del consenso esplicito siano state soddisfatte quando la dichiarazione è stata registrata.

Un'organizzazione può anche ottenere il consenso esplicito tramite una conversazione telefonica, a condizione che le informazioni sulla scelta siano corrette, intelligibili e chiare e che venga richiesta una conferma specifica da parte dell'interessato (ad esempio premendo un pulsante o fornendo una conferma verbale).

[Esempio 17]

Il titolare del trattamento può ottenere il consenso esplicito da un visitatore del proprio sito web mettendo a disposizione una schermata di consenso esplicito contenente caselle di controllo "Sì" e "No", a condizione che il testo indichi chiaramente il consenso, ad esempio con una dicitura del tipo "In questo modo acconsento al trattamento dei miei dati" e non ad esempio tramite una formulazione del tipo "Mi è chiaro che i miei dati saranno trattati". Va da sé che devono essere soddisfatte le condizioni per il consenso informato e le altre condizioni per la validità del consenso.

[Esempio 18]

Una clinica per chirurgia estetica chiede il consenso esplicito di un paziente al trasferimento della cartella clinica a un esperto per un secondo parere sulla condizione del paziente. La cartella clinica è costituita da un file digitale. Data la natura specifica delle informazioni in questione, la clinica chiede la firma elettronica dell'interessato per ottenere un consenso esplicito valido e per essere in grado di dimostrare che è stato ottenuto detto consenso esplicito⁴⁸.

Anche la verifica in due fasi del consenso può essere un modo per assicurarsi che il consenso esplicito sia valido. Ad esempio, l'interessato riceve un'e-mail che gli notifica l'intenzione del titolare del trattamento di trattare una cartella contenente dati medici. Il titolare del trattamento spiega nell'e-mail che chiede il consenso all'uso di un insieme specifico di informazioni per una finalità specifica. Se l'interessato acconsente all'utilizzo dei dati, il titolare del trattamento gli chiede una risposta via e-mail contenente la dichiarazione "Acconsento". Dopo l'invio della risposta, l'interessato riceve un link di verifica da cliccare oppure un messaggio SMS con un codice di verifica, in maniera da confermare il consenso.

⁴⁷ Cfr. anche Gruppo di lavoro Articolo 29, Parere 15/2011 sulla definizione di consenso (WP 187), pag. 29.

⁴⁸ Questo esempio non pregiudica il regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

L'articolo 9, paragrafo 2, non riconosce il trattamento "necessario all'esecuzione di un contratto" come un'eccezione al divieto generale di trattare categorie particolari di dati. Di conseguenza i titolari del trattamento e gli Stati membri che rientrano nel contesto di applicazione di tale circostanza dovrebbero esaminare le eccezioni specifiche di cui all'articolo 9, paragrafo 2, lettere da b) a j). Qualora non si applichi nessuna delle eccezioni da b) a j), l'ottenimento del consenso esplicito in conformità con le condizioni per il consenso valido previste dal regolamento rimane l'unica eccezione lecita possibile per trattare tali dati.

[Esempio 19]

La compagnia aerea Holiday Airways offre un servizio di assistenza di viaggio ai passeggeri che non possono viaggiare senza assistenza, ad esempio a causa di una disabilità. Un cliente prenota un volo da Amsterdam a Budapest e richiede l'assistenza di viaggio per salire a bordo dell'aereo. Holiday Airways richiede al passeggero di fornire informazioni sulle sue condizioni di salute per essere in grado di organizzare i servizi appropriati (ad esempio, una sedia a rotelle a disposizione alla porta di imbarco o un assistente che viaggia con il passeggero da A a B). Holiday Airways richiede il consenso esplicito per trattare i dati sanitari del passeggero allo scopo di organizzare l'assistenza richiesta per il viaggio. I dati trattati sulla base del consenso devono essere necessari per il servizio richiesto. Inoltre i voli per Budapest sono disponibili anche senza assistenza di viaggio. Si noti che poiché tali dati sono necessari per la prestazione del servizio richiesto, l'articolo 7, paragrafo 4, non si applica.

[Esempio 20]

Un'azienda di successo è specializzata nella fornitura di occhiali da sci e da snowboard su misura e altri tipi di occhiali personalizzati per gli sport all'aria aperta. L'idea è che le persone possano indossare tali occhiali senza dover portare anche gli occhiali da vista. La società riceve ordini presso un punto centrale e consegna prodotti in tutta l'UE a partire da un'unica sede. Per poter fornire i propri prodotti personalizzati ai clienti miopi, tale titolare del trattamento richiede il consenso all'uso delle informazioni sulle condizioni di vista dei clienti. I clienti forniscono i dati sanitari necessari - ad esempio i dati della loro prescrizione - online quando effettuano l'ordine. Senza questi dati non sarebbe possibile fornire gli occhiali personalizzati richiesti. L'azienda offre anche una serie di occhiali con valori correttivi standardizzati. I clienti che non desiderano condividere i dati sanitari possono optare quindi per le versioni standard. Di conseguenza, nel caso di specie, è richiesto un consenso esplicito ai sensi dell'articolo 9 e il consenso può essere considerato come espresso liberamente.

5. Condizioni aggiuntive per l'ottenimento di un consenso valido

Il regolamento generale sulla protezione dei dati introduce requisiti che impongono al titolare del trattamento di prevedere modalità aggiuntive per garantire che ottiene un consenso valido, lo mantiene e sia in grado di dimostrarne l'esistenza. L'articolo 7 del stabilisce queste condizioni aggiuntive per il consenso valido tramite disposizioni specifiche sulla conservazione di registrazioni del consenso e sul diritto di revocare facilmente il consenso espresso. L'articolo 7 si applica anche al consenso di cui ad altri articoli del regolamento, ad esempio gli articoli 8 e 9. Si riportano in appresso orientamenti sull'ulteriore requisito di dimostrare l'esistenza di un consenso valido e sulla revoca del consenso.

