PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Linee guida sulle questioni etiche e legali della protezione dei dati nella ricerca e nell'innovazione delle TIC

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (GDPR) – DIRITTI DEGLI INTERESSATI

Questo progetto è stato finanziato dal programma di ricerca e innovazione Horizon 2020 dell'Unione Europea con l'accordo di sovvenzione n. 788039. Il presente documento riflette esclusivamente il punto di vista degli autori e l'Agenzia non può essere ritenuta responsabile per l'uso che può essere fatto delle informazioni in esso contenute.

4 Diritti degli interessati

Carlotta Rigotti, Andrés Chomczyk Penedo, Alessandro Ortalda, Paul De Hert (tutti VUB)

Ringraziamenti: Gli autori ringraziano la revisione e i suggerimenti di Rosario Duaso Cales e Saverio Carusso.

Questa parte delle Linee guida è stata convalidata da Willem Debeuckelaere, ex presidente dell'autorità belga per la protezione dei dati e vicepresidente del comitato europeo per la protezione dei dati

Il capitolo III del GDPR prevede una serie di diritti che gli interessati possono esercitare per salvaguardare i loro dati personali. Anche se ogni diritto ha dettagli specifici e questioni che potrebbero riguardare ed essere influenzate dalla ricerca[155] ICT, tutti condividono alcune caratteristiche generali riguardanti la loro informazione trasparente, la comunicazione e le modalità di esercizio (articolo 12 GDPR). A questo proposito, prima di lanciarsi nell'analisi di ogni diritto specifico (articolo 13-22 GDPR), è opportuno menzionare brevemente alcune questioni che ogni ricercatore e istituto di ricerca dovrebbe prendere in considerazione quando rispetta l'esercizio di uno dei diritti dell'interessato.

L'articolo 12.1 del GDPR inizia fornendo come le informazioni devono essere date agli interessati, in modo che possano esercitare efficacemente i loro diritti. In breve, il **titolare del trattamento deve fornire informazioni corrette e complete**, evitando così le informazioni inutili. Inoltre, **il linguaggio utilizzato deve essere comprensibile per l'interessato medio e fornito per iscritto** (a meno che l'interessato non richieda diversamente). A questo proposito, maggiori dettagli saranno forniti nella sezione 6.1.

Per quanto riguarda i tempi, il titolare del trattamento deve fornire informazioni sul seguito dato a una richiesta di esercizio del diritto dell'interessato senza ritardi indebiti o eccessivi e, in ogni caso, entro un mese dal ricevimento della richiesta, in base all'articolo 12.3 GDPR. Questo periodo può essere prorogato di altri due mesi, se necessario e a condizione che il titolare del trattamento informi l'interessato della proroga e la giustifichi entro un mese dal ricevimento della richiesta.

L'articolo 12.5 del GDPR consente al titolare del trattamento di rifiutare la richiesta dell'interessato se questa è manifestamente infondata o eccessiva. A questo proposito, alcuni

155 Come dimostrato da Ducato, infatti, il trattamento per finalità di ricerca gode di un regime favorevole all'interno del GDPR, in quanto cerca di bilanciare tra i diritti dell'interessato, la libertà d'impresa e le legittime aspettative della società per un aumento della conoscenza. Su tali premesse, l'articolo 89 del GDPR permette di derogare agli articoli 14, 15, 16, 18 e 21 del GDPR, alla sola condizione che siano fornite garanzie adeguate. In particolare, la disposizione richiede l'utilizzo di misure tecniche e organizzative per adempiere alla minimizzazione dei dati, nonché tecniche di anonimizzazione e pseudonimizzazione. In R. Ducato, "Data Protection, Scientific Research and the Role of Information", *Computer Law & Security Review,* 2020, Vol. 37, pp. 4-5

esempi potrebbero essere: gli interessati non hanno alcuna intenzione di esercitare i loro diritti (e richiedono, ad esempio, benefici in cambio del ritiro della richiesta), cercano di attaccare il titolare del trattamento, presentano richieste identiche nello stesso lasso di tempo, e così via. Contemporaneamente, l'articolo 12.5 GDPR stabilisce anche che l'esercizio di ogni diritto dell'interessato deve essere **gratuito**, a meno che il titolare del trattamento non sia in grado di dimostrare che la richiesta era manifestamente infondata o eccessiva. In questo caso, il titolare del trattamento può addebitare un costo ragionevole, considerando i costi amministrativi della procedura.

