17 / IT WP259

Rev.01

Gruppo dell'articolo 29

Orientamenti in materia di autorizzazione ai sensi del regolamento 2016/679

Adottato il 28 Novembre 2017, riveduta da

ultimo e adottato il 10 Aprile 2018

IL GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL

TRATTAMENTO DEI DATI PERSONALI

istituito dalla direttiva 95/46 / CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995,

visti gli articoli 29 e 30,

visto il suo regolamento,

Avrà adottato gli orientamenti presenti:

Contenuto

1. introduzione

Queste linee guida forniscono un'analisi approfondita della nozione di consenso regolamento 2016/679, il regolamento sulla protezione dei dati generali (qui di seguito: GDPR). Il concetto del consenso come usato nella direttiva sulla protezione dei dati (qui di seguito: la direttiva 95/46 / CE) e nella direttiva e-privacy fino ad oggi, si è evoluto. Il GDPR fornisce ulteriori chiarimenti e specifiche dei requisiti per l'ottenimento e dimostrando valido consenso. Queste linee guida si concentrano su questi cambiamenti, fornendo una guida pratica per garantire il rispetto del GDPR e sviluppando nel parere 15/2011 sul consenso. L'obbligo è sui controller di innovare di trovare nuove soluzioni che operano all'interno dei parametri di legge e meglio supportano la protezione dei dati personali e gli interessi dei titolari dei dati.

Consenso rimane una delle sei basi legali per elaborare i dati personali, come elencate all'articolo 6 del GDPR. [1] Quando si inizia le attività che comportano il trattamento dei dati personali, un controller deve sempre prendere tempo per valutare quale sarebbe il terreno legale appropriata per il trattamento previsto.

In generale, il consenso può essere solo una base legale appropriata se l'interessato è offerto di controllo e viene offerta una scelta vera e propria in materia di accettare o rifiutare i termini offerti o in declino senza danno. Quando si chiede il consenso, un controllore ha il dovere di valutare se soddisferà tutti i requisiti per ottenere un valido consenso. Se ottenuti nel pieno rispetto della GDPR, il consenso è uno strumento che permette di controllare le persone interessate nel corso dell'esistenza o meno di dati personali che li riguardano saranno trattati. In caso contrario, il controllo della persona interessata diventa illusorio e il consenso sarà una base valida per l'elaborazione, rendendo l'attività di trattamento illecito. [2]

Il Gruppo di lavoro articolo 29 attuale (WP29) Opinioni sul consenso [3] rimanere rilevante, purché sia coerente con il nuovo quadro giuridico, come la codifica GDPR WP29 orientamenti e buone pratiche generali esistenti e la maggior parte degli elementi chiave del consenso rimangono gli stessi sotto la GDPR. Pertanto, in questo documento, WP29 amplia e completa precedenti pareri su argomenti specifici che includono riferimento al consenso ai sensi della direttiva 95/46 / CE, piuttosto che la loro sostituzione.

Come indicato nel parere 15/2011 sulla definizione sul consenso, invitando la gente ad accettare un'operazione di trattamento dei dati dovrebbe essere soggetta a rigorosi requisiti, in quanto riguarda i diritti fondamentali delle persone interessate e il controllore vuole impegnarsi in un'operazione di trattamento che sarebbe illegale, pur senza il consenso della persona interessata. [4] Il ruolo cruciale del consenso è sottolineata dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Inoltre, ottenere il consenso, inoltre, non nega o sminuisce in alcun modo gli obblighi del controller di osservare i principi di trattamento sancito dalla GDPR, in particolare l'articolo 5 del GDPR per quanto riguarda la correttezza, necessità e proporzionalità, così come la qualità dei dati. Anche se il trattamento dei dati personali è

---

[1] Articolo 9 GDPR fornisce un elenco di possibili deroghe al divieto di trattamento di categorie particolari di dati. Una delle eccezioni elencate è la situazione in cui l'interessato fornisce il consenso esplicito per l'utilizzo di questi dati.

[2] Vedi anche il parere 15/2011 sulla definizione del consenso (WP 187), pp. 6-8, e / o parere 06/2014 sulla nozione di interessi legittimi del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46 / CE (WP 217), pp. 9, 10, 13 e 14.

[3] Più in particolare, parere 15/2011 sulla definizione del consenso (WP 187).

[4] Parere 15/2011, pag sulla definizione del consenso (WP 187), p. 8

basata sul consenso della persona, questo non sarebbe legittimare raccolta di dati che non è necessaria in relazione ad uno scopo specifico di lavorazione ed essere fondamentalmente sleale. [5]

Nel frattempo, WP29 è consapevole della revisione della direttiva e-privacy (2002/58 / CE). La nozione di consenso nel progetto di regolamento della privacy resta legato alla nozione di consenso nel GDPR. [6]

Le organizzazioni sono probabilmente bisogno di consenso ai sensi dello strumento e-privacy per la maggior parte dei messaggi di marketing on-line o chiamate di marketing, e metodi di monitoraggio on-line, tra cui con l'uso di cookie o applicazioni o altro software. WP29 ha già fornito consigli e linee guida per il legislatore europeo in merito alla Proposta di regolamento relativo e-privacy. [7]

Per quanto riguarda la direttiva e-privacy esistente, WP29 fa notare che i riferimenti al abrogata la direttiva 95/46 / CE, devono intendersi come riferimenti al GDPR. [8] Questo vale anche per i riferimenti al consenso nella direttiva 2002/58 / CE, in quanto il regolamento privacy non sarà (ancora) in vigore dal 25 maggio 2018. In base all'articolo 95 GDPR, obblighi supplementari in relazione al trattamento in relazione alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione non deve essere imposta nella misura in cui l'e-privacy direttiva impone obblighi specifici con lo stesso obiettivo. WP29 sottolinea che i requisiti per il consenso alle GDPR non sono considerati un 'obbligo aggiuntivo', ma piuttosto come precondizioni per l'elaborazione legittima. Pertanto, le condizioni GDPR per ottenere un valido consenso sono applicabili in situazioni che rientrano nel campo di applicazione della direttiva e-privacy.

2. Il consenso di cui all'articolo 4 (11) del GDPR

L'articolo 4 (11) del GDPR definisce il consenso come: *"Qualsiasi dato liberamente, specifica indicazione, informato e inequivocabile della volontà della persona interessata con cui lui o lei, da una dichiarazione o da una chiara azione affermativa, significa consenso al trattamento dei dati personali che lo riguardano o lei."*

Il concetto di base del consenso rimane simile a quella ai sensi della direttiva 95/46 / CE e il consenso è uno dei motivi legittimi su cui trattamento dei dati personali deve essere basata, ai sensi dell'articolo 6 del GDPR. [9] Oltre alla definizione modificata di cui all'articolo 4 (11), il GDPR fornisce ulteriori

---

[5] Vedi anche il parere 15/2011 sulla definizione del consenso (WP 187), e l'articolo 5 GDPR.

[6] Ai sensi dell'articolo 9 della proposta di regolamento e-privacy, la definizione di e le condizioni per il consenso di cui agli articoli 4 (11) e l'articolo 7 del GDPR applicare.

[7] Vedere Parere 03/2016 sulla valutazione e la revisione della direttiva e-privacy (WP 240).

[8] Si veda l'articolo 94 GDPR.

[9] Il consenso è stato definito nella direttiva 95/46 / CE come " *qualsiasi volontà libera, specifica e informata con la volontà con la quale la persona significa accettare di dati personali che lo riguardano in fase di elaborazione* "Che deve essere ' *inequivocabilmente* 'Al fine di rendere il trattamento dei dati personali legittimi (articolo 7 (a), della direttiva 95/46 / CE)). Vedere WP29 parere 15/2011 sulla definizione del consenso (WP 187) per gli esempi sull'opportunità del consenso basi lecito. In questo parere, WP29 ha fornito indicazioni per distinguere in cui il consenso è una base legale appropriata da quelli in cui fare affidamento sul terreno interesse legittimo (magari con la possibilità di opt-out) è sufficiente o un rapporto contrattuale sarebbe raccomandato. Vedi anche WP29 parere 06/2014, paragrafo III.1.2, pag. 14 e oltre. consenso esplicito è anche una delle deroghe al divieto di trattamento di categorie particolari di dati: vedasi articolo 9 GDPR.

orientamento all'articolo 7 e ai punti 32, 33, 42, e 43 su come il regolatore deve agire per rispettare gli elementi principali del requisito consenso.

Infine, l'inclusione di disposizioni specifiche e recital sulla revoca del consenso conferma che l'autorizzazione deve essere una decisione reversibile e che ci rimane un certo grado di controllo sul lato della persona.

3. Elementi di consenso valido

L'articolo 4 (11) del GDPR stabilisce che il consenso della persona interessata qualsiasi:

- dato liberamente,
- specifica,
- informati e
- l'indicazione inequivocabile della volontà della persona interessata con cui lui o lei, da una dichiarazione o da una chiara azione affermativa, significa consenso al trattamento dei dati personali che lo riguardano o lei.

Nelle sezioni seguenti, si è analizzato in che misura la formulazione dell'articolo 4 (11) richiede controller di cambiare le loro richieste di consenso / forme, al fine di garantire il rispetto del GDPR. [10]

3.1. Libero / gratuità [11]

L'elemento “libera” implica vera scelta e controllo per gli interessati. Come regola generale, il GDPR prescrive che se la persona interessata non ha scelta vera e propria, si sente in dovere di acconsentire o durerà conseguenze negative se non acconsentono, allora il consenso non sarà valido. [12] Se il consenso si avvolge come una parte non negoziabile delle condizioni si presume che non sia stato dato liberamente. Di conseguenza, il consenso non sarà considerato di essere libero se l'interessato è in grado di rifiutare o revocare il proprio consenso senza danno. [13] La nozione di squilibrio tra il controllore e l'interessato viene preso in considerazione dalla GDPR.

Nel valutare se il consenso è liberamente dato, si dovrebbe anche tener conto della situazione specifica del consenso legatura contratti o la fornitura di un servizio come descritto nell'articolo 7 (4). Articolo 7 (4) è stata redatta in modo non esaustivo dalle parole “tra l'altro”, il che significa che ci può essere una serie di altre situazioni che rientrano nel campo di questa disposizione. In termini generali, qualsiasi

---

[10] Per la guida per quanto riguarda le attività di trattamento in corso sulla base di consenso nella direttiva 95/46, vedere il capitolo 7 del presente documento e il considerando 171 del GDPR.

[11] In diversi pareri, il gruppo di lavoro Articolo 29 ha esplorato i limiti del consenso in situazioni in cui non può essere dato liberamente. Questo è stato in particolare il caso nel suo parere 15/2011 sulla definizione del consenso (WP 187), il 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 dati nel contesto lavorativo (WP48), e secondo parere 4/2009 sul trattamento dei dati da parte dell'Agenzia mondiale anti-doping (WADA) (standard internazionale per la tutela della privacy e dati personali, sulle disposizioni relative del Codice WADA e sulla altri problemi di privacy nel contesto della lotta contro il doping nello sport dalla WADA e organizzazioni (nazionali) anti-doping (WP 162).

[12] Vedere Parere 15/2011 sulla definizione del consenso (WP187), p. 12

[13] Considerando da 42, 43 e GDPR WP29 parere 15/2011 sulla definizione di consenso, adottata il 13 luglio 2011, (WP 187), p. 12.

elemento di pressione contenuti o influenza sulla persona (che può manifestarsi in molti modi diversi), che impedisce una persona interessata di esercitare la propria volontà, esporrà il consenso valido.

[Esempio 1]
Un app mobile per il fotoritocco chiede ai suoi utenti di avere la loro localizzazione GPS attivato per l'uso dei suoi servizi. L'applicazione racconta anche i suoi utenti che potranno utilizzare i dati raccolti per scopi pubblicitari comportamentali. Né la localizzazione geo o la pubblicità comportamentale online sono necessari per la fornitura del servizio di photo editing e vanno oltre la fornitura del servizio principale fornito. Poiché gli utenti non possono utilizzare l'applicazione senza consentendo a questi scopi, il consenso non può essere considerata come dato liberamente.

3.1.1. Squilibrio di potere

Considerando 43 [14] indica chiaramente che è improbabile che **autorità pubbliche** può contare su consenso alla trasformazione di ogni volta che il controllore è un ente pubblico, v'è spesso un chiaro squilibrio di potere nella relazione tra il controllore e l'interessato. E 'anche chiaro nella maggior parte dei casi che la persona interessata non avrà alternative realistiche per accettare la trasformazione (termini) di questo controller. WP29 ritiene che vi siano altre basi legali che sono, in linea di principio, più appropriati per l'attività delle autorità pubbliche. [15]

Fatte salve queste considerazioni generali, l'uso del consenso come base legale per l'elaborazione dei dati da parte delle autorità pubbliche non è totalmente esclusa nell'ambito del quadro giuridico del GDPR. I seguenti esempi mostrano che l'uso di consenso può essere appropriato in determinate circostanze.