5.1. Dimostrazione del consenso

L'articolo 7, paragrafo 1, prevede in maniera chiara l'obbligo esplicito del titolare del trattamento di dimostrare il consenso dell'interessato. Conformemente a tale articolo, l'onere della prova è a carico del titolare del trattamento.

Il considerando 42 afferma: *“Per i trattamenti basati sul consenso dell’interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l’interessato ha acconsentito al trattamento”*.

Il titolare del trattamento è libero di sviluppare metodi propri per rispettare tale disposizione in maniera adatta alle sue attività quotidiane. Allo stesso tempo, l’obbligo in capo al titolare del trattamento di dimostrare l’ottenimento di un consenso valido non dovrebbe di per sé portare a quantità eccessive di trattamenti di dati supplementari. Ciò significa che il titolare del trattamento dovrebbe disporre di dati sufficienti per mostrare un collegamento al trattamento (ossia per fornire la prova che è stato ottenuto il consenso) ma non dovrebbe raccogliere più informazioni di quanto necessario.

Spetta al titolare del trattamento dimostrare che è stato ottenuto un consenso valido dall’interessato. Il regolamento non prescrive esattamente come ciò debba avvenire. Tuttavia, il titolare del trattamento deve essere in grado di dimostrare che l’interessato nel caso specifico ha espresso il proprio consenso. Fintantoché dura l’attività di trattamento dei dati in questione, sussiste l’obbligo di dimostrare l’esistenza del consenso. Al termine dell’attività di trattamento, la prova del consenso deve essere conservata non più di quanto strettamente necessario per adempiere ad obblighi giuridici o per l’accertamento, l’esercizio o la difesa di un diritto in sede giudiziaria, in conformità con l’articolo 17, paragrafo 3, lettere b) ed e).

Ad esempio, il titolare del trattamento può tenere una registrazione delle dichiarazioni di consenso ricevute onde poter dimostrare come e quando è stato ottenuto il consenso, e rendere dimostrabili le informazioni fornite all’interessato al momento dell’espressione del consenso. Il titolare del trattamento deve anche essere in grado di dimostrare che l’interessato è stato informato e che la propria procedura ha soddisfatto tutti i criteri pertinenti per la validità del consenso. La logica alla base di tale obbligo è che il titolare del trattamento deve essere responsabilizzato in relazione all’ottenimento di un consenso valido dell’interessato e ai meccanismi di consenso che ha messo in atto. Ad esempio, in un contesto online, il titolare del trattamento può conservare informazioni sulla sessione in cui è stato espresso il consenso, unitamente alla documentazione della procedura di consenso al momento della sessione, oltre a una copia delle informazioni presentate all’interessato in quel momento. Non sarebbe sufficiente fare semplicemente riferimento a una corretta configurazione del sito web.

[Esempio 21]

Un ospedale istituisce un programma di ricerca scientifica per il quale sono necessarie cartelle cliniche odontoiatriche di pazienti. I partecipanti sono selezionati tramite telefonate a pazienti che hanno volontariamente accettato di essere inseriti in un elenco di candidati che possono essere contattati a tale fine. Il titolare del trattamento chiede il consenso esplicito degli interessati all’uso della loro cartella clinica odontoiatrica. Il consenso viene ottenuto durante una telefonata, registrando una dichiarazione verbale dell’interessato nella quale quest’ultimo conferma di acconsentire all’uso dei suoi dati per le finalità del programma.

Il regolamento non specifica alcun termine per la durata del consenso. Questa dipenderà dal contesto, dalla portata del consenso originale e dalle aspettative dell’interessato. Se i trattamenti

cambiano o si evolvono in maniera considerevole, il consenso originale non è più valido e occorrerà un nuovo consenso.

Come migliore prassi il Gruppo di lavoro raccomanda di aggiornare il consenso a intervalli appropriati. Fornire nuovamente tutte le informazioni contribuisce a garantire che l'interessato rimanga ben informato su come vengono utilizzati i suoi dati e su come può esercitare i suoi diritti⁴⁹.

5.2.Revoca del consenso

Il regolamento generale sulla protezione dei dati dà ampio rilievo alla revoca del consenso. Le disposizioni e i considerando relativi alla revoca del consenso possono considerarsi una codificazione dell'interpretazione data al riguardo nei pareri del Gruppo di lavoro⁵⁰.

L'articolo 7, paragrafo 3, prescrive che il titolare del trattamento deve garantire che l'interessato possa revocare il consenso in qualsiasi momento con la stessa facilità con cui lo ha espresso. Il regolamento non dispone che l'espressione e la revoca del consenso debbano avvenire sempre allo stesso modo.

Tuttavia, quando il consenso viene prestato per via elettronica con un solo clic di mouse, un solo scorrimento o premendo un tasto, l'interessato deve, in pratica, poterlo revocare con altrettanta facilità. Se il consenso è espresso attraverso un'interfaccia utente specifica di servizio (ad esempio un sito web, un'applicazione, un account protetto, l'interfaccia di un dispositivo IoT oppure posta elettronica), è indubbio che l'interessato deve poterlo revocare tramite la medesima interfaccia elettronica, poiché il passaggio a un'altra interfaccia per la sola revoca richiederebbe uno sforzo eccessivo. Inoltre, l'interessato dovrebbe poter revocare il consenso senza subire pregiudizio. Ciò significa, tra l'altro, che il titolare del trattamento deve consentire la revoca senza spese o senza abbassare i livelli del servizio⁵¹.

[Esempio 22]

Un festival musicale vende biglietti tramite un agente di vendita di biglietti online. All'atto della vendita del biglietto viene richiesto il consenso all'uso dei dettagli di contatto per finalità di marketing. Per acconsentire o meno a tale finalità, il cliente può cliccare su "Sì" oppure su "No". Il titolare del trattamento informa il cliente che può revocare il consenso contattando gratuitamente un call center nei giorni lavorativi tra le 8:00 e le 17:00. Il titolare del trattamento di questo esempio non rispetta l'articolo 7, paragrafo 3, del regolamento. Telefonare durante l'orario di lavoro per revocare il consenso è più oneroso rispetto a un clic di mouse per prestare il consenso attraverso il venditore di biglietti online, che è aperto 24 ore al giorno, 7 giorni la settimana.