Se il titolare del trattamento ha ragionevoli dubbi sull'identità della persona che presenta una richiesta, il titolare del trattamento può richiedere la fornitura di informazioni aggiuntive al fine di confermare l'identità dell'interessato, sulla base dell'articolo 12.6 GDPR.

L'esercizio dei diritti dell'interessato: Trasparenza, comunicazione e modalità:

- ☐ Le informazioni fornite devono essere:
  - Corretto e completo, evitando così quelli inutili;
  - Comprensibile per l'interessato medio;
  - Facilmente accessibile, sia per iscritto che con qualsiasi altro mezzo;
  - In una lingua che l'interessato padroneggia bene.
- ☐ Le informazioni devono essere fornite:
  - Senza ritardi ingiustificati o eccessivi e, in ogni caso, entro un mese dalla richiesta dell'interessato;
  - Entro due mesi dalla richiesta dell'interessato, se necessario e previa comunicazione e giustificazione entro un mese dalla richiesta dell'interessato;
- ☐ La richiesta dell'interessato può essere rifiutata, in qualsiasi momento:
  - Manifestamente infondato;
  - Eccessivo;
- ☐ L'esercizio di ogni diritto dell'interessato deve essere gratuito. Se la richiesta è manifestamente infondata o eccessiva, può essere applicata una tassa ragionevole.
- ☐ Ulteriori informazioni possono essere richieste per confermare l'identità dell'interessato.

4.1 Diritto all'informazione

In base all'articolo 12 GDPR, i titolari del trattamento sono tenuti a informare gli interessati sul trattamento che intendono effettuare. Il diritto all'informazione è quindi intrecciato con il principio di trasparenza descritto nella sezione 3.1.1.4 e nel considerando 39 del GDPR.

Il diritto all'informazione **non richiede alcuna azione da parte dell'interessato, ma deve essere adempiuto proattivamente dal titolare del trattamento.** Come devono essere queste informazioni? A questo proposito, come già detto, qualsiasi informazione deve essere *concisa, trasparente, intelligibile e facilmente accessibile, utilizzando un linguaggio chiaro e semplice, in particolare per qualsiasi informazione rivolta specificamente a un bambino. Le informazioni devono essere fornite per iscritto o con altri mezzi, anche elettronici,*

eventualmente, e possono anche essere fornite oralmente su richiesta dell'interessato e se la sua identità è provata al di là di ogni dubbio. Le informazioni devono essere fornite senza ritardi o spese eccessive (articolo 12 del GDPR).

Le informazioni devono essere fornite in **modo efficiente e breve**, in modo che la persona interessata non sia sommersa da esse e possa prevedere la portata e le conseguenze del trattamento.[156] Per raggiungere tali obiettivi, è necessario considerare alcuni aspetti. In primo luogo, l'informazione dovrebbe essere **fatta su misura per "il membro medio del pubblico previsto"**[157], che nel caso di una ricerca sarebbe il partecipante medio. In caso di dubbio su come sia l'individuo medio, le autorità per la protezione dei dati o altre parti interessate *(per esempio,* gruppi di difesa) potrebbero fornire un feedback. In alternativa, le bozze dei testi informativi possono essere convalidate prima di testare i soggetti prima del lancio di un progetto di ricerca e delle attività di raccolta dati[158].

In secondo luogo, poiché non è richiesto alcuno sforzo attivo da parte dell'**interessato**, le informazioni dovrebbero essere **immediatamente disponibili per l'interessato.** Il titolare del trattamento può quindi fornirle come meglio si adatta al contesto: direttamente