[Esempio 2] Un locale comune ha in programma lavori di manutenzione stradale. Come i lavori stradali possono interrompere il traffico per un lungo periodo, il comune offre ai suoi cittadini la possibilità di iscriversi a una mailing list per ricevere gli aggiornamenti sullo stato di avanzamento dei lavori e sui ritardi previsti. Il comune chiarisce che non v'è alcun obbligo di partecipare e chiede il consenso di utilizzare indirizzi e-mail per questo (esclusiva) scopo. I cittadini che non consenso non perdere su qualsiasi servizio di base del comune o l'esercizio di qualsiasi diritto, in modo che siano in grado di dare o negare il loro consenso a tale uso dei dati liberamente. Tutte le informazioni sulle opere stradali sarà disponibile anche sul sito web del comune.

[Esempio 3] Un individuo che possiede un terreno ha bisogno di determinati documenti da entrambi sua municipalità locale e dal governo provinciale in cui si trova il comune. Entrambi gli organismi pubblici richiedono le stesse informazioni per il rilascio del permesso, ma non sono l'accesso di ogni altri database. Pertanto, sia chiedere le stesse informazioni e il proprietario del terreno invia i suoi dettagli per entrambi gli enti pubblici. Il Comune e la Provincia chiedono il suo consenso per unire i file, al fine di evitare procedure di duplicati e la corrispondenza. Entrambi gli enti pubblici garantiscono che questo è facoltativo e che le richieste di permesso sarà ancora da lavorare separatamente, se si decide di non acconsentire alla fusione dei propri dati. Il proprietario del terreno è in grado di dare il consenso alle autorità al fine di fondere i file liberamente.

[14] Considerando 43 stati GDPR: *"Per assicurare che il consenso è liberamente dato, il consenso non dovrebbe fornire un motivo giuridico valido per il trattamento dei dati personali in un caso specifico in cui v'è un chiaro squilibrio tra la persona e il controllore, in particolare quando il controllore è un autorità pubblica ed è quindi improbabile che il consenso è stato dato gratuitamente in tutte le circostanze di quella specifica situazione. (...)"*

[15] Si veda l'articolo 6 GDPR, in particolare i paragrafi (1c) e (1e).

[Esempio 4] Una scuola pubblica chiede agli studenti per il consenso ad utilizzare le loro fotografie in una rivista studentesca stampata. Il consenso in queste situazioni sarebbe una scelta vera e propria finché gli studenti non verrà negato l'istruzione o servizi e potrebbe impedire l'installazione delle stesse senza alcun pregiudizio. 16

Uno squilibrio di potenza si verifica anche nel **occupazione** contesto. [17] Data la dipendenza che deriva dal rapporto datore di lavoro / dipendente, è improbabile che la persona è in grado di negare la sua / suo consenso datore di lavoro per l'elaborazione dei dati senza provare la paura o rischio reale di effetti negativi a seguito di un rifiuto. È improbabile che un dipendente sarebbe in grado di rispondere liberamente a una richiesta di consenso dalla sua / il suo datore di lavoro, ad esempio, attivare sistemi di monitoraggio, come Camera-osservazione in un posto di lavoro, o per compilare i moduli di valutazione, senza sentire alcuna pressione consentire. [18] Pertanto, WP29 ritiene problematico per i datori di lavoro per elaborare i dati personali dei dipendenti attuali o futuri sulla base del consenso in quanto è improbabile che possa essere dato liberamente. Per la maggior parte del loro trattamento sul posto di lavoro, la base legale non può e non deve essere il consenso dei lavoratori (articolo 6 (1) (a)), a causa della natura del rapporto tra datore di lavoro e lavoratore. [19]

Tuttavia, questo non significa che i datori di lavoro possono mai fare affidamento sul consenso come base legale per l'elaborazione. Ci possono essere situazioni in cui è possibile per il datore di dimostrare che il consenso effettivamente è liberamente determinato. Dato lo squilibrio di potere tra un datore di lavoro ed i suoi collaboratori, i dipendenti possono solo dare un consenso libero, in circostanze eccezionali, quando non avrà conseguenze negative a tutti anche se non danno il consenso. [20]

[Esempio 5]
Una troupe cinematografica sta per essere riprese in una certa parte di un ufficio. Il datore di lavoro chiede a tutti i dipendenti che siedono in quella zona per il loro consenso a essere filmati, come possono apparire sullo sfondo del video. Coloro che non vogliono farsi riprendere non siano penalizzati in alcun modo, ma invece sono date scrivanie equivalenti altrove nell'edificio per tutta la durata delle riprese.

Gli squilibri di potere non si limitano alle autorità pubbliche ei datori di lavoro, che possono verificarsi anche in altre situazioni. Come evidenziato dal WP29 in diversi pareri, il consenso può essere valido solo se il soggetto è in grado di esercitare una vera e propria scelta, e non v'è alcun rischio di inganno, l'intimidazione, coercizione o significative conseguenze negative (ad esempio notevoli costi aggiuntivi) se lui / lei non consenso. Il consenso non sarà libero nei casi in cui non v'è alcun elemento di costrizione, pressione o l'incapacità di esercitare il libero arbitrio.

3.1.2. Condizionalità

---

[16] Ai fini di questo esempio, una scuola pubblica significa una scuola finanziata con fondi pubblici o di qualsiasi struttura educativa che si qualifica come un ente pubblico o un organismo dalla legislazione nazionale.

[17] Vedi anche l'articolo 88 GDPR, in cui si sottolinea la necessità di tutela degli interessi specifici dei dipendenti e una possibilità di deroga in materia di diritto Stato membro siano creati. Vedere anche considerando 155.

[18] Vedere Parere 15/2011 sulla definizione del consenso (WP 187), pp. 12-14, Parere 8/2001 sul trattamento dei dati personali nel contesto lavorativo (WP 48), capitolo 10, documento di lavoro sulla sorveglianza delle elettronica comunicazioni nei luoghi di lavoro (WP 55), paragrafo 4.2 e Parere 2/2017 sul trattamento dei dati sul posto di lavoro (WP 249), paragrafo 6.2.

[19] Vedere Parere 2/2017 sul trattamento dei dati sul posto di lavoro, pagina 6-7

[20] Vedi anche il parere 2/2017 sul trattamento dei dati sul posto di lavoro (WP249), paragrafo 6.2.

Per valutare se il consenso è liberamente dato, l'articolo 7 (4) GDPR gioca un ruolo importante. [21]

Articolo 7 (4) GDPR indica che, tra l'altro, la situazione del consenso “bundling” con l'accettazione dei termini o condizioni, o “legare” la fornitura di un contratto o di un servizio ad una richiesta di consenso al trattamento dei dati personali che non sono necessario per l'esecuzione del contratto o di un servizio, è considerato altamente indesiderabili. Se il consenso viene dato in questa situazione, si presume non essere liberamente proposta (punto 43). Articolo 7 (4) mira a garantire che la finalità del trattamento dei dati personali non è mascherato né in bundle con la fornitura di un contratto di un servizio per il quale tali dati personali non sono necessari. In tal modo, il GDPR garantisce che il trattamento dei dati personali di cui si chiede il consenso non può diventare direttamente o indirettamente, il contro-esecuzione di un contratto. Le due basi legali per il trattamento legittimo dei dati personali, ossia

Coazione a d'accordo con l'uso di dati personali aggiuntivi a quanto è strettamente scelte limiti dati necessari del soggetto e si trova nel modo di libero consenso. Poiché il diritto alla protezione dei dati mira alla tutela dei diritti fondamentali, il controllo di un individuo sui propri dati personali è essenziale e v'è una forte presunzione che il consenso al trattamento dei dati personali che non è necessaria, non può essere visto come una considerazione obbligatoria in cambio di l'esecuzione di un contratto o la prestazione di un servizio.

Quindi, ogni volta che una richiesta di consenso è legato alla performance di un contratto da parte del controllore, l'interessato che non vuole fare il suo / suoi dati personali disponibili per l'elaborazione dal controller corre il rischio di essere negato servizi che hanno richiesto.

Per valutare se si verifica una tale situazione di vendite abbinate o di legatura, è importante per determinare ciò che il campo di applicazione del contratto è e quali sono i dati sarebbe necessario per l'esecuzione di tale contratto. Secondo Parere 06/2014 del WP29, il termine “necessario per l'esecuzione di un contratto” deve essere interpretata restrittivamente. Il trattamento deve essere necessario per adempiere al contratto con ogni singolo interessato. Questo può includere, ad esempio, l'elaborazione di l'indirizzo della persona in modo che le merci acquistati online possono essere consegnati, o estremi della carta di credito di trasformazione al fine di facilitare il pagamento. Nel contesto lavorativo, questo terreno può consentire, ad esempio, il trattamento delle informazioni e le coordinate bancarie di stipendio dettagli in modo che i salari possono essere pagati. [22] Ci deve essere un collegamento diretto e oggettivo tra l'elaborazione dei dati e la finalità della esecuzione del contratto.

Se un controller cerca di elaborare i dati personali che sono di fatto necessari per l'esecuzione di un contratto, allora il consenso non è la base legale appropriata. [23]

---

[21] Articolo 7 (4) GDPR: “ *Nel valutare se il consenso viene dato liberamente, massima si tiene conto del fatto che, tra l'altro, l'esecuzione di un contratto, compresa la fornitura di un servizio, è subordinato al consenso al trattamento dei dati personali che non è necessario per l'esecuzione di tale contratto.* ”Vedere anche considerando 43 GDPR, che afferma:“[*...] Il consenso si presume che non essere liberamente determinato se non permette consenso separato da dare alle diverse operazioni di trattamento dei dati personali nonostante fosse opportuna nel caso specifico, o se l'esecuzione di un contratto, compresa la fornitura di un servizio, dipende dal consenso, nonostante tale consenso non sia necessario che tali prestazioni.* ”

[22] Per ulteriori informazioni ed esempi, vedere Parere 06/2014 sulla nozione di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46 / CE, adottata dal WP29 il 9 aprile 2014, pag. 16-17. (WP 217).

[23] La base legale appropriata potrebbe quindi essere l'articolo 6, (1) (b) (contratto).

Articolo 7 (4) è rilevante solo quando i dati richiesti sono **non** necessari per l'esecuzione del contratto, (compresa la fornitura di un servizio), e l'esecuzione di tale contratto è subordinata all'ottenimento di tali dati sulla base del consenso. Viceversa, se la trasformazione **è**
necessaria per eseguire il contratto (compreso quello di fornire un servizio), quindi l'articolo 7 non si applica (4).

> [Esempio 6]
> Una banca chiede ai clienti il consenso per permettere a terzi di utilizzare i loro dati di pagamento per scopi di marketing diretto. Questa attività di trasformazione non è necessario per l'esecuzione del contratto con il cliente e la fornitura di servizi ordinari di conto bancario. Se il rifiuto del cliente di consentire a questo scopo l'elaborazione porterebbe alla negazione dei servizi bancari, la chiusura del conto bancario, o, a seconda dei casi, un aumento della tassa, il consenso non può essere dato liberamente.

La scelta del legislatore per evidenziare condizioni, tra l'altro, una presunzione di mancanza di libertà di consenso, dimostra che il verificarsi di condizioni deve essere attentamente esaminato. Il termine “massimo conto” di cui all'articolo 7 (4) suggerisce che la particolare cautela è necessaria dal controllore quando un contratto (che potrebbe includere la fornitura di un servizio) ha una richiesta di consenso al trattamento dei dati personali legate ad esso.

Come la formulazione dell'articolo 7 (4) non è interpretata in modo assoluto, ci potrebbe essere spazio molto limitato ai casi in cui tale condizione non renderebbe il consenso valido. Tuttavia, la parola “presunto” nel considerando 43 indica chiaramente che tali casi saranno altamente eccezionale.

In ogni caso, l'onere della prova di cui all'articolo 7 (4) è sul controller. [24] Questa regola specifica riflette il principio generale di responsabilità che corre per tutta la GDPR. Tuttavia, quando l'articolo 7 (4) si applica, sarà più difficile per il controller per dimostrare che il consenso è stato dato liberamente dalla persona. [25]

Il controller potrebbe sostenere che la sua organizzazione offre interessati genuina scelta se fossero in grado di scegliere tra un servizio che include consenso al trattamento dei dati personali per finalità ulteriori, da un lato, e un servizio equivalente offerto dallo stesso controllore che non lo fa coinvolgere consentendo ad uso dati per ulteriori scopi dall'altro. Finché v'è la possibilità di esecuzione al contratto o il servizio contratto consegnato da questo controller, senza acconsentire al utilizzo diverso o che i dati in questione, questo significa che non c'è più un servizio condizionale. Tuttavia, entrambi i servizi devono essere equivalenti veramente.

Il WP29 ritiene che il consenso non può essere considerato come dato liberamente se un controller sostiene che esiste una scelta tra il servizio che include consenso all'utilizzo dei dati personali per altre finalità, da un lato, e un servizio equivalente offerto da un controller diverso sulla altro

---

[24] Si veda anche l'articolo 7 (1) GDPR, in cui si afferma che il controllore ha bisogno di dimostrare che l'accordo della persona interessata è stato dato liberamente.