⁴⁹ Cfr. linee guida del Gruppo di lavoro sulla trasparenza. [Citazione da finalizzare quando disponibile]

⁵⁰ Il Gruppo di lavoro ha discusso questo argomento nel parere sul consenso [cfr. parere 15/2011 sulla definizione di consenso (WP 187), pagg. 11, 14, 23, 32 e 38-39] e, tra l'altro, nel parere sull'uso dei dati relativi all'ubicazione. [cfr. parere 5/2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto (WP 115), pag. 7].

⁵¹ Cfr. anche i seguenti pareri del Gruppo di lavoro: parere 4/2010 sul codice di condotta europeo della FEDMA per l'utilizzazione dei dati personali nel marketing diretto (WP 174) e parere 5/2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto (WP 115).

In base al regolamento il requisito della facilità della revoca è un elemento necessario del consenso valido. Se il diritto di revoca non soddisfa i requisiti del regolamento, il meccanismo di consenso del titolare del trattamento non è conforme al regolamento. Come menzionato nella sezione 3.1 sulla condizione del consenso *informato*, a norma dell'articolo 7, paragrafo 3, del regolamento il titolare del trattamento deve informare l'interessato del diritto di revoca prima che quest'ultimo presti effettivamente il consenso. Inoltre, nel contesto dell'obbligo di trasparenza, il titolare del trattamento deve informare l'interessato sulle modalità di esercizio dei suoi diritti⁵².

Di norma, se il consenso viene revocato, tutti i trattamenti dei dati basati sul consenso avvenuti prima della revoca (e in conformità con il regolamento) rimangono leciti, tuttavia il titolare del trattamento deve interrompere le attività di trattamento interessate. Qualora non sussista un'altra base legittima per il trattamento (ad esempio l'ulteriore archiviazione) dei dati, questi dovrebbero essere cancellati dal titolare del trattamento⁵³.

Come già accennato, prima di raccogliere i dati è molto importante che il titolare del trattamento valuti le finalità per le quali i dati sono effettivamente trattati e le basi legittime del trattamento. Spesso le aziende hanno bisogno di dati personali per diverse finalità e il trattamento si basa su più basi legittime, ad esempio il trattamento di dati dei clienti può basarsi su un contratto e sul consenso. Di conseguenza, la revoca del consenso non implica che il titolare del trattamento deve cancellare i dati trattati per una finalità che si basa sull'esecuzione del contratto stipulato con l'interessato. Il titolare del trattamento dovrebbe pertanto precisare chiaramente sin dall'inizio la finalità che si applica a ciascun dato e le basi legittime del trattamento.

Il titolare del trattamento deve cancellare i dati trattati sulla base del consenso non appena questo viene revocato, supponendo che non vi siano altre finalità che giustificano l'ulteriore conservazione⁵⁴.

Oltre a questa situazione, prevista dall'articolo 17, paragrafo 1, lettera b), l'interessato può chiedere la cancellazione di altri dati che lo riguardano trattati sulla base di un'altra base legittima, ad esempio l'articolo 6, paragrafo 1, lettera b)⁵⁵. Il titolare del trattamento è tenuto a valutare se la prosecuzione del trattamento dei dati in questione sia appropriata, anche in assenza di una richiesta di cancellazione da parte dell'interessato⁵⁶.

In caso di revoca del consenso, il titolare del trattamento, se vuole continuare a trattare i dati personali in base a un'altra base legittima, non può passare tacitamente dal consenso (che è stato revocato) all'altra base legittima. Qualsiasi modifica della base legittima del trattamento deve essere

⁵² Il considerando 39 del regolamento generale sulla protezione dei dati, che fa riferimento ai suoi articoli 13 e 14, afferma che “[è] opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento”.

⁵³ Cfr. articolo 17, paragrafo 1, lettera b) e articolo 17, paragrafo 3 del regolamento generale sulla protezione dei dati.

⁵⁴ In tal caso, l'altra finalità che giustifica il trattamento deve disporre di una propria base legittima distinta. Ciò non significa che il titolare del trattamento possa passare dal consenso a un'altra base legittima, cfr. la seguente sezione 6.

⁵⁵ Cfr. articolo 17, comprese le eccezioni che possono essere applicabili, e il considerando 65 del regolamento generale sulla protezione dei dati.

⁵⁶ Cfr. anche articolo 5, paragrafo 1, lettera e), del regolamento generale sulla protezione dei dati.

notificata all'interessato in conformità ai requisiti di informazione di cui agli articoli 13 e 14, nonché al principio generale di trasparenza.

6. Interazione tra il consenso e altre basi legittime di cui all'articolo 6 del regolamento generale sulla protezione dei dati

L'articolo 6 stabilisce le condizioni per la liceità del trattamento dei dati personali ed elenca sei basi legittime su cui il titolare del trattamento può fondarsi. L'applicazione di una di queste sei basi deve essere stabilita prima di procedere al trattamento e in relazione a una finalità specifica⁵⁷.

È importante osservare che, se sceglie di basarsi sul consenso per ogni parte del trattamento, il titolare del trattamento deve essere preparato a rispettare tale scelta e interrompere la parte del trattamento in caso di revoca del consenso. Comunicare che i dati saranno trattati sulla base del consenso mentre in realtà si fa affidamento su un'altra base legittima sarebbe fundamentalmente scorretto nei confronti dell'interessato.

In altre parole, il titolare del trattamento non può passare dal consenso ad altre basi legittime. Ad esempio non può ricorrere retroattivamente alla base dell'interesse legittimo in caso di problemi di validità del consenso. Poiché ha l'obbligo di comunicare la base legittima al momento della raccolta dei dati personali, il titolare del trattamento deve aver deciso la base legittima prima della raccolta dei dati.

7. Settori specifici di interesse nel regolamento generale sulla protezione dei dati

7.1. Minori (articolo 8)

Rispetto alla direttiva attuale, il regolamento generale sulla protezione dei dati crea un ulteriore livello di protezione per il trattamento dei dati personali delle persone fisiche vulnerabili, in particolare i minori. L'articolo 8 introduce obblighi supplementari per garantire una maggiore protezione dei dati dei minori in relazione ai servizi della società dell'informazione. I motivi di tale protezione rafforzata sono specificati nel considerando 38: *“I minori [...] possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali [...]”*. Sempre al considerando 38 si afferma che *“[t]ale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore”*. La precisazione “in particolare” indica che la protezione specifica non si limita al marketing o alla profilazione, ma si estende alla più ampia “raccolta di dati personali relativi ai minori”.

L'articolo 8, paragrafo 1, stabilisce che laddove si applichi il consenso, per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui il consenso è prestato o autorizzato dal titolare

⁵⁷ Ai sensi dell'articolo 13, paragrafo 1, lettera c) e/o dell'articolo 14, paragrafo 1, lettera c), il titolare del trattamento è tenuto a informarne l'interessato.

della responsabilità genitoriale⁵⁸. Per quanto concerne il limite di età per il consenso valido, il regolamento offre flessibilità, in quanto gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

Come menzionato nella sezione 3.1. sul consenso informato, le informazioni fornite dal titolare del trattamento devono essere comprensibili per il pubblico al quale sono destinate, con particolare attenzione alla posizione dei minori. Per ottenere il “consenso informato” di un minore, il titolare del trattamento deve spiegare in un linguaggio chiaro e semplice, comprensibile per i minori, come intende trattare i dati raccolti⁵⁹. Se spetta al genitore prestare il consenso, può essere necessario fornire un insieme di informazioni che consentano agli adulti di prendere una decisione informata.

Da quanto precede risulta evidente che l'articolo 8 si applica esclusivamente quando sono soddisfatte le seguenti condizioni:

- il trattamento è correlato all'offerta diretta di servizi della società dell'informazione ai minori^{60, 61};
- il trattamento è basato sul consenso.

7.1.1. Servizio della società dell'informazione

Al fine di determinare la portata dell'espressione “servizio della società dell'informazione”, il regolamento generale sulla protezione dei dati, all'articolo 4, punto 25, fa riferimento alla direttiva (UE) 2015/1535.

Per valutare la portata di tale definizione, il Gruppo di lavoro fa riferimento anche alla giurisprudenza della Corte di giustizia⁶². La Corte di giustizia ha affermato che la nozione di *servizi della società dell'informazione* interessa contratti e altri servizi conclusi o trasmessi online.

⁵⁸ Fatta salva la possibilità per il diritto degli Stati membri di derogare al limite di età, cfr. articolo 8, paragrafo 1.

⁵⁹ Il considerando 58 del regolamento generale sulla protezione dei dati riafferma questo obbligo, dichiarando che, se del caso, il titolare del trattamento dovrebbe assicurarsi di fornire informazioni comprensibili per i minori.

⁶⁰ Ai sensi dell'articolo 4, paragrafo 25, del regolamento generale sulla protezione dei dati, per servizio della società dell'informazione si intende un servizio di cui all'articolo 1, paragrafo 1, lettera b), della direttiva 2015/1535: “b) *‘servizio’*: qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Ai fini della presente definizione si intende per: i) *‘a distanza’*: un servizio fornito senza la presenza simultanea delle parti; ii) *‘per via elettronica’*: un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici o altri mezzi elettromagnetici; iii) *‘a richiesta individuale di un destinatario di servizi’*: un servizio fornito mediante trasmissione di dati su richiesta individuale”. Nell'allegato I di detta direttiva figura un elenco indicativo di servizi non contemplati da tale definizione. Cfr. anche il considerando 18 della direttiva 2000/31/CE.

⁶¹ Secondo la Convenzione delle Nazioni Unite sulla protezione dei minori, articolo 1, “[...] si intende per fanciullo ogni essere umano avente un'età inferiore a diciott'anni, salvo se abbia raggiunto prima la maturità in virtù della legislazione applicabile”, cfr. Nazioni Unite, risoluzione 44/25 dell'Assemblea Generale del 20 novembre 1989 (Convenzione sui diritti del fanciullo).

⁶² Cfr. Corte di giustizia, 2 dicembre 2010, causa C-108/09, (*Ker-Optika*), punti 22 e 28. In relazione ai “servizi compositi”, il Gruppo di lavoro fa riferimento anche alla causa C-434/15 (*Asociacion Profesional Elite Taxi/Uber Systems Spain SL*), punto 40, al quale si afferma che un servizio della società dell'informazione che costituisce parte integrante di un servizio generale la cui componente principale non è un servizio della società dell'informazione (in questo caso un servizio di trasporto), non rientra nella qualificazione di “servizio della società dell'informazione”.

Laddove un servizio presenti due componenti economicamente indipendenti, una delle quali è la componente online (ad esempio l'offerta e l'accettazione di un'offerta nel contesto della conclusione di un contratto, o le informazioni relative a prodotti o servizi, comprese le attività di marketing) e l'altra è la consegna fisica o la distribuzione di merci, la prima rientra nella definizione di servizio della società dell'informazione, mentre la seconda no. La consegna online di un servizio rientrerebbe nell'espressione *servizio della società dell'informazione* di cui all'articolo 8 del regolamento generale sulla protezione dei dati.

7.1.2. Forniti direttamente a un minore

La precisazione “offerta diretta [...] ai minori” indica che l'articolo 8 si applica ad alcuni ma non a tutti i servizi della società dell'informazione. A tale riguardo, se un prestatore di servizi della società dell'informazione chiarisce ai potenziali utenti che il servizio è offerto esclusivamente a persone aventi almeno 18 anni, e ciò non è smentito da altri elementi (come il contenuto del sito o piani di marketing), allora il servizio non sarà considerato fornito direttamente a un minore e l'articolo 8 non si applicherà.