[25] In una certa misura, l'introduzione di questo paragrafo è la codificazione della WP29 guida esistenti. Come descritto nel parere 15/2011, quando l'interessato è in una situazione di dipendenza dal titolare - a causa della natura del rapporto o di circostanze particolari - ci può essere una presunzione forte che libera consenso è limitata a tali contesti (ad esempio in un rapporto di lavoro o se la raccolta dei dati viene eseguita da un ente pubblico). Dell'articolo 7 (4) in vigore, sarà più difficile per il controller per dimostrare che il consenso è stato dato liberamente dalla persona. Vedere: Parere 15/2011 sulla definizione del consenso (WP 187), pp 12-17..

mano. In tal caso, la libertà di scelta sarebbe fatta dipende da ciò che gli altri operatori di mercato fanno e se un dato individuo soggetto avrebbe trovato i servizi di l'altro controller veramente equivalente. Sarebbe, inoltre, implica l'obbligo per i controllori di monitorare gli sviluppi del mercato per garantire la costante validità del consenso per le loro attività di trattamento dei dati, come un concorrente può alterare il suo servizio in una fase successiva. Quindi, utilizzando questo argomento significa questo consenso non rispetta la GDPR.

3.1.3. granularità

Un servizio può coinvolgere molteplici lavorazioni per più di uno scopo. In questi casi, le persone interessate devono essere liberi di scegliere quale scopo essi accettano, piuttosto che dover acconsentire a un fascio di finalità di trattamento. In un determinato caso, parecchi consensi può essere giustificata per iniziare ad offrire un servizio, ai sensi della GDPR.

Considerando 43 chiarisce che il consenso si presume che non essere liberamente determinato se il processo / procedura per ottenere il consenso non permette interessati a dare il consenso separato per le operazioni di trattamento dei dati personali rispettivamente (ad esempio solo per alcune operazioni di trattamento e non per altri) nonostante fosse appropriato nel singolo caso. Considerando 32 Stati " *Consenso dovrebbe coprire tutte le attività di trattamento svolte per lo stesso scopo o scopi. Quando l'elaborazione ha molteplici scopi, il consenso deve essere dato per tutti loro* ".

Se il controllore ha conflated diversi scopi per l'elaborazione e non ha cercato di ottenere il consenso separato per ogni scopo, v'è una mancanza di libertà. Questa granularità è strettamente legata alla necessità di consenso essere specifici, come discusso nella sezione 3.2 più avanti. Quando l'elaborazione dei dati avviene nel perseguimento di diversi scopi, la soluzione di rispettare le condizioni per il consenso valido risiede nella granularità, cioè la separazione di questi scopi ottenendone per ogni scopo.

> [Esempio 7]
> All'interno della stessa richiesta di consenso un rivenditore chiede ai suoi clienti per il consenso al trattamento dei dati per inviare loro commercializzazione per e-mail e anche di condividere i propri dati con altre società all'interno del loro gruppo. Questo consenso non è granulare in quanto non v'è alcuna autorizzazioni separate per questi due scopi distinti, quindi il consenso non sarà valido. In questo caso, uno specifico consenso deve essere raccolto per inviare i dati di contatto per i partner commerciali. Tale consenso specifico sarà considerata valida per ogni partner (vedi anche la sezione 3.3.1), la cui identità è stata fornita alla persona interessata al momento della raccolta del suo consenso, nella misura in cui viene inviato a loro per lo stesso scopo (in questo esempio: un obiettivo di marketing).

3.1.4. detrimento

Il regolatore deve dimostrare che è possibile rifiutare o ritirare il consenso senza pregiudizio (punto 42). Ad esempio, il controllore deve dimostrare di ritirare il consenso non comporti costi per la persona e quindi chiara svantaggio per coloro ritirare il consenso.

Altri esempi di pregiudizio sono inganno, l'intimidazione, coercizione o significative conseguenze negative se un soggetto di dati non acconsente. Il regolatore deve essere in grado di dimostrare che l'interessato aveva una scelta libera o vero e proprio sul fatto di consentire e che era possibile di revocare il consenso senza danno.

Se un controller è in grado di dimostrare che un servizio prevede la possibilità di ritirare il consenso senza conseguenze negative per esempio, senza la prestazione del servizio declassamento a danno dell'utente, puo 'servire per dimostrare che il consenso è stato dato liberamente. Il GDPR non esclude tutti gli incentivi ma l'onere sarebbe sul controller di dimostrare che il consenso era ancora dato liberamente in tutte le circostanze.

[Esempio 8]
Quando si scarica un'applicazione mobile stile di vita, l'applicazione chiede il consenso per accedere accelerometro del telefono. Questo non è necessario per l'applicazione al lavoro, ma è utile per il controller che vuole saperne di più sui movimenti e livelli di attività dei suoi utenti. Quando l'utente in seguito revoca che il consenso, scopre che l'applicazione ora funziona solo in misura limitata. Questo è un esempio di danno come inteso nel considerando 42, il che significa che il consenso non è mai stato validamente ottenuta (e quindi, il controllore deve eliminare tutti i dati personali relativi movimenti degli utenti così raccolti).

[Esempio 9]
L'interessato sottoscrive lettera d'informazione di un rivenditore di moda con sconti generali. Il rivenditore chiede al soggetto di dati di consenso per raccogliere più dati sulle preferenze commerciali di adattare le offerte per le sue preferenze in base alla cronologia di shopping o un questionario che è volontaria da compilare. Quando la persona interessata in seguito revoca il consenso, lui o lei riceverà di nuovo sconti moda non personalizzati. Ciò non equivale a discapito come solo l'incentivo consentito è stato perso.

[Esempio: 10]
Una rivista di moda offre ai lettori l'accesso a comprare nuovi prodotti make-up prima del lancio ufficiale. I prodotti saranno presto resi disponibili per la vendita, ma i lettori di questa rivista sono offerti un'anteprima esclusiva di questi prodotti. Per poter godere di questo beneficio, le persone devono dare il loro indirizzo postale e accettare di sottoscrizione sulla mailing list della rivista. L'indirizzo postale è necessario per il trasporto e la mailing list viene utilizzata per inviare offerte commerciali per prodotti come cosmetici o t-shirt per tutto l'anno. La società spiega che i dati sulla mailing list saranno utilizzati esclusivamente per l'invio di merce e la pubblicità della carta dalla rivista stessa e non deve essere condiviso con qualsiasi altra organizzazione. Nel caso in cui il lettore non vuole rivelare il proprio indirizzo per questo motivo, non v'è alcun pregiudizio,

3.2. Specifica

Articolo 6 (1) (a) conferma che il consenso della persona interessata deve essere somministrato in relazione a “uno o più specifici” scopi e che un soggetto di dati ha una scelta in relazione a ciascuno di essi. [26] Il requisito che il consenso deve essere ' *specifica'* intende garantire un certo grado di controllo utente e trasparenza per la persona. Questo requisito non è stato modificato dal GDPR e rimane strettamente legato al requisito del consenso 'informato'. Allo stesso tempo deve essere interpretato in linea con l'esigenza di 'granularità' per ottenere il consenso 'libera'. [27] In sintesi, per conformarsi con l'elemento 'specifico' il controllore deve applicarsi:

(io) specifiche finalità come salvaguardia contro la funzione di scorrimento, (ii) La granularità nelle richieste di consenso, e (iii) Netta separazione delle informazioni relative a ottenere il consenso per le attività di trattamento dei dati da informazioni su altre questioni.

[26] Ulteriori orientamenti sulla determinazione di 'scopi' può essere trovato nel parere 3/2013 sulla limitazione dello scopo (WP 203).

[27] Considerando 43 GDPR afferma che sarà necessario consenso separato per le diverse lavorazioni ove opportuno. Opzioni di consenso granulari devono essere forniti per consentire agli interessati di consenso separatamente a scopi diversi.

Anno Domini. (io): Ai sensi dell'articolo 5 (1) (b) GDPR, ottenendo un valido consenso è sempre preceduta dalla determinazione di uno scopo specifico, espliciti e legittimi per l'attività di trasformazione previsto. [28]

La necessità di consenso specifico in combinazione con la nozione di limitazione dello scopo all'articolo 5 (1) (b) funziona come una salvaguardia contro l'allargamento graduale o sfocatura scopi per cui i dati sono trattati, dopo l'interessato ha accettato di raccolta iniziale dei dati. Questo fenomeno, noto anche come funzione creep, è un rischio per gli interessati, in quanto può provocare uso imprevista dei dati personali dal controllore o da terzi e la perdita di controllo dati soggetto.

Se il controller si basa sull'articolo 6 (1) (a), gli interessati devono sempre dare il consenso per uno scopo specifico trattamento. [29] In linea con il concetto di *limitazione delle finalità,* Articolo 5 (1) (b) e punto 32, il consenso può coprire diverse operazioni, purché queste operazioni hanno lo stesso scopo. Va da sé che il consenso specifico può essere ottenuto solo se le persone interessate sono specificamente informati sulle finalità d'uso previste dati che li riguardano.

Nonostante le disposizioni sulla compatibilità di scopi, consenso deve essere specifico per lo scopo. Le persone interessate potranno dare il proprio consenso con la consapevolezza che sono in controllo ei loro dati saranno trattati solo per le finalità indicate. Se i dati a processi di controllo basata sul consenso e desidera elaborare i dati per un altro scopo, anche, che di controllo ha bisogno di cercare ulteriore consenso per questo altro scopo a meno che non v'è un altro base legale che riflette meglio la situazione.

> [Esempio 11] Una rete televisiva via cavo raccoglie i dati personali degli abbonati, in base alla loro consenso, per presentare loro con suggerimenti personali per nuovi film che potrebbero essere interessati a in base alle loro abitudini di visione. Dopo un po ', la rete televisiva decide che vorrebbe consentire a terzi di inviare (o visualizzare) pubblicità mirata sulla base delle abitudini di visione del sottoscrittore. Dato questo nuovo scopo, è necessario un nuovo consenso.

Anno Domini. (Ii): meccanismi di consenso non solo deve essere granulare per soddisfare il requisito di 'libera', ma anche per soddisfare l'elemento di 'specifico'. Ciò significa, un controller che cerca il consenso per vari scopi diversi dovrebbero fornire un separato opt-in per ogni scopo, per consentire agli utenti di dare specifico consenso per scopi specifici.

Anno Domini. (Iii): Infine, i controllori devono fornire informazioni specifiche a ogni richiesta di consenso separato sui dati che vengono elaborati per ogni scopo, al fine di rendere le persone interessate consapevoli dell'impatto delle diverse scelte che hanno. Così, gli interessati sono abilitati a dare specifico consenso. Questo problema si sovrappone con il requisito che i titolari devono fornire informazioni chiare, come discusso nel paragrafo 3.3. sotto.

3.3. Informato

Il GDPR rafforza l'esigenza che il consenso deve essere informato. Sulla base dell'articolo 5 del GDPR, l'esigenza di trasparenza è uno dei principi fondamentali, strettamente legata alla

---

[28] Vedi WP 29 Parere 3/2013 sulla limitazione dello scopo (WP 203), p. 16,: " *Per queste ragioni, uno scopo che è vago o generale, come ad esempio 'migliorare utenti' esperienza', 'scopi di marketing', 'scopi,-security' o 'ricerca futura' sarà - senza ulteriori dettagli - di solito non soddisfare i criteri di essere 'specifica'.* "

[29] Ciò è coerente con WP29 parere 15/2011 sulla definizione di consenso (WP 187), ad esempio, a pag. 17.

principi di correttezza e liceità. Fornire informazioni alle persone interessate prima di ottenere il loro consenso è essenziale al fine di consentire loro di prendere decisioni informate, capiscono quello che sono d'accordo a, e, per esempio esercitare il diritto di ritirare il loro consenso. Se il controller non fornisce informazioni accessibili, il controllo utente diventa illusorio e il consenso sarà una base valida per l'elaborazione.

La conseguenza di non rispettare i requisiti per il consenso informato è che il consenso non sarà valida e il controller può essere in violazione dell'articolo 6 della GDPR.

3.3.1. Requisiti minimi di contenuto per il consenso ad essere 'informati'

Per il consenso ad essere informati, è necessario informare l'interessato di alcuni elementi che sono fondamentali per fare una scelta. Pertanto, WP29 è del parere che almeno sono necessarie le seguenti informazioni per l'ottenimento di un valido consenso:

(io) l'identità del controller, [30]
(Ii) lo scopo di ciascuno dei trattamenti di cui si chiede il consenso, [31]
(Iii) quale (tipo di) dati saranno raccolti e utilizzati, [32]
(Iv) l'esistenza del diritto di recesso consenso, [33]
(V) informazioni circa l'utilizzo dei dati per il processo decisionale automatizzato ai sensi dell'articolo 22 (2) (c) [34] se del caso, e (vi)
sui possibili rischi di trasferimenti di dati a causa di mancanza di una decisione di adeguatezza e di garanzie appropriate come descritto nell'articolo 46. [35]

Per quanto riguarda il punto (i) e (iii), WP29 osserva che nel caso in cui il consenso ricercato è quello di essere invocato da più controllori (comuni) o se i dati devono essere trasferiti o elaborati da altri controllori che desiderano si basano sul consenso originale, queste organizzazioni dovrebbero essere chiamati. I processori non hanno bisogno di essere nominato come parte dei requisiti di consenso, anche se per conformarsi agli articoli 13 e 14 del GDPR, i controllori dovranno fornire un elenco completo dei soggetti o delle categorie di destinatari, tra cui processori. Per concludere, WP29 rileva che a seconda delle circostanze e nell'ambito di un caso, ulteriori informazioni possono essere necessarie per consentire alla persona di comprendere realmente le operazioni di trattamento a portata di mano.