7.1.3. Età

Il regolamento specifica che “[g]li Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni”. Nel tenere conto del pubblico destinatario dei suoi servizi, il titolare del trattamento deve tenere presenti le diverse leggi nazionali. In particolare, il titolare del trattamento che fornisce un servizio transfrontaliero non può sempre fare affidamento sul solo rispetto della legge dello Stato membro in cui ha lo stabilimento principale, perché potrebbe dover rispettare le leggi nazionali di ciascuno Stato membro in cui offre i servizi della società dell'informazione, a seconda che lo Stato membro scelga di usare come criterio di legge il luogo dello stabilimento principale del titolare del trattamento oppure il luogo di residenza dell'interessato. Nello scegliere il criterio da usare gli Stati membri devono considerare innanzitutto l'interesse superiore del minore. Il Gruppo di lavoro incoraggia gli Stati membri a cercare una soluzione armonizzata.

Nel fornire servizi della società dell'informazione ai minori sulla base del consenso, il titolare del trattamento dovrà compiere ogni ragionevole sforzo per verificare che l'utente abbia raggiunto l'età del consenso digitale, e le misure dovrebbero essere proporzionate alla natura e ai rischi delle attività di trattamento.

Se l'utente afferma di aver raggiunto l'età del consenso digitale, il titolare del trattamento può effettuare controlli appropriati per verificare la veridicità della dichiarazione. Sebbene il regolamento non richieda esplicitamente di intraprendere sforzi ragionevoli per verificare l'età, tale necessità è implicita, poiché se un minore presta il consenso senza avere l'età sufficiente per prestare un consenso valido per proprio conto il trattamento dei dati sarà illecito.

Se l'utente dichiara di avere un'età inferiore a quella del consenso digitale, il titolare del trattamento può accettare tale dichiarazione senza ulteriori verifiche, ma dovrà ottenere l'autorizzazione dei genitori e verificare che la persona che esprime il consenso sia titolare della responsabilità genitoriale.

La verifica dell'età non deve comportare un eccessivo trattamento di dati. Il meccanismo scelto per verificare l'età dell'interessato dovrebbe prevedere una valutazione del rischio del trattamento proposto. In alcune situazioni a basso rischio, potrebbe essere adeguato richiedere al nuovo abbonato al servizio di rivelare il proprio anno di nascita oppure di compilare un modulo in cui dichiara di (non) essere un minore⁶³. Qualora dovessero sorgere dubbi, il titolare del trattamento dovrebbe riesaminare i meccanismi di verifica dell'età nel caso di specie e valutare se siano necessari controlli alternativi⁶⁴.

7.1.4. Consenso del minore e responsabilità genitoriale

Per quanto riguarda l'autorizzazione del titolare della responsabilità genitoriale, il regolamento non prevede modalità pratiche per raccogliere il consenso del genitore o per stabilire che qualcuno è autorizzato a prestare il consenso⁶⁵. Di conseguenza il Gruppo di lavoro raccomanda l'adozione di un approccio proporzionato, in linea con l'articolo 8, paragrafo 2, e l'articolo 5, paragrafo 1, lettera c), del regolamento (minimizzazione dei dati). Un approccio proporzionato potrebbe essere quello di concentrarsi sull'ottenimento di una quantità limitata di informazioni, ad esempio i dettagli di contatto di un genitore o del tutore.

La ragionevolezza degli sforzi, in termini di verifica tanto che l'utente abbia l'età sufficiente per esprimere il consenso quanto che la persona che esprime il consenso a nome del minore sia il titolare della responsabilità genitoriale, può dipendere dai rischi inerenti al trattamento e dalla tecnologia disponibile. Nei casi a basso rischio, può essere sufficiente la verifica della responsabilità genitoriale a mezzo posta elettronica. Viceversa, nei casi ad alto rischio, può essere opportuno chiedere ulteriori prove affinché il titolare del trattamento sia in grado di verificare e conservare le informazioni di cui all'articolo 7, paragrafo 1⁶⁶. I servizi di verifica di terzi fidati possono offrire soluzioni che riducono al minimo la quantità di dati personali che il titolare del trattamento deve trattare autonomamente.

[Esempio 23]

Una piattaforma di gioco online vuole assicurarsi che i clienti minorenni si abbonino ai servizi esclusivamente con il consenso dei genitori o tutori. Il titolare del trattamento segue questi passaggi:

passaggio 1: chiede all'utente di indicare se ha meno o più di 16 anni (o dell'età alternativa per il consenso digitale).

Se l'utente dichiara di avere un'età inferiore a quella per il consenso digitale:

⁶³ Sebbene non sia una soluzione ideale in tutti i casi, è un esempio per rispondere a tale disposizione.

⁶⁴ Cfr. Gruppo di lavoro Articolo 29, *Opinion 5/2009 on social networking services* [Parere 5/2009 sui servizi di rete sociale] (WP 163) (in inglese).

⁶⁵ Il Gruppo di lavoro osserva che non sempre il titolare della responsabilità genitoriale è il genitore naturale del minore e che la responsabilità genitoriale può essere detenuta da più parti che possono comprendere tanto persone fisiche quanto persone giuridiche.

⁶⁶ Ad esempio a un genitore o un tutore potrebbe essere chiesto di effettuare un pagamento di 0,01 EUR al titolare del trattamento tramite una transazione bancaria, nonché una breve conferma nella riga descrittiva della transazione che il titolare del conto bancario è titolare della responsabilità genitoriale rispetto all'utente. Se del caso, dovrebbe essere previsto un metodo alternativo di verifica per evitare un indebito trattamento discriminatorio nei confronti delle persone che non dispongono di un conto bancario.

passaggio 2: il servizio informa il minore della necessità che un genitore o il tutore acconsenta o autorizzi il trattamento prima che venga erogato il servizio. All'utente viene quindi richiesto di rivelare l'indirizzo di posta elettronica di un genitore o del tutore;

passaggio 3: il servizio contatta il genitore o il tutore e ne ottiene il consenso al trattamento tramite posta elettronica e adotta misure ragionevoli per ottenere la conferma che l'adulto abbia la responsabilità genitoriale;

passaggio 4: in caso di reclami, la piattaforma adotta ulteriori provvedimenti per verificare l'età dell'abbonato. Se soddisfa gli altri requisiti del consenso, la piattaforma può soddisfare i criteri supplementari di cui all'articolo 8 del regolamento seguendo questi passaggi.

L'esempio mostra che il titolare del trattamento può mettersi in una posizione tale da dimostrare che sono stati compiuti sforzi ragionevoli per garantire che è stato ottenuto un consenso valido in relazione ai servizi forniti a un minore. L'articolo 8, paragrafo 2, aggiunge in particolare che *“[i]l titolare del trattamento si adopera in ogni modo ragionevole per verificare che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili”*.

Spetta al titolare del trattamento stabilire quali misure siano appropriate in un caso specifico. Di norma, il titolare del trattamento dovrebbe evitare soluzioni di verifica che implicino una raccolta eccessiva di dati personali.

Il Gruppo di lavoro riconosce che in determinati casi la verifica è difficile, ad esempio se il minore che presta il consenso non ha ancora lasciato un'“impronta di identità” o se la responsabilità genitoriale non è facilmente verificabile. Tale aspetto può essere preso in considerazione nel decidere quali sforzi siano ragionevoli, tuttavia ci si aspetta anche che il titolare del trattamento tenga sotto costante controllo i suoi processi e la tecnologia disponibile.

Per quanto riguarda l'autonomia dell'interessato a manifestare il consenso al trattamento dei dati personali e il pieno controllo sul trattamento, nel momento in cui raggiunge l'età del consenso digitale l'interessato può confermare, modificare o revocare il consenso prestato o autorizzato dal titolare della responsabilità genitoriale.

In pratica, ciò significa che se il minore non intraprende alcuna azione, il consenso prestato o autorizzato dal titolare della responsabilità genitoriale in relazione al trattamento dei dati personali forniti prima dell'età del consenso digitale rimarrà un presupposto valido per il trattamento.

Una volta raggiunta l'età del consenso digitale, il minore avrà la possibilità di revocare il consenso, in linea con l'articolo 7, paragrafo 3. In conformità con i principi di correttezza e responsabilizzazione, il titolare del trattamento deve informare il minore di questa possibilità⁶⁷.

È importante sottolineare che, ai sensi del considerando 38, il consenso di un genitore o del tutore non è richiesto nel contesto di servizi di prevenzione o consulenza offerti direttamente al minore. Ad esempio, per i servizi di protezione dei minori offerti online ai minori tramite un servizio di chat non occorre la previa autorizzazione dei genitori.

⁶⁷ Inoltre, gli interessati dovrebbero essere consapevoli del diritto all'oblio di cui all'articolo 17, che è particolarmente rilevante per il consenso dato quando l'interessato era ancora un minore, cfr. considerando 63.

Infine, il regolamento prevede che le norme relative ai requisiti di autorizzazione genitoriale nei confronti dei minori non pregiudicano “le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l’efficacia di un contratto rispetto a un minore”. Di conseguenza i requisiti per la validità del consenso all’uso dei dati relativi a minori rientrano in un quadro giuridico da considerarsi distinto dal diritto contrattuale nazionale. Le presenti linee guida non affrontano pertanto la questione se sia lecito o meno per un minore concludere contratti online. Entrambi i regimi giuridici possono essere applicati simultaneamente e l’ambito di applicazione del regolamento generale sulla protezione dei dati non include l’armonizzazione delle disposizioni nazionali di diritto contrattuale.

7.2. Ricerca scientifica

La definizione di finalità di ricerca scientifica ha implicazioni sostanziali per la gamma di attività di trattamento di dati che un titolare del trattamento può intraprendere. L’espressione “ricerca scientifica” non è definita nel regolamento. Il considerando 159 afferma: “[...] *Nell’ambito del presente regolamento, il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato. [...]*”, tuttavia il Gruppo di lavoro ritiene che tale nozione non possa essere estesa oltre il suo significato comune e che per “ricerca scientifica” in questo contesto si intenda un progetto di ricerca istituito in conformità con le pertinenti norme metodologiche e deontologiche settoriali, in linea con le buone prassi.

Quando il consenso costituisce la base legittima per condurre ricerche in conformità con il regolamento, tale consenso all’uso dei dati personali dovrebbe essere distinto dagli altri requisiti del consenso che fungono da norme deontologiche od obbligo procedurale. Un esempio di obbligo procedurale, in cui il trattamento si basa non sul consenso ma su un’altra base giuridica, figura nel regolamento sulla sperimentazione clinica. Nel contesto del diritto in materia di protezione dei dati, quest’ultima forma di consenso potrebbe essere considerata una garanzia aggiuntiva⁶⁸. Allo stesso tempo, il regolamento generale sulla protezione dei dati non limita l’applicazione dell’articolo 6 al solo consenso, per quanto riguarda il trattamento di dati per fini di ricerca. Fintantoché sussistono garanzie adeguate, quali i requisiti di cui all’articolo 89, paragrafo 1, e il trattamento è corretto, lecito, trasparente e conforme alle norme sulla minimizzazione dei dati e ai diritti individuali, potrebbero essere disponibili altre basi legittime quali l’articolo 6, paragrafo 1, lettera e) o f)⁶⁹. Ciò vale anche per le categorie particolari di dati ai sensi della deroga di cui all’articolo 9, paragrafo 2, lettera j)⁷⁰.

Il considerando 33 sembra consentire una certa flessibilità al grado di specificazione e granularità del consenso nel contesto della ricerca scientifica. Esso afferma: “*In molti casi non è possibile individuare pienamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, dovrebbe essere consentito agli interessati di prestare il*

⁶⁸ Cfr. anche il considerando 161 del regolamento generale sulla protezione dei dati.

⁶⁹ L’articolo 6, paragrafo 1, lettera c), può anche essere applicabile a parti dei trattamenti specificamente richiesti dalle disposizioni di legge, come la raccolta di dati affidabili e solidi secondo il protocollo approvato dallo Stato membro ai sensi del regolamento sulla sperimentazione clinica.