3.3.2. Come fornire informazioni

Il GDPR non prescrive la forma o la forma in cui le informazioni devono essere fornite al fine di soddisfare il requisito del consenso informato. Ciò significa che le informazioni valide può essere presentato in vari modi, ad esempio dichiarazioni scritte o orali, o messaggi audio o video. Tuttavia, il GDPR

---

30 Si veda anche il considerando 42 GDPR: "[*...] Per il consenso di essere informati, la persona interessata deve essere consapevole di almeno l'identità del responsabile del trattamento e le finalità del trattamento cui i dati personali sono destinati. [...]."*

31 Ancora una volta, vedasi considerando 42 GDPR

32 Vedi anche WP29 parere 15/2011 sulla definizione del consenso (WP 187) pp.19-20

33 Si veda l'articolo 7 (3) GDPR

34 Vedi anche WP29 Orientamenti in materia di Automated individuale decisionale e Profiling ai fini del regolamento 2016/679 (WP251), paragrafo IV.B, pag. 20 in avanti.

35 Ai sensi dell'articolo 49 (1) (a), informazioni specifiche è necessario per l'assenza di misure di salvaguardia di cui all'articolo 46, in cui è richiesta consenso esplicito. Vedi anche WP29 parere 15/2011 sulla definizione del consenso (WP 187) p. 19

mette diversi requisiti per il consenso informato in atto, prevalentemente all'articolo 7 (2) e considerando 32. Questo porta a uno standard più elevato per la chiarezza e l'accessibilità delle informazioni.

Quando si cerca il consenso, i controller dovrebbero assicurare che usano un linguaggio chiaro e semplice in tutti i casi. Ciò significa che un messaggio deve essere facilmente comprensibile per la persona media e non solo per gli avvocati. Controllori non possono utilizzare le politiche sulla privacy lunghi che sono difficili da capire o dichiarazioni piene di gergo legale. Consenso deve essere chiaro e distinguibile da altri aspetti e disponibile in forma comprensibile e facilmente accessibile. Questo requisito significa essenzialmente che le informazioni rilevanti per prendere decisioni informate sulla necessità o meno di consentire non può essere nascosta in termini e condizioni generali. [36]

Un controllore deve garantire che il consenso è fornito sulla base di informazioni che permette agli interessati di individuare facilmente chi è il controllore e per capire che cosa sono d'accordo a. Il regolatore deve descrivere chiaramente lo scopo del trattamento per il quale è richiesto il consenso. [37]

Altre indicazioni specifiche sull'accessibilità sono state fornite nelle linee guida in materia di trasparenza WP29. Se il consenso deve essere dato per via elettronica, la richiesta deve essere chiara e concisa. informazioni strati e granulare può essere un modo appropriato per affrontare l'obbligo duplice di essere preciso e completo, da un lato e comprensibile dall'altro.

Un controller deve valutare che tipo di pubblico è che fornisce i dati personali per la loro organizzazione. Ad esempio, nel caso in cui il pubblico mirato include interessati che sono minorenni, il controller è prevista per assicurarsi che le informazioni è comprensibile per i minori. [38] Dopo aver identificato il loro pubblico, i controllori devono determinare quali informazioni devono fornire e, successivamente, come si presenteranno le informazioni alle persone interessate.

L'articolo 7 (2) affronta pre-formulate dichiarazioni scritte del consenso che riguardano anche altre questioni. Quando il consenso è richiesto come parte di un (carta) del contratto, la richiesta di consenso deve essere chiaramente distinguibile dalle altre questioni. Se il contratto di carta comprende molti aspetti che non sono collegati alla questione del consenso al trattamento dei dati personali, la questione del consenso dovrebbe essere trattata in un modo che si distingue nettamente, o in un documento separato. Analogamente, se il consenso è richiesto per via elettronica, la richiesta di consenso deve essere separata e distinta, non può essere semplicemente un paragrafo all'interno termini e condizioni, ai sensi Considerando 32. [39] Per ospitare per piccoli schermi o situazioni con spazio limitato per informazioni, un modo stratificata di presentazione di informazioni può essere considerata, se del caso, per evitare un'eccessiva perturbazione esperienza dell'utente o progettazione.

[36] La dichiarazione di consenso deve essere chiamato come tale. Redazione, come ad esempio "io so che ..." non soddisfa il requisito di un linguaggio chiaro.

[37] Si vedano gli articoli 4 (11) e 7 (2) GDPR.

[38] Vedi anche il considerando 58 per quanto riguarda informazioni comprensibili per i bambini.

[39] Vedi anche il considerando 42 e la direttiva 93/13 / CE, in particolare l'articolo 5 (un linguaggio semplice e comprensibile e in caso di dubbio, l'interpretazione sarà a favore dei consumatori) e l'articolo 6 (invalidità delle clausole abusive, contratto continua ad esistere senza questi termini solo se ancora sensibile, altrimenti l'intero contratto è valido).

Un controller che si basa sul consenso della persona interessata deve anche trattare con i doveri di informazione separati di cui agli articoli 13 e 14, al fine di essere conformi alla GDPR. In pratica, rispetto degli obblighi di informazione e il rispetto del requisito del consenso informato può portare ad un approccio integrato in molti casi. Tuttavia, questa sezione è scritto nella comprensione che un valido consenso "informato" può esistere, anche se non tutti gli elementi di cui agli articoli 13 e / o 14 sono menzionati nel processo di ottenimento del consenso (questi punti devono ovviamente essere menzionati in altri luoghi, come ad esempio l'informativa sulla privacy di una società). WP29 ha emanato linee guida separati sul requisito di trasparenza.

[Esempio 12]
La società X è un controller che ha ricevuto denunce che non è chiaro agli interessati per quali scopi di dati utilizzano gli viene chiesto di acconsentire. L'azienda vede la necessità di verificare se le sue informazioni nella richiesta di consenso è comprensibile per gli interessati. X organizza pannelli di prova volontarie di categorie specifiche dei propri clienti e presenta nuove versioni delle sue informazioni il consenso a questo pubblico di prova prima di comunicarla all'esterno. La selezione del pannello rispetta il principio di indipendenza e viene effettuata sulla base di standard che garantiscano un rappresentante, esito non-polarizzata. Il pannello riceve un questionario e indica quali hanno capito delle informazioni e come avrebbero segnare in termini di informazioni comprensibili e pertinenti. Il controllore continua prova fino a quando i pannelli indicano che l'informazione è comprensibile. X redige un rapporto del test e mantiene questo disponibile per riferimento futuro. Questo esempio mostra un possibile modo per X per dimostrare che gli interessati stavano ricevendo informazioni chiare prima di consentire l'elaborazione dei dati personali da X.

[Esempio 13]
Una società si impegna nel trattamento dei dati sulla base del consenso. L'azienda utilizza un avviso di privacy più livelli che include una richiesta di consenso. L'azienda rivela tutti i dettagli di base del controller e le attività di trattamento dei dati previsti.[40] Tuttavia, la società non indica come il loro responsabile della protezione dei dati può essere contattato nel primo strato informazioni del bando. Ai fini di avere una base legale valida a titolo dell'articolo 6, questo controller ottenuto un valido consenso "informato", anche quando i dati di contatto del responsabile della protezione dei dati non sono stati comunicati alla persona interessata (nel primo strato informazioni), ai sensi dell'articolo 13 (1) (b) o 14 (1) (b) GDPR.

3.4. l'indicazione inequivocabile dei desideri

Il GDPR è chiaro che il consenso richiede una dichiarazione della persona interessata o un chiaro atto affermativa che significa che deve sempre essere somministrato attraverso un movimento attivo o una dichiarazione. Deve essere chiaro che la persona ha acconsentito alla particolare lavorazione.

Articolo 2 (h), della direttiva 95/46 / CE, ha descritto il consenso come un "indicazione di desideri con la quale la persona significa accettare di dati personali che lo riguardano in fase di elaborazione". L'articolo 4 (11) GDPR si basa su questa definizione, chiarendo che un valido consenso richiede un *non ambiguo* indicazione mediante *dichiarazione o da una chiara azione affermativa,* in linea con la guidance precedente rilasciata dal WP29.

[40] Si noti che quando l'identità del controllore o lo scopo del trattamento non è evidente dal primo strato informazione sulla privacy stratificato (e si trovano in ulteriori sotto-strati), sarà difficile per il titolare del trattamento per dimostrare che il persona interessata abbia dato consenso informato, a meno che il titolare del trattamento in grado di dimostrare che la persona in questione accede tali informazioni prima di dare il consenso.

Un “atto affermativa chiaro” significa che la persona deve aver preso dell'azione volontaria per consentire alla particolare lavorazione. [41] Considerando 32 stabilisce ulteriori indicazioni in merito. Il consenso può essere raccolto attraverso una o (una registrazione) dichiarazione orale scritta, anche per via elettronica.

Forse il modo più letterale a rispettare il criterio di una “dichiarazione scritta” è quello di assicurarsi che un soggetto di dati scrive in una lettera o una e-mail tipo al controller spiegare cosa esattamente lui / lei accetta di. Tuttavia, questo spesso non è realistico. dichiarazioni scritte possono venire in molte forme e dimensioni che potrebbe essere compatibile con il GDPR.

Fatte salve le disposizioni esistenti legge (nazionale) del contratto, il consenso può essere ottenuto attraverso una dichiarazione orale registrata, anche se a causa nota deve essere presa in considerazione delle informazioni disponibili alla persona, prima che l'indicazione del consenso. L'uso di riquadri già contrassegnati opt-in non è valido sotto il GDPR. Silenzio o l'inazione da parte della persona, così come semplicemente di procedere con un servizio non possono essere considerate come un'indicazione attiva di scelta.

> [Esempio 14]
> Quando si installa il software, l'applicazione chiede al soggetto di dati per il consenso a utilizzare segnalazioni di crash non anonimi per migliorare il software. Un avviso privacy strati fornire le informazioni necessarie accompagna la richiesta di consenso. Spuntando attivamente il box opzionale affermando, “acconsento”, l'utente è in grado di eseguire validamente un act' affermativa'clear per il consenso al trattamento.

Un controllore deve anche attenzione che il consenso non può essere ottenuto attraverso lo stesso movimento come accettando un contratto o accettare termini e condizioni di servizio generali. Blanket accettazione delle condizioni generali non può essere visto come una chiara azione affermativa di consentire l'utilizzo dei dati personali. Il GDPR non permette ai controllori di offrire riquadri già contrassegnati o costruzioni che richiedono un intervento da parte della persona interessata per evitare che un accordo (ad esempio 'scatole di opt-out') opt-out. [42]

Quando consenso deve essere dato seguito di una richiesta per via elettronica, la richiesta di consenso non dovrebbe essere *inutilmente* dannoso per l'utilizzo del servizio per il quale è fornito il consenso. [43] Un movimento affermativo attivo con cui i dati soggetto indica consenso può essere necessario quando un modus meno violazione o sgradevole comporterebbe ambiguità. Pertanto, può essere necessario che una richiesta consenso interrompe l'esperienza d'uso in una certa misura a rendere tale domanda efficace.

---

[41] Vedi Documento di lavoro della Commissione, la valutazione d'impatto, allegato 2, pag. 20 e anche pp 105-106:. “ *Come anche sottolineato nel parere adottato dal WP29 sul consenso, sembra essenziale chiarire che il consenso valido richiede l'utilizzo di meccanismi che non lasciano dubbi dell'intenzione della persona interessata al consenso, rendendo chiaro che - nel contesto del on- ambiente linea - l'utilizzo di opzioni prestabilite che la persona interessata di modificare al fine di rifiutare l'elaborazione ('consenso basata sul silenzio') non costituisce di per sé consenso inequivocabile. Questo darebbe individui un maggiore controllo sui propri dati, ogni volta che l'elaborazione si basa sulla sua / il suo consenso. Per quanto riguarda l'impatto sui responsabili del trattamento, questo non avrebbe un impatto importante come esso unicamente chiarisce e incantesimi meglio le implicazioni della direttiva vigente in relazione alle condizioni per un consenso valido e significativo dalla persona interessata. In particolare,* ”

[42] Si veda l'articolo 7 (2). Vedi anche il documento di lavoro 02/2013 su come ottenere il consenso per i cookie (WP 208), pp. 3-6.

[43] Vedere Considerando 32 GDPR.

Tuttavia, entro i requisiti della GDPR, i controllori hanno la libertà di sviluppare un flusso di consenso che si adatta alle loro organizzazione. A questo proposito, movimenti fisici possono essere qualificati come un chiaro azione affermativa in conformità alla GDPR.

Controller dovrebbero progettare meccanismi di consenso in modi che sono chiare agli interessati. Controllori devono evitare ambiguità e devono garantire che il ricorso con cui viene dato consenso può essere distinta da altre azioni. Pertanto, solo continuando l'uso normale di un sito web non è una condotta da cui si può dedurre l'indicazione della volontà della persona interessata per significare il suo consenso a un trattamento previsto.

[Esempio 15]

Swiping un bar su uno schermo, rinuncia di fronte a una telecamera intelligente, trasformando uno smartphone in giro in senso orario, o in una figura otto movimento può essere opzioni per indicare accordo, le informazioni finché chiaro è fornito, ed è chiaro che il movimento domanda significa accettazione di una richiesta specifica (ad esempio, se swipe questa barra a sinistra, l'utente accetta di l'utilizzo delle informazioni X a scopo Y. Ripetere il movimento per confermare). Il regolatore deve essere in grado di dimostrare che il consenso è stato ottenuto in questo modo e interessati devono essere in grado di ritirare il consenso facilmente come è stato dato.

[Esempio 16]

Scorrendo verso il basso o strisciata attraverso un sito web non in grado di soddisfare l'esigenza di un'azione chiara e positiva. Questo perché l'avviso che continua a scorrere costituirà consenso può essere difficile distinguere e / o può essere persa quando un soggetto di dati è rapidamente scorre attraverso grandi quantità di testo e di una tale azione non è sufficientemente univoca.

Nel contesto digitale, molti servizi hanno bisogno di dati personali alla funzione, di conseguenza, le persone interessate ricevono più richieste di consenso che hanno bisogno di risposte attraverso scatti e colpi ogni giorno. Ciò può causare un certo grado di stanchezza click: quando incontrato troppe volte, l'effetto di allarme reale di meccanismi di consenso sta diminuendo.

Ciò si traduce in una situazione in cui le domande di consenso non sono più letti. Questo è un rischio particolare per gli interessati, come, in genere, il consenso è richiesto per le azioni che sono in linea di principio illegali senza il loro consenso. I posti GDPR su controller l'obbligo di sviluppare modi per affrontare questo problema.

Un esempio spesso citato per fare questo nel contesto on-line è quello di ottenere il consenso degli utenti di Internet tramite le impostazioni del browser. Tali impostazioni devono essere sviluppati in linea con le condizioni di consenso valido nel GDPR, come per esempio che il consenso è granulare per ciascuna delle finalità previste e che le informazioni da fornire, dovrebbe nominare i controllori.

In ogni caso, il consenso deve sempre essere ottenuta prima che il controllore avvia l'elaborazione dei dati personali per cui è necessario consenso. WP29 ha costantemente affermato in precedenti opinioni che il consenso dovrebbe essere dato prima dell'attività elaborazione. [44] Sebbene il GDPR non letteralmente prescrive all'articolo 4 (11) che il consenso deve essere dato prima dell'attività lavorazione, questo è chiaramente implicita. Il titolo dell'articolo 6 (1) e la dicitura “ha dato” di cui all'articolo 6 (1) (a), supporta questa interpretazione. Ne consegue logicamente l'articolo 6 e il considerando 40 che una base legale valida deve essere presente prima

[44] WP29 ha costantemente sostenuto questa posizione dal parere 15/2011 sulla definizione del consenso (WP 187), pp. 30-31.

iniziare un'elaborazione dei dati. Pertanto, il consenso deve essere somministrato prima dell'attività elaborazione. In linea di principio, può essere sufficiente per chiedere il consenso del soggetto dati una volta. Tuttavia, i controllori hanno bisogno di ottenere un nuovo e specifico consenso se scopi di cambiamento trattamento dei dati dopo il consenso è stato ottenuto o se è prevista uno scopo ulteriore.

4. Ottenere il consenso esplicito

consenso esplicito è richiesto in alcune situazioni in cui rischio serio protezione dati emergono, quindi, in cui un elevato livello di controllo individuale sui dati personali si ritenga opportuno. Sotto la GDPR, esplicito consenso svolge un ruolo di cui all'articolo 9 sul trattamento di categorie particolari di dati, le disposizioni in materia di trasferimenti di dati verso paesi terzi o organizzazioni internazionali, in assenza di adeguate garanzie di cui all'articolo 49 [45], e all'articolo 22 sulla automatizzato individuale processo decisionale, tra cui profiling. [46]

Il GDPR prescrive che una “dichiarazione o chiara azione affermativa” è un prerequisito per il consenso 'regolare'. Come il requisito del consenso 'regolare' nella GDPR è già elevato a un livello superiore rispetto al requisito del consenso nella direttiva 95/46 / CE, deve essere chiarito che cosa sforzi supplementari un controller dovrebbe impegnarsi al fine di ottenere il *esplicito* consenso della persona interessata in linea con il GDPR.

Il termine *esplicito* si riferisce al modo consenso è espressa dalla persona. Ciò significa che la persona interessata deve dare una manifestazione espressa del consenso. Un modo ovvio per assicurarsi il consenso è esplicita sarebbe quello di confermare espressamente il consenso in una dichiarazione scritta. Se del caso, il controller potrebbe assicurarsi che la dichiarazione scritta è firmata dal titolare dei dati, al fine di rimuovere ogni possibile dubbio e potenziale mancanza di prove nel futuro. [47]

Tuttavia, una tale dichiarazione firmata non è l'unico modo per ottenere il consenso esplicito e, non si può dire che il GDPR prescrive dichiarazioni scritte e firmato in tutte le circostanze che richiedono un valido consenso esplicito. Per esempio, nel contesto digitale o on-line, l'interessato può essere in grado di rilasciare la dichiarazione richiesta compilando un modulo elettronico, mediante l'invio di una e-mail, caricando un documento digitalizzato che porta la firma della persona, oppure utilizzando un firma elettronica. In teoria, l'uso di dichiarazioni orali può anche essere sufficientemente esplicita per ottenere un valido consenso esplicito, tuttavia, può essere difficile da provare per il controllore che tutte le condizioni per un valido consenso esplicito sono stati raggiunti quando l'istruzione è stata registrata.

---

[45] Secondo l'articolo 49 (1) (a) GDPR, esplicito consenso può revocare il divieto di trasferimenti di dati verso paesi senza adeguati livelli di legge sulla protezione dei dati. Si noti inoltre Documento di lavoro su un'interpretazione comune dell'articolo 26 (1) della direttiva 95/46 / CE del 24 ottobre 1995 (WP 114), p. 11, dove WP29 ha indicato che il consenso per il trasferimento di dati che si verificano periodicamente o su una base in corso è appropriato.

[46] All'articolo 22, il GDPR introduce disposizioni volte a tutelare gli interessati contro le decisioni basate unicamente su un trattamento automatizzato, tra cui profiling. Le decisioni prese su questa base sono autorizzati a determinate condizioni legali. Consenso gioca un ruolo chiave in questo meccanismo di protezione, come l'articolo 22 (2) (c) GDPR chiarisce che un controllore può procedere con il processo automatizzato decisionale, inclusi profili, che possono influenzare in modo significativo l'individuo, con il consenso esplicito della persona interessata. WP29 hanno prodotto linee guida separate su questo tema: linee guida su WP29 automatizzato il processo decisionale e Profiling ai fini del regolamento 2016/679, 3 ottobre 2017 (WP 251).

[47] Vedi anche WP29 parere 15/2011, sulla definizione del consenso (WP 187), p. 25.

Un'organizzazione può anche ottenere il consenso esplicito attraverso una conversazione telefonica, a condizione che le informazioni circa la scelta è giusto, comprensibile e chiaro, e chiede una conferma specifica presso la persona interessata (ad esempio premendo un pulsante o fornire conferma orale).

> [Esempio 17] Un controllore dei dati può anche ottenere il consenso esplicito da un visitatore al suo sito web, offrendo uno schermo consenso esplicito che non contiene le caselle di controllo Sì e, a condizione che il testo indica chiaramente il consenso, per esempio “Io, con la presente, il consenso al al trattamento dei miei dati”, e non per esempio,‘e 'chiaro per me che i miei dati saranno trattati’. Va da sé che le condizioni per il consenso informato, nonché le altre condizioni per ottenere un valido consenso devono essere soddisfatte.

> [Esempio 18] Una clinica per la chirurgia estetica cerca consenso esplicito da un paziente a trasferire la sua cartella clinica di un esperto il cui parere secondo viene richiesto dalle condizioni del paziente. La cartella clinica è un file digitale. Data la specificità delle informazioni in questione, la clinica chiede una firma elettronica della persona per ottenere un valido consenso esplicito e di essere in grado di dimostrare che esplicito consenso è stato ottenuto. [48]

Due verifica fase del consenso può anche essere un modo per assicurarsi un consenso esplicito è valido. Ad esempio, un soggetto di dati riceve una e-mail che li informa di intenti del controller per elaborare un record contenente i dati medici. Il controller spiega nella e-mail che chiede il consenso per l'utilizzo di uno specifico set di informazioni per uno scopo specifico. Se le persone interessate non convengano di utilizzare di questi dati, il controller di lui o lei chiede una risposta e-mail contenente la dichiarazione 'Accetto'. Dopo la risposta viene inviata, l'interessato riceve un link di verifica che deve essere cliccato, o un messaggio SMS con un codice di verifica, a confermare l'accordo.

Articolo 9 (2) non riconosce “necessario per l'esecuzione di un contratto” in deroga al divieto generale di elaborare categorie particolari di dati. Pertanto i controller e gli Stati membri che si occupano di questa situazione dovrebbero esplorare le eccezioni specifiche di cui all'articolo 9 (2) commi (b) a (j). Qualora nessuna delle eccezioni (b) applicare (j), ottenere il consenso esplicito in conformità con le condizioni per un valido consenso nel GDPR rimane l'unica eccezione legale possibile trattare tali dati.

> [Esempio 19]
> Una compagnia aerea, vacanze Airways, offre un servizio itinerante assistito per i passeggeri che non possono viaggiare senza assistenza, per esempio a causa di una disabilità. Un cliente prenota un volo da Amsterdam a Budapest e le richieste di assistenza di viaggio per essere in grado di salire sull'aereo. Vacanze Airways lei richiede di fornire informazioni sul suo stato di salute per essere in grado di organizzare i servizi appropriati per il suo (e quindi, ci sono molte possibilità
> es carrozzina sul cancello di arrivo, o un assistente che viaggiano con lei da A a B.) Casa Airways chiede esplicito consenso al trattamento dei dati sanitari di questo cliente al fine di organizzare l'assistenza di viaggio richiesto. -I dati elaborati sulla base del consenso dovrebbe essere necessario per il servizio richiesto. Inoltre, i voli per Budapest rimangono disponibili senza assistenza di viaggio. Si prega di notare che, dal momento che i dati sono necessari per l'erogazione del servizio richiesto, l'articolo 7 (4) non si applica.

> [Esempio 20]
> Un'azienda di successo è specializzata nella fornitura di sci e snowboard occhiali su misura, e di altri tipi di occhiali su misura per gli sport all'aria aperta. L'idea è che le persone potevano indossare questi senza i propri occhiali. L'azienda riceve ordini ad un punto centrale e fornisce prodotti da una singola postazione in tutta l'Unione europea.

---

[48] Questo esempio è fatto salvo il regolamento (UE) n 910/2014 del Parlamento europeo dell'UE e del Consiglio, del 23 luglio 2014 in servizi di identificazione e di fiducia elettronici per le transazioni elettroniche nel mercato interno.

Al fine di essere in grado di fornire ai propri prodotti su misura per i clienti che sono miope, questo le richieste del controller il consenso per l'utilizzo delle informazioni sulla patologia oculare clienti. I clienti forniscono i dati sanitari necessari, come ad esempio i dati di prescrizione on-line quando mettono il loro ordine. Senza questo, non è possibile fornire l'occhiale personalizzato richiesto. L'azienda offre anche una serie di occhiali con valori di correzione standardizzati. I clienti che non desiderano condividere dati sanitari potrebbero optare per le versioni standard. Pertanto, un consenso esplicito ai sensi dell'articolo 9 è richiesta e il consenso può essere considerato per essere dato liberamente.

5. Ulteriori condizioni per ottenere un valido consenso

Il GDPR introduce requisiti per i controller di fare accordi supplementari per assicurare che ottenere e mantenere e sono in grado di dimostrare, un valido consenso. L'articolo 7 della GDPR definisce queste condizioni supplementari per un valido consenso, con disposizioni specifiche in materia di tenuta dei registri il consenso e il diritto di ritirare facilmente il consenso. L'articolo 7 si applica anche ai consenso di cui in altri articoli di GDPR, ad esempio articoli 8 e 9. Guida alla ulteriore requisito per dimostrare un valido consenso e sulla revoca del consenso è fornito di seguito.

5.1. dimostrare il consenso

All'articolo 7 (1), il GDPR delinea chiaramente l'obbligo esplicito del controller per dimostrare il consenso di un soggetto di dati . L'onere della prova sarà sul controller, ai sensi dell'articolo 7 (1).

Considerando 42 Stati: *"Se la trasformazione si basa sul consenso della persona interessata, il regolatore deve essere in grado di dimostrare che il soggetto abbia dato consenso alla operazione di elaborazione."*

Controller sono liberi di sviluppare metodi per conformarsi alla presente disposizione in un modo che si addice nelle loro operazioni quotidiane. Allo stesso tempo, il dovere di dimostrare che un valido consenso è stato ottenuto da un controllore, non dovrebbe di per sé portare a quantità eccessive di elaborazione dati aggiuntivi. Ciò significa che i controllori devono avere dati sufficienti per mostrare un collegamento al trattamento (per mostrare il consenso è stato ottenuto), ma non dovrebbero essere la raccolta di ulteriori informazioni del necessario.