⁷⁰ La sperimentazione specifica di medicinali può aver luogo sulla base di una legislazione UE o nazionale ai sensi dell’articolo 9, paragrafo 2, lettera i).

proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica. Gli interessati dovrebbero avere la possibilità di prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista”.

In primo luogo, va osservato che il considerando 33 non inficia gli obblighi relativi al requisito del consenso specifico. Ciò significa che, in linea di principio, i progetti di ricerca scientifica possono includere dati personali sulla base del consenso soltanto se hanno una finalità ben descritta. Nei casi in cui le finalità del trattamento dei dati nell’ambito di un progetto di ricerca scientifica non possono essere specificate in via preliminare, il considerando 33 consente in via eccezionale che la finalità possa essere descritta a un livello più generale.

Tenuto conto delle condizioni rigorose stabilite dall’articolo 9 in merito al trattamento di categorie particolari di dati, il Gruppo di lavoro rileva che quando categorie particolari di dati vengono trattate sulla base del consenso esplicito, l’applicazione dell’approccio flessibile di cui al considerando 33 sarà soggetta a un’interpretazione più rigorosa e richiede un elevato livello di controllo.

Considerato nel suo insieme, il regolamento generale sulla protezione dei dati non può essere interpretato in maniera tale da consentire al titolare del trattamento di aggirare il principio chiave della specificazione delle finalità per le quali viene richiesto il consenso dell’interessato.

Quando non è possibile specificare appieno le finalità della ricerca, il titolare del trattamento deve cercare altri modi per garantire il rispetto dell’essenza dei requisiti del consenso, ad esempio permettendo agli interessati di acconsentire a una finalità di ricerca in termini più generali e a fasi specifiche di un progetto di ricerca che si sa già sin dall’inizio avranno luogo. Mano a mano che la ricerca avanza, sarà quindi possibile ottenere il consenso per le fasi successive del progetto prima dell’inizio della fase corrispondente. Tuttavia, tale consenso dovrebbe comunque essere in linea con le norme deontologiche applicabili alla ricerca scientifica.

Inoltre, il titolare del trattamento può applicare ulteriori garanzie in questi casi. L’articolo 89, paragrafo 1, ad esempio, sottolinea la necessità di prevedere garanzie nelle attività di trattamento di dati per fini di ricerca scientifica o storica o per fini statistici. Tali finalità “*[sono] soggett[e] a garanzie adeguate per i diritti e le libertà dell’interessato, in conformità del presente regolamento*”. Come possibili garanzie si menzionano la minimizzazione dei dati, l’anonimizzazione e la sicurezza dei dati⁷¹. L’anonimizzazione rappresenta la soluzione preferita non appena la finalità della ricerca possa essere conseguita senza il trattamento di dati personali.

⁷¹ Cfr. ad esempio il considerando 156. Il trattamento di dati personali a fini scientifici dovrebbe inoltre essere conforme ad altre normative pertinenti come quella sulle sperimentazioni cliniche; cfr. considerando 156 che menziona il regolamento (UE) n. 536/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, sulla sperimentazione clinica di medicinali per uso umano. Cfr. anche il parere del Gruppo di lavoro 15/2011 sulla definizione di consenso (WP 187), pag. 8: “*l’ottenimento del consenso non esonera il titolare del trattamento dagli obblighi di cui all’articolo 6 con riferimento ai principi di lealtà, necessità e proporzionalità, oltre che di qualità dei dati. Per esempio, anche qualora il trattamento dei dati personali poggia sul consenso dell’utilizzatore, ciò di per sé non legittima una raccolta dei dati supplementare rispetto allo scopo specifico. [...] In linea di principio, il consenso non dev’essere considerato come una*

La trasparenza è un'ulteriore garanzia quando le circostanze della ricerca non consentono un consenso specifico. La mancanza di specificazione della finalità può essere compensata dalla fornitura periodica, da parte del titolare del trattamento, di informazioni sullo sviluppo della finalità durante l'avanzamento del progetto di ricerca, in maniera tale che, nel tempo, il consenso sia il più specifico possibile. In tal modo l'interessato ha quanto meno una conoscenza di base dello stato di avanzamento, che gli consente di valutare se esercitare o meno, ad esempio, il diritto di revoca del consenso ai sensi dell'articolo 7, paragrafo 3⁷².

Anche la messa a disposizione di un piano di ricerca esaustivo al quale gli interessati possano fare riferimento prima di esprimere il loro consenso potrebbe contribuire a compensare una mancanza di specificazione delle finalità⁷³. Il piano di ricerca dovrebbe specificare nella maniera più chiara possibile i quesiti che la ricerca si pone e i metodi di lavoro previsti. Il piano di ricerca potrebbe altresì contribuire al rispetto dell'articolo 7, paragrafo 1, in quanto, per poter dimostrare che il consenso è valido, il titolare del trattamento è tenuto a dimostrare quali informazioni erano disponibili agli interessati al momento dell'espressione del consenso.

È importante ricordare che quando il consenso costituisce la base legittima del trattamento, l'interessato deve avere la possibilità di revocarlo. Il Gruppo di lavoro rileva che la revoca del consenso potrebbe compromettere taluni tipi di ricerca scientifica che richiedono dati che possano essere collegati a persone fisiche, tuttavia il regolamento è chiaro nello stabilire che il consenso può essere revocato e che il titolare del trattamento deve tenerne conto: non vi è alcuna esenzione a questo requisito per la ricerca scientifica. Se riceve una richiesta di revoca, il titolare del trattamento deve, in linea di principio, cancellare immediatamente i dati personali se vuole continuare a utilizzare i dati per le finalità della ricerca⁷⁴.

7.3. Diritti dell'interessato

Se l'attività di trattamento di dati si basa sul consenso, i diritti dell'interessato subiscono alcune ripercussioni: l'interessato può avere il diritto alla portabilità dei dati (articolo 20), ma non il diritto di opposizione (articolo 21), sebbene il diritto di revocare il consenso in qualsiasi momento possa portare a un esito analogo.