Spetta al controllore per dimostrare che un valido consenso è stato ottenuto dalla persona. Il GDPR non prescrive esattamente come questo deve essere fatto. Tuttavia, il regolatore deve essere in grado di dimostrare che un soggetto di dati in un dato caso è consentito. Fintanto di un'attività di trasformazione di dati in questione dura, l'obbligo di dimostrare consenso esiste. Dopo l'attività di trasformazione si conclude, la prova del consenso deve essere tenuto più quindi strettamente necessario per adempiere un obbligo legale o per costituire, esercitare o difendere un diritto per via giudiziaria, ai sensi dell'articolo 17 (3) (b) e (e) .

Per esempio, il controllore può tenere un registro delle dichiarazioni di consenso ricevuti, in modo che possa dimostrare come il consenso è stato ottenuto, quando il consenso è stato ottenuto e le informazioni fornite alla persona interessata al momento deve essere dimostrabile. Il regolatore deve anche essere in grado di dimostrare che l'interessato è stato informato e il flusso di lavoro controller's incontrato tutti i criteri rilevanti per un valido consenso. La logica alla base di questo obbligo in GDPR è che i controllori devono rendere conto per quanto riguarda l'ottenimento di un valido consenso da titolari dei dati e dei meccanismi di consenso che hanno messo in atto. Ad esempio, in un contesto online, un controller potrebbe conservare le informazioni sulla sessione in cui è stato espresso il consenso e la documentazione del flusso di lavoro il consenso al momento della sessione, e un

copia delle informazioni che è stato presentato alla persona in quel momento. Non sarebbe sufficiente indirizzare ad una corretta configurazione del rispettivo sito.

> [Esempio 21] Un ospedale istituisce un programma di ricerca scientifica, chiamato progetto X, per i quali sono necessarie le impronte dentali di pazienti reali. I partecipanti sono stati reclutati attraverso chiamate telefoniche a pazienti che volontariamente hanno accettato di essere su una lista di candidati che possono essere avvicinato a questo scopo. Il controllore cerca consenso esplicito da parte dei soggetti di dati per l'utilizzo dei loro record dentale. Il consenso si ottiene durante una telefonata registrando una dichiarazione orale della persona in cui l'interessato conferma di essere d'accordo con l'uso dei propri dati ai fini del progetto X.

Non v'è alcun limite di tempo specifico nel GDPR per quanto tempo durerà il consenso. Quanto tempo dura il consenso dipenderà dal contesto, la portata del consenso originale e le aspettative della persona interessata. Se le operazioni di trattamento cambiano o si evolvono considerevolmente allora il consenso originale non è più valida. Se questo è il caso, allora nuovo il consenso deve essere ottenuto.

WP29 raccomanda come una best practice che il consenso deve essere aggiornata ad intervalli appropriati. Fornendo tutte le informazioni aiuta ancora una volta a garantire la persona interessata rimane ben informati su come i loro dati viene utilizzato e come esercitare i loro diritti. [49]

5.2. Ritiro del consenso

Revoca del consenso viene dato un posto di rilievo nel GDPR. Le disposizioni e recital di revoca del consenso nel GDPR possono essere considerati come codificazione del l'interpretazione attuale di questa materia nel WP29 pareri. [50]

Articolo 7 (3) della GDPR prevede che il controllore deve garantire che il consenso può essere ritirato dal soggetto dati facile come dare consenso e in qualsiasi momento. Il GDPR non dice che dare e ritirare il consenso deve sempre essere fatto attraverso la stessa azione.

Tuttavia, quando il consenso è ottenuto tramite mezzi elettronici attraverso un solo clic del mouse, colpo, o battitura, interessati deve, in pratica, in grado di prelevare tale consenso altrettanto facilmente. In cui il consenso è ottenuto attraverso l'uso di un'interfaccia utente specifica del servizio (ad esempio, attraverso un sito web, un'applicazione, un log-in considerazione, l'interfaccia di un dispositivo degli oggetti o per e-mail), v'è senza dubbio un soggetto di dati deve essere in grado di ritirare il consenso tramite la stessa interfaccia elettronica, come il passaggio a un'altra interfaccia per il solo fatto di ritirare il consenso richiederebbe sforzo eccessivo. Inoltre, la persona interessata dovrebbe essere in grado di ritirare il suo / proprio consenso senza danno. Ciò significa, tra l'altro, che un controllore deve fare revoca del consenso possibile a titolo gratuito o senza abbassare i livelli di servizio. [51]

---

[49] Vedere WP29 linee guida in materia di trasparenza. [Citazione da finalizzare quando disponibile]

[50] WP29 ha discusso questo argomento nel loro parere sul consenso (vedi parere 15/2011 sulla definizione di consenso (WP 187), pp. 9, 13, 20, 27 e 32-33) e, tra l'altro, il loro parere in merito all'utilizzo dei dati di localizzazione. (Vedi Parere 5/2005 sull'uso di dati relativi all'ubicazione, al fine di fornire servizi a valore aggiunto (WP 115), p. 7).

[51] Vedi anche il parere WP29 Parere 4/2010 sul codice di condotta europeo della FEDMA per l'uso dei dati personali nel settore direct marketing (WP 174) e il parere sull'uso dei dati di localizzazione al fine di fornire servizi a valore aggiunto (WP 115).

[Esempio 22] Un festival di musica vende i biglietti attraverso un agente di viaggio on-line. Con ogni vendita di biglietti on-line, il consenso è richiesta al fine di utilizzare informazioni di contatto per scopi di marketing. Per indicare il consenso per questo scopo, i clienti possono selezionare No o Sì. Il controller informa i clienti che hanno la possibilità di ritirare il consenso. Per fare questo, si potrebbe contattare un call center nei giorni lavorativi 8:00-17:00, a titolo gratuito. Il controllore in questo esempio fa non conformi all'articolo 7 (3) della GDPR. Ritirare il consenso in questo caso richiede una chiamata telefonica durante l'orario lavorativo, questo è più gravoso di quello clic del mouse necessario per dare il consenso attraverso il venditore di biglietti on-line, che è aperto 24/7.

Il requisito di un recesso facile è descritto come un aspetto necessario di consenso valido per la GDPR. Se il diritto di recesso non soddisfa i requisiti GDPR, allora il meccanismo di consenso del regolatore non conforme alla GDPR. Come menzionato nella sezione 3.1 sulla condizione *informato* il consenso, il regolatore deve informare la persona del diritto di revocare il consenso prima di effettivamente dare il consenso, ai sensi dell'articolo 7 (3) della GDPR. Inoltre, il regolatore deve, nell'ambito dell'obbligo di trasparenza informare le persone interessate su come esercitare i loro diritti. [52]

Come regola generale, se il consenso viene ritirata, tutte le operazioni di trattamento dei dati che erano basati sul consenso e hanno avuto luogo prima del ritiro del consenso - e in accordo con la GDPR - rimangono lecito, tuttavia, il regolatore deve fermare le azioni di trasformazione interessati. Se non v'è altra base legale che giustifica il trattamento (ad esempio a seguito di stoccaggio) dei dati, dovrebbero essere eliminati dal controllore. [53]

Come accennato in precedenza in queste linee guida, è molto importante che i controllori valutano gli scopi per cui i dati vengono effettivamente trattati ei motivi legittimi su cui si basa prima di raccogliere i dati. Spesso le aziende hanno bisogno di dati personali per scopi diversi, e l'elaborazione si basa su più di una base legale, ad esempio, i dati dei clienti possono essere basati su contratto e consenso. Quindi, un ritiro del consenso non significa un controllore deve cancellare i dati che vengono elaborati per uno scopo che si basa sulle prestazioni del contratto con la persona. Controller dovrebbero quindi essere chiaro fin dall'inizio su quale scopo si applica ad ogni elemento dei dati, e che base legale viene invocata da.

Controller hanno l'obbligo di cancellare i dati che sono stati elaborati sulla base del consenso, una volta che il consenso è ritirato, supponendo che non v'è nessun altro scopo che giustifica il mantenimento continuato. [54]

Oltre a questa situazione, coperto all'articolo 17 (1) (b), un singolo dato soggetto può richiedere la cancellazione dei dati che lo riguardano altri che viene elaborato su un'altra base legittima, ad esempio sulla base dell'articolo 6 (1) (b). [55] Controller hanno l'obbligo di valutare se continuare l'elaborazione dei dati in questione è opportuno, anche in assenza di una richiesta di cancellazione da parte dell'interessato. [56]

---

[52] Considerando 39 GDPR, che fa riferimento agli articoli 13 e 14 del suddetto regolamento, stabilisce che *"Le persone fisiche devono essere consapevoli dei rischi, regole, tutele e diritti in relazione al trattamento dei dati personali e il modo di esercitare i loro diritti in relazione a tale trattamento.*

[53] Si veda l'articolo 17 (1) (b) e (3) GDPR.

[54] In tal caso, l'altro scopo che giustifica il trattamento deve avere una propria base giuridica distinta. Questo non significa che il controllore può passare dal consenso ad un'altra base legale, vedere la sezione 6 di seguito.

[55] Si veda l'articolo 17, incluse le eccezioni che si possono applicare, e Considerando 65 GDPR

[56] Vedi anche l'articolo 5 (1) (e) GDPR

Nei casi in cui la persona ritira la / il suo consenso e il controllore desidera continuare ad elaborare i dati personali su un'altra base legittima, non possono migrare da silenzio consenso (che viene ritirata) a questa altra base legale. Qualsiasi cambiamento nella base legale per l'elaborazione deve essere notificata ad un soggetto dei dati in conformità con gli obblighi di informazione di cui agli articoli 13 e 14 e in base al principio generale di trasparenza.

6. L'interazione tra il consenso e altri motivi legittimi di cui all'articolo 6 GDPR

L'articolo 6 stabilisce le condizioni per un legittimo trattamento dei dati personali e descrive sei basi legali su cui un controllore può fare affidamento. L'applicazione di uno di questi sei basi deve essere stabilito prima dell'attività trasformazione e in relazione ad uno scopo specifico. [57]

E 'importante notare che se un controllore sceglie contare su consenso per qualsiasi parte del trattamento, devono essere disposti a rispettare tale scelta e fermare quella parte dell'elaborazione se un individuo si ritira consenso. Invio il messaggio che i dati saranno trattati sulla base del consenso, mentre in realtà un altro fondamento legittimo è invocato, sarebbe fondamentalmente ingiusto per gli individui.

In altre parole, il controllore non può passare dal consenso ad altre basi legali. Ad esempio, non è consentito di utilizzare in modo retrospettivo la base interesse legittimo al fine di giustificare l'elaborazione, in cui sono stati riscontrati problemi con la validità del consenso. A causa del requisito di rivelare la base legale, che il controllore fa affidamento su al momento della raccolta dei dati personali, i controllori devono aver deciso in anticipo della raccolta ciò che la base legale applicabile è.

7. specifiche aree di interesse nel GDPR

7.1. Bambini (articolo 8)

Rispetto alla direttiva vigente, la GDPR crea un ulteriore livello di protezione in cui sono trattati i dati personali delle persone fisiche vulnerabili, soprattutto i bambini,. L'articolo 8 introduce ulteriori obblighi al fine di garantire un maggiore livello di protezione dei dati dei minori in relazione ai servizi della società dell'informazione. Le ragioni di maggior tutela sono specificati nel considerando 38: *"[...] possono essere meno consapevoli dei rischi, le conseguenze e le garanzie in questione e dei loro diritti in relazione al trattamento dei dati personali [...]"* Considerando 38 afferma anche che " *Tale protezione specifico dovrebbe, in particolare, si applica al trattamento dei dati personali dei bambini a fini di commercializzazione o la creazione di personalità o profili utente e la raccolta di dati personali per quanto riguarda i bambini quando utilizzano i servizi offerti direttamente ad un minore."* Le parole 'in particolare' indicano che la protezione specifica non si limita al marketing o profilazione ma include la 'raccolta di dati personali per quanto riguarda i bambini' più ampio.

Articolo 8 (1) stabilisce che se il consenso si applica, in relazione all'offerta di servizi della società dell'informazione direttamente ad un minore, il trattamento dei dati personali di un bambino è lecito in cui il bambino è di almeno 16 anni. Dove il bambino è di età inferiore ai 16 anni, tale trattamento sarà lecito

[57] Conformemente agli articoli 13 (1) (c) e / o 14 (1) (c), il regolatore deve informare la persona stessa.

solo se e nella misura in cui il consenso è dato o autorizzato dal titolare della responsabilità genitoriale sul minore. [58] Per quanto riguarda il limite di età di un valido consenso del GDPR fornisce la flessibilità, gli Stati membri possono prevedere nella legislazione nazionale un'età inferiore, ma questa età non può essere inferiore a 13 anni.

Come menzionato nella sezione 3.1. il consenso informato, l'informazione deve essere comprensibile per il pubblico indirizzato dal regolatore, prestando particolare attenzione alla posizione dei bambini. Al fine di ottenere il “consenso informato” da un bambino, il regolatore deve spiegare in un linguaggio chiaro e semplice per i bambini come intende elaborare i dati raccolti. [59] Se è il genitore che dovrebbe consentire, poi una serie di informazioni può essere richiesto che permette agli adulti di prendere una decisione informata.

E 'chiaro da quanto precede che l'articolo 8 si applica soltanto se sono soddisfatte le seguenti condizioni:

- Il trattamento è legata alla offerta di servizi della società dell'informazione direttamente ad un minore. [60, 61]
- Il trattamento si basa sul consenso.

7.1.1. servizio della società dell'informazione

Per determinare la portata della nozione di 'servizio della società dell'informazione”nel GDPR, si fa riferimento all'articolo 4 (25) GDPR della direttiva 2015/1535.

Mentre valutare la portata di questa definizione, WP29 riferisce anche alla giurisprudenza della CGE. [62] La Corte di giustizia ha ritenuto che *servizi della società dell'informazione* contratti di copertura e altri servizi che sono conclusi o trasmessi on-line. Quando un servizio ha due componenti economicamente indipendenti, uno è il componente online, come 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, questa componente è definita come un servizio della società dell'informazione, l'altro componente è la consegna fisica o la distribuzione di merci non è coperta dalla nozione di un servizio della società dell'informazione. La consegna online di un servizio sarebbe rientrano nell'ambito di applicazione del termine *servizio della società dell'informazione* all'articolo 8 GDPR.

---

[58] Fatta salva la possibilità di legislazione degli Stati membri di derogare al limite di età, vedere l'articolo 8, (1).

[59] Considerando 58 GDPR riafferma tale obbligo, affermando che, se del caso, un controller dovrebbe assicurarsi che le informazioni fornite siano comprensibili per i bambini.

[60] Ai sensi dell'articolo 4 (25) GDPR un servizio della società dell'informazione: un servizio di cui alla lettera (b) dell'articolo 1 (1), 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 ea richiesta individuale di un destinatario di servizi. Ai fini della presente definizione: (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' significa che il servizio è fornito mediante trasmissione di dati su richiesta individuale “*. Un elenco indicativo di servizi non contemplati da tale definizione di cui all'allegato I della suddetta direttiva. Vedi anche il considerando 18 della direttiva 2000/31.

[61] Secondo la Convenzione delle Nazioni Unite sulla protezione del minore, l'articolo 1, *“[...] un bambino significa ogni essere umano avente un'età inferiore a diciotto anni a meno che sotto la legge applicabile al bambino, la maggioranza abbia raggiunto prima,”* vedi Nazioni Unite, Risoluzione dell'Assemblea Generale 44/25 del 20 novembre 1989 (Convenzione sui diritti del fanciullo).

[62] Vedere Corte di giustizia europea, 2 dicembre 2010, causa C-108/09, (*Ker-Optika),* punti 22 e 28. In relazione alla 'servizi compositi', WP29 riferisce anche a causa C-434/15 (*Asociacion Profesional Elite Taxi v Uber Sistemi Spain SL),* para 40, che stabilisce che un servizio della società dell'informazione facente parte integrante di un servizio globale cui componente principale non è un servizio della società dell'informazione (in questo caso un servizio di trasporto), non deve essere qualificata come 'un servizio della società dell'informazione'.

7.1.2. Offerto direttamente ad un minore

L'inserimento della dicitura 'offerto direttamente ad un minore' indica che l'articolo 8 è destinato ad essere applicato ad alcuni, non tutti i servizi della società dell'informazione. A questo proposito, se un fornitore di servizi della società dell'informazione rende chiaro ai potenziali utenti che sta solo offrendo il suo servizio alle persone di età 18 anni, e questo non venga compromessa da altri elementi (come ad esempio il contenuto dei piani del sito o di marketing) quindi il servizio non sarà considerato 'offerto direttamente ad un minore' e l'articolo 8 non si applica.

7.1.3. Età

Il GDPR specifica che *"Gli Stati membri possono disporre per legge per un periodo inferiore a tali fini, a condizione che tale età inferiore non sia inferiore a 13 anni."* Il regolatore deve essere a conoscenza di tali diverse leggi nazionali, prendendo in considerazione il pubblico interessato dai suoi servizi. In particolare si segnala che un controller che fornisce un servizio transfrontaliero non può sempre contare su rispettare solo la legge dello Stato membro in cui ha la sua sede principale, ma potrebbe essere necessario rispettare le rispettive leggi nazionali di ciascuno Stato membro in che offre il servizio della società dell'informazione (s). Questo dipende dal fatto che uno Stato membro decide di utilizzare il luogo di stabilimento principale del controller come un punto di riferimento nella propria legislazione nazionale, o la residenza della persona interessata. Prima di tutto gli Stati membri prendere in considerazione l'interesse superiore del bambino durante fare la loro scelta. Il gruppo di lavoro incoraggia gli Stati membri a cercare una soluzione armonizzata in questa materia.

Nel fornire servizi della società dell'informazione per i bambini sulla base del consenso, i controllori dovranno compiere sforzi ragionevoli per verificare che l'utente è finita l'età del consenso digitale, e queste misure dovrebbero essere proporzionate alla natura e dei rischi delle attività di trattamento.

Se gli utenti affermano che sono oltre l'età del consenso digitale, allora il controller può effettuare controlli adeguati per verificare che questa affermazione è vera. Anche se la necessità di intraprendere gli sforzi ragionevoli per verificare l'età non è esplicito nella GDPR è implicitamente richiesto, per se un bambino dà il consenso anche se non abbastanza grande per fornire un valido consenso per proprio conto, allora questo renderà il trattamento dei dati illegali.

Se l'utente dichiara che lui / lei è sotto l'età del consenso digitale allora il controller può accettare questa affermazione senza ulteriori verifiche, ma avrà bisogno di andare avanti per ottenere l'autorizzazione dei genitori e verificare che la persona che fornisce che il consenso è un titolare della responsabilità genitoriale .

verifica dell'età non dovrebbe portare a un eccessivo trattamento dei dati. Il meccanismo scelto per verificare l'età del soggetto dati dovrebbe comportare una valutazione del rischio del trattamento proposto. In alcune situazioni a basso rischio, può essere opportuno richiedere un nuovo abbonato ad un servizio di rivelare il loro anno di nascita o per compilare un modulo affermando che sono (non) un minore. [63] In caso di dubbi il controller

[63] Anche se questa non può essere una soluzione tenuta in tutti i casi, è un esempio di affrontare questa disposizione

dovrebbero rivedere i loro meccanismi di verifica dell'età in un determinato caso e valutare se controlli alternativi sono necessari. [64]

7.1.4. il consenso per bambini e responsabilità genitoriale

Per quanto riguarda l'autorizzazione di un titolare della responsabilità genitoriale, il GDPR non specifica le modalità pratiche per raccogliere il consenso del genitore o di stabilire che qualcuno ha il diritto di eseguire questa azione. [65] Pertanto, il WP29 raccomanda l'adozione di un approccio proporzionato, in linea con l'articolo 8 (2) GDPR e dell'articolo 5 (1) (c) GDPR (minimizzazione dei dati). Un approccio proporzionato può essere quello di concentrarsi su come ottenere una quantità limitata di informazioni, come ad esempio informazioni di contatto di un genitore o tutore.

Che cosa è ragionevole, sia in termini di verificare che un utente è abbastanza grande per fornire il proprio consenso, e in termini di verificare che una persona che fornisce il consenso per conto di un bambino è un titolare della responsabilità genitoriale, può dipendere i rischi inerenti l'elaborazione e la tecnologia disponibile. Nei casi a basso rischio, la verifica della responsabilità genitoriale via e-mail può essere sufficiente. Al contrario, nei casi ad alto rischio, può essere opportuno chiedere di più la prova, in modo che il controller è in grado di verificare e conservare le informazioni a norma dell'articolo 7 (1) GDPR. [66] servizi di verifica di terze parti di fiducia possono offrire soluzioni che riducono al minimo la quantità di dati personali del controllore deve processare se stesso.

> [Esempio 23] Una piattaforma di gioco online vuole assicurarsi che i clienti minorenni abbonarsi solo ai suoi servizi con il consenso dei loro genitori o tutori. Il controllore segue questi passaggi:
> Fase 1: chiedere all'utente di indicare se sono sotto o sopra l'età di 16 (o l'età del consenso alternativa digitale) Se l'utente dichiara che sono sotto l'età del consenso digitale:
> Fase 2: il servizio informa il bambino che un genitore o tutore deve consentire o autorizzare il trattamento prima che il servizio è fornito al bambino. L'utente è pregato di comunicare l'indirizzo e-mail di un genitore o di un tutore. Fase 3: i contatti di servizio del genitore o tutore e ottiene la loro consenso via e-mail per l'elaborazione e adottare misure ragionevoli per verificare che l'adulto ha la responsabilità dei genitori.
>
> Fase 4: in caso di disturbi, la piattaforma prende ulteriori passaggi per verificare l'età del sottoscrittore. Se la piattaforma ha incontrato gli altri requisiti di consenso, la piattaforma può soddisfare i criteri supplementari di cui all'articolo 8 GDPR seguendo questi passaggi.

L'esempio mostra che il controllore può collocarsi in grado di dimostrare che sono stati fatti sforzi per garantire che un valido consenso è stato ottenuto, in relazione ai servizi forniti ad un bambino. L'articolo 8 (2) in particolare aggiunge che " *Il controller compiono sforzi ragionevoli per verificare che il consenso è dato o autorizzato dal titolare della responsabilità genitoriale sul minore, prendendo in considerazione la tecnologia disponibile ".*

---

[64] Vedere WP29 Parere 5/2009 sui servizi di social networking (WP 163).

[65] WP 29 note che non sempre il caso che il titolare della responsabilità genitoriale è il padre naturale del bambino e che la responsabilità dei genitori può essere ritenuta da più parti che possono includere legale così come le persone fisiche.

[66] Ad esempio, un genitore o un tutore potrebbe essere chiesto di effettuare un pagamento di € 0,01 al controller tramite una transazione bancaria, tra cui una breve conferma nella linea descrizione dell'operazione che il titolare del conto bancario è un titolare della responsabilità genitoriale su l'utente. Se del caso, deve essere fornito un metodo alternativo di verifica per impedire il trattamento discriminatorio indebita di persone che non hanno un conto bancario.

Spetta al controllore per determinare quali misure sono appropriate in un caso specifico. Come regola generale, i controllori dovrebbero evitare soluzioni di verifica che si coinvolgono la raccolta eccessiva di dati personali.

WP29 riconosce che ci possono essere casi in cui la verifica è impegnativo (per esempio dove i bambini che forniscono il proprio consenso non hanno ancora stabilito un 'identità impronta', o dove la responsabilità dei genitori non è facilmente controllato. Questo può essere preso in considerazione per decidere quali sforzi sono ragionevole, ma i controllori saranno inoltre tenuti a mantenere i loro processi e la tecnologia disponibile costantemente sotto controllo.

Per quanto riguarda l'autonomia della persona interessata per il consenso al trattamento dei propri dati personali e avere il pieno controllo del processo, il consenso da un titolare della responsabilità genitoriale o autorizzato da un titolare della responsabilità genitoriale per il trattamento dei dati personali dei bambini può essere confermata , modificate o ritirate, una volta che la persona raggiunge l'età di consenso digitale. In pratica, questo significa che se il bambino non prende alcuna azione, il consenso dato da un titolare della responsabilità genitoriale o autorizzato da un titolare della responsabilità genitoriale per il trattamento dei dati personali forniti prima l'età del consenso digitale, rimarrà una valida terreno per l'elaborazione. Dopo aver raggiunto l'età del consenso digitale, il bambino avrà la possibilità di ritirare il consenso se stesso, in linea con l'articolo 7 (3). [67]

E 'importante sottolineare che, in conformità con il considerando 38, il consenso da un genitore o tutore non è necessario nel contesto dei servizi di prevenzione e di consulenza offerti direttamente ad un minore. Per esempio la fornitura di servizi di protezione dell'infanzia offerti on-line ad un bambino per mezzo di un servizio di chat online non richiedono previa autorizzazione dei genitori.

Infine, il GDPR stabilisce che le norme relative ai requisiti di autorizzazione dei genitori dei minori nei confronti non devono interferire con “il diritto contrattuale generale degli Stati membri, come le norme sulla formazione, validità o efficacia di un contratto in relazione ad un bambino” . Pertanto, i requisiti per un valido consenso per l'uso dei dati relativi a bambini sono parte di un quadro giuridico che deve essere considerato come separato dal diritto contrattuale nazionale. Pertanto, questo documento di orientamento non tratta la questione se sia lecito per un minore di concludere contratti on-line. Entrambi i regimi giuridici possono verificare contemporaneamente, e, la portata della GDPR non comportano l'armonizzazione delle disposizioni nazionali di diritto contrattuale.

7.2. Ricerca scientifica

La definizione di scopi di ricerca scientifica ha ramificazioni importanti per la gamma delle attività di trattamento dei dati di un controllore può intraprendere. Il termine *'ricerca scientifica'* non è definita nel GDPR. Punto 159 Stati “(...) *Ai fini del presente regolamento, al trattamento di dati personali per scopi di ricerca scientifica deve essere interpretato in modo ampio. (* ...)”, ma il WP29

[67] Inoltre, le persone interessate devono essere consapevoli del diritto all'oblio di cui all'articolo 17, che mira in particolare rilevante per consenso quando la persona interessata era ancora un bambino, si veda il considerando 63.

considera l'idea non può essere allungato oltre il suo significato comune e capisce che ' *ricerca scientifica'* in questo contesto significa un progetto di ricerca impostato secondo i principi metodologici ed etici settoriali pertinenti, in conformità alla buona pratica.