Gli articoli da 16 a 20 del regolamento generale sulla protezione dei dati indicano che (quando il trattamento dei dati è basato sul consenso) l'interessato ha il diritto alla cancellazione, in caso di revoca del consenso, e i diritti di limitazione del trattamento, rettifica e accesso⁷⁵.

forma di esonero dagli altri principi di protezione dei dati, bensì come una salvaguardia. Esso è, in prima linea, un motivo di liceità e non comporta una rinuncia all'applicazione di altri principi”.

⁷² Possono essere pertinenti anche altre misure di trasparenza. Quando i titolari del trattamento svolgono un trattamento di dati a fini scientifici, nonostante non sia possibile fornire informazioni complete sin dall'inizio, possono comunque designare un referente specifico al quale gli interessati possono rivolgere eventuali quesiti.

⁷³ Tale possibilità si può riscontrare nell'articolo 14, paragrafo 1, dell'attuale legge sui dati personali della Finlandia (*Henkilötietolaki*, 523/1999).

⁷⁴ Cfr. anche il parere del Gruppo di lavoro 05/2014 sulle tecniche di anonimizzazione (WP 216).

⁷⁵ Nei casi in cui determinate attività di trattamento dei dati sono limitate ai sensi dell'articolo 18, può essere necessario il consenso dell'interessato per annullare le limitazioni interessate.

8. Consenso ottenuto a norma della direttiva 95/46/CE

I titolari del trattamento che attualmente trattano dati sulla base del consenso conformemente alla normativa nazionale in materia di protezione dei dati non sono automaticamente tenuti a rinnovare completamente tutte le relazioni di consenso con gli interessati in preparazione dell'entrata in vigore del regolamento generale sulla protezione dei dati. Il consenso ottenuto continua ad essere valido nella misura in cui è in linea con le condizioni stabilite nel regolamento generale sulla protezione dei dati.

È importante che prima del 25 maggio 2018 i titolari del trattamento rivedano in maniera approfondita i processi di lavoro e le registrazioni correnti, al fine di accertarsi che i consensi in essere soddisfino quanto previsto dal regolamento generale sulla protezione dei dati (cfr. considerando 171 del regolamento generale sulla protezione dei dati⁷⁶). In pratica, il regolamento generale sulla protezione dei dati fissa prescrizioni più rigorose riguardo all'attuazione di meccanismi di consenso e introduce nuovi requisiti che impongono ai titolari del trattamento di modificare i meccanismi di consenso, non di riscrivere soltanto le politiche in materia di protezione dei dati⁷⁷.

Ad esempio, poiché il regolamento impone al titolare del trattamento di essere in grado di dimostrare che ha ottenuto un consenso valido, tutti i presunti consensi dei quali non viene conservato alcun riferimento si considereranno automaticamente al di sotto del livello di consenso fissato dal regolamento e dovranno quindi essere rinnovati. Analogamente, poiché il regolamento richiede una “dichiarazione o un'azione positiva inequivocabile”, tutti i presunti consensi basati su una forma di azione più implicita dell'interessato (ad esempio una casella di adesione preselezionata) non saranno conformi al livello di consenso stabilito dal regolamento.

Inoltre, per poter dimostrare l'ottenimento del consenso o fornire indicazioni più granulari sulle volontà dell'interessato, il titolare del trattamento potrebbe dover effettuare un riesame delle operazioni e dei sistemi informativi. Devono essere disponibili meccanismi che consentano agli interessati di revocare facilmente il consenso e devono essere fornite informazioni su come revocare il consenso. Se le procedure esistenti per l'ottenimento e la gestione del consenso non soddisfano i livelli previsti dal regolamento, il titolare del trattamento dovrà ottenere un nuovo consenso conforme al regolamento.

⁷⁶ Il considerando 171 del regolamento generale sulla protezione dei dati afferma: “Il presente regolamento dovrebbe abrogare la direttiva 95/46/CE. Il trattamento già in corso alla data di applicazione del presente regolamento dovrebbe essere reso conforme al presente regolamento entro un periodo di due anni dall'entrata in vigore del presente regolamento. Qualora il trattamento si basi sul consenso a norma della direttiva 95/46/CE, non occorre che l'interessato presti nuovamente il suo consenso, se questo è stato espresso secondo modalità conformi alle condizioni del presente regolamento, affinché il titolare del trattamento possa proseguire il trattamento in questione dopo la data di applicazione del presente regolamento. Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate”.

⁷⁷ Come indicato nell'introduzione, il regolamento generale sulla protezione dei dati fornisce ulteriori chiarimenti e specifiche sui requisiti per ottenere e dimostrare un consenso valido. Molti dei nuovi requisiti si basano sul parere 15/2011 sul consenso.

D'altro canto, poiché non tutti gli elementi indicati negli articoli 13 e 14 devono sempre essere presenti come condizione per un consenso informato, gli obblighi di informazione estesa ai sensi del regolamento non si oppongono necessariamente alla continuità del consenso prestato prima dell'entrata in vigore del regolamento (cfr. precedente pagina 15). La direttiva 95/46/CE non prevedeva alcun obbligo di informare gli interessati in merito alla base del trattamento.

Qualora ritenga che il consenso ottenuto in base alla vecchia normativa non rispetti le norme per il consenso fissate dal regolamento, il titolare del trattamento deve agire per conformarvisi, ad esempio mediante il rinnovo del consenso in un maniera conforme al regolamento. Ai sensi del regolamento non è possibile passare da una base legittima a un'altra. Se il titolare del trattamento non è in grado di rinnovare il consenso in maniera conforme né è in grado, come circostanza una tantum, di conformarsi al regolamento basando il trattamento dei dati su una base legittima diversa garantendo nel contempo che la prosecuzione del trattamento corrisponda ai principi di correttezza e responsabilizzazione, le attività di trattamento devono essere interrotte. In ogni caso, il titolare del trattamento deve rispettare i principi di un trattamento lecito, corretto e trasparente.

***** FINE DEL DOCUMENTO *****