Quando il consenso è la base giuridica per condurre ricerche in base alla GDPR, questo consenso al trattamento dei dati personali deve essere distinto da altri obblighi previsti che servono come uno standard etico o obbligo procedurale. Un esempio di un tale obbligo procedurale, in cui il trattamento non si basa sul consenso, ma su un altro fondamento giuridico, è da ricercarsi nel regolamento studi clinici. Nel contesto della tutela dei dati, quest'ultima forma di consenso può essere considerato come ulteriore garanzia. [68] Allo stesso tempo, il GDPR non limita l'applicazione dell'articolo 6 per consentire da solo, per quanto riguarda il trattamento dei dati per scopi di ricerca. Fintanto che adeguate garanzie sono in atto, come ad esempio i requisiti di cui all'articolo 89 (1), e l'elaborazione è giusto, legale, trasparente e accordi con standard dati minimizzazione e diritti individuali, altre basi legali come articolo 6 (1) (e) o (f) potrebbero essere disponibili. [69] Questo vale anche per categorie particolari di dati ai sensi della deroga di cui all'articolo 9 (2) (j). [70]

Considerando 33 sembra portare una certa flessibilità al grado di specificazione e la granularità del consenso nel contesto della ricerca scientifica. Considerando 33 afferma: " *Spesso non è possibile identificare pienamente lo scopo del trattamento dei dati personali a fini di ricerca scientifica, al momento della raccolta dei dati. Pertanto, gli interessati dovrebbero essere autorizzati a dare il loro consenso ad alcune aree della ricerca scientifica quando è in linea con gli standard etici riconosciuti per la ricerca scientifica. Gli interessati devono avere la possibilità di dare il proprio consenso solo a determinate aree di ricerca o parti di progetti di ricerca nella misura consentita dalla destinazione.* "

In primo luogo, va osservato che il considerando 33 non disapplicare gli obblighi per quanto riguarda il requisito del consenso specifico. Ciò significa che, in linea di principio, i progetti di ricerca scientifica possono includere solo i dati personali sulla base del consenso se hanno uno scopo ben descritto. Per i casi in cui ai fini del trattamento dei dati all'interno di un progetto di ricerca scientifica non possono essere specificate, in via preliminare, il considerando 33 permette come eccezione che lo scopo può essere descritto a un livello più generale.

Considerando le rigorose condizioni fissate dall'articolo 9 GDPR per quanto riguarda il trattamento di categorie particolari di dati, WP29 osserva che quando le categorie particolari di dati vengono elaborati sulla base di un consenso esplicito, applicando l'approccio flessibile del considerando 33 sarà oggetto di un'interpretazione più rigorosa e richiede un alto grado di controllo.

Quando considerato nel suo complesso, il GDPR non può essere interpretato per consentire un controller per navigare nel principio fondamentale di scopi per cui si chiede il consenso della persona specifica.

---

[68] Vedi anche il considerando 161 del GDPR.

[69] L'articolo 6 (1) (c) può essere applicata anche per le parti delle operazioni di trattamento specificamente previste dalla legge, come ad esempio la raccolta di dati affidabili e robuste seguendo il protocollo approvato dallo Stato membro ai sensi del regolamento sperimentazione clinica.

[70] test specifici di medicinali può avvenire sulla base di una legge dell'UE o nazionale ai sensi dell'articolo 9 (2) (i).

Quando fini della ricerca non possono essere completamente specificati, un controllore deve cercare altri modi per garantire l'essenza degli obblighi previsti sono serviti meglio, per esempio, per consentire agli interessati di consenso per uno scopo di ricerca, in termini più generali e per le fasi specifiche di una ricerca progetto che sono già noti che si terrà in via preliminare. Con l'avanzare della ricerca, il consenso per le successive fasi del progetto può essere ottenuto prima che inizi la prossima fase. Tuttavia, un tale consenso dovrebbe essere ancora in linea con gli standard etici applicabili per la ricerca scientifica.

Inoltre, il controllore può applicare ulteriori garanzie in tali casi. Articolo 89 (1), ad esempio, mette in evidenza la necessità di garanzie nelle attività di trattamento dei dati a fini scientifici o storici o statistici. Questi scopi " *sono soggetti ad adeguate misure di salvaguardia, a norma del presente regolamento, per i diritti e le libertà delle persone interessate.* "Minimizzazione dei dati, in forma anonima e la sicurezza dei dati sono menzionati come possibili misure di salvaguardia. [71] Anonimizzazione è la soluzione preferita non appena lo scopo della ricerca può essere raggiunto senza il trattamento dei dati personali.

La trasparenza è una garanzia supplementare quando le circostanze della ricerca non consentono per uno specifico consenso. La mancanza di specifiche finalità può essere compensato da informazioni sullo sviluppo dello scopo di essere regolarmente fornito dai controller come il progetto di ricerca progredisce in modo che, nel corso del tempo, il consenso sarà il più specifici possibile. Nel fare ciò, la persona interessata ha almeno una conoscenza di base dello stato di avanzamento, consentendo lui / lei per valutare se utilizzare o meno, ad esempio, il diritto di ritirare il consenso ai sensi dell'articolo 7 (3). [72]

Inoltre, avere un piano di ricerca completo disponibile per gli interessati di prendere atto di, prima di consenso potrebbe aiutare a compensare la mancanza di specifiche finalità. [73] Questo piano di ricerca deve specificare le domande di ricerca e metodi di lavoro previsti nel modo più chiaro possibile. Il piano di ricerca potrebbe anche contribuire al rispetto dell'articolo 7 (1), i controllori devono mostrare quali informazioni era disponibile agli interessati al momento del consenso, al fine di essere in grado di dimostrare che il consenso sia valido.

È importante ricordare che, quando il consenso viene utilizzato come base legittima per l'elaborazione deve essere una possibilità per un soggetto di dati di ritirare tale consenso. WP29 sottolinea che la revoca del consenso potrebbe minare i tipi di ricerca scientifica che richiedono i dati che possono essere collegati a singoli individui, ma il GDPR è chiaro che il consenso può essere ritirato e controllori deve agire su questo - ci

---

[71] Si veda ad esempio il considerando 156. Il trattamento dei dati personali per scopi scientifici dovrebbero anche rispettare altre normative pertinenti, come sulle sperimentazioni cliniche, vedasi considerando 156, citando il regolamento (UE) n 536/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014 sulle sperimentazioni cliniche di medicinali ad uso umano. Vedi anche WP29 parere 15/2011 sulla definizione del consenso (WP 187), p. 7: *"Inoltre, ottenere il consenso non annulla gli obblighi del controllore di cui all'articolo 6 per quanto riguarda la correttezza, necessità e proporzionalità, così come la qualità dei dati. Ad esempio, anche se il trattamento dei dati personali si basa sul consenso dell'utente, ciò non legittimare la raccolta di dati che è eccessivo rispetto ad uno scopo particolare. "[...] In linea di principio, il consenso non deve essere visto come un esonero dagli altri principi di protezione dei dati, ma come salvaguardia. E 'principalmente un motivo di liceità, e non rinuncia all'applicazione di altri principi."*

[72] Altre misure di trasparenza possono essere rilevanti. Quando i controllori impegnarsi nel trattamento dei dati per scopi scientifici, mentre le informazioni completo non può essere fornita in via preliminare, si potrebbe designare una persona di contatto specifici per le persone per affrontare con le domande.

[73] Tale possibilità può essere trovato nell'articolo 14 (1) della corrente legge sui dati personali di Finlandia (*Henkilötietolaki,* 523/1999)

è nessuna esenzione a questo requisito per la ricerca scientifica. Se un controller riceve una richiesta di prelievo, esso deve in linea di principio cancellare i dati personali subito se vuole continuare a utilizzare i dati per le finalità della ricerca. [74]

7.3. Diritti dell'interessato

Se un'attività di elaborazione dei dati si basa sul consenso di una persona interessata, questo influenzerà diritti dell'individuo. Gli interessati possono avere il diritto di portabilità dei dati (articolo 20), quando l'elaborazione è basata sul consenso. Allo stesso tempo, il diritto di opposizione (articolo 21) non si applica quando l'elaborazione si basa sul consenso, sebbene il diritto di ritirare il consenso in qualsiasi momento può fornire un risultato simile.

Articoli da 16 a 20 della GDPR indicare che (ove elaborazione dati si riferiscono al consenso), si ha il diritto di cancellazione quando il consenso è stata ritirata ei diritti alla restrizione, rettifica e accesso. [75]

8. Consenso ottenuto ai sensi della direttiva 95/46 / CE

I controller che attualmente trattano dati sulla base del consenso in conformità con il diritto nazionale sulla protezione dei dati non sono tenuti automaticamente per aggiornare completamente tutti i rapporti esistenti con il consenso interessati in preparazione per la GDPR. Il consenso che è stato ottenuto fino ad oggi continua ad essere valido in quanto è in linea con le condizioni stabilite nel GDPR.

E 'importante per i controllori di rivedere i processi di lavoro attuali e le registrazioni in dettaglio, prima del 25 maggio 2018, per essere sicuri che i consensi esistenti soddisfano gli standard GDPR (vedi considerando 171 del GDPR [76]). In pratica, il GDPR alza la barra quanto riguarda i meccanismi di attuazione e di consenso introduce diverse nuove esigenze che richiedono controllori di alterare i meccanismi di consenso, piuttosto che riscrivere le norme sulla privacy da solo. [77]

Ad esempio, come il GDPR richiede che un controller deve essere in grado di dimostrare che un valido consenso è stato ottenuto, tutti i consensi presunti di cui nessun riferimento sono mantenuti sarà automaticamente di sotto dello standard consenso del GDPR e dovranno essere rinnovati. Allo stesso modo come il GDPR richiede un “istruzione o una chiara azione affermativa”, tutti i consensi presunti che erano basati su una forma più implicita di azione da parte della persona (ad esempio un pre-spuntato opt-in box) anche non essere adatto per la standard di GDPR del consenso.

---

[74] Vedi anche WP29 parere 05/2014 sulla "Tecniche anonimizzazione" (WP216).

[75] Nei casi in cui le attività di elaborazione di alcuni dati sono limitate ai sensi dell'articolo 18, GDPR, il consenso della persona interessata può essere necessaria per eliminare le restrizioni.

[76] Considerando 171 stati GDPR: “ *La direttiva 95/46 / CE deve essere abrogata dal presente regolamento. Trasformazione già in corso alla data di applicazione del presente regolamento deve essere portato in conformità al presente regolamento entro il periodo di due anni dopo la quale il regolamento entra in vigore. Se la trasformazione è basata sul consenso ai sensi della direttiva 95/46 / CE, non è necessario per la persona a dare il proprio consenso ancora se il modo in cui è stato dato il consenso è in linea con le condizioni del presente regolamento, in modo da consentire il controller di continuare tale trattamento dopo la data di applicazione del presente regolamento. Le decisioni della Commissione adottate e delle autorizzazioni da parte delle autorità di vigilanza sulla base della direttiva 95/46 / CE restano in vigore fino modificato, sostituito o abrogate.* ”

[77] Come indicato nell'introduzione, la GDPR fornisce ulteriori chiarimenti e specifiche dei requisiti per l'ottenimento e dimostrando valido consenso. Molti dei nuovi requisiti di costruire su di parere 15/2011 sul consenso.

Inoltre, per essere in grado di dimostrare che il consenso è stato ottenuto o per consentire indicazioni più granulari interrogando dell'interessato, operazioni e sistemi possono avere bisogno di revisione. Inoltre, i meccanismi per le persone interessate a ritirare il loro consenso facilmente devono essere disponibili e le informazioni su come ritirare il consenso deve essere fornita. Se le procedure esistenti per ottenere e gestire il consenso non soddisfano gli standard del GDPR, controller sarà necessario ottenere il consenso fresca GDPR- compatibile.

D'altra parte, come non tutti gli elementi nominati agli articoli 13 e 14 devono essere sempre presenti come condizione per il consenso informato, gli obblighi di informazione concessi alle GDPR non necessariamente si oppongono la continuità del consenso che è stato concesso prima della GDPR entra in forza (vedi sopra pagina 15). Ai sensi della direttiva 95/46 / CE, non vi era alcun obbligo di informare gli interessati della base su cui è stata condotta l'elaborazione.

Se un controller rileva che il consenso ottenuto in precedenza sotto la vecchia normativa non soddisfare lo standard del consenso GDPR, poi i controllori devono intervenire per rispettare queste norme, ad esempio aggiornando il consenso in maniera GDPR-compliant. Sotto il GDPR, non è possibile scambiare tra una base legale e altro. Se un controller è in grado di rinnovare consenso in modo compatibile ed è anche in grado -come una tantum situazione-per rendere la transizione a GDPR rispetto basando elaborazione dati su una diversa base legale garantendo nel contempo che continua elaborazione è equo e rappresentato, le attività di trattamento devono essere fermati. In ogni caso, il controllore deve rispettare i principi di liceità, equo e trasparente.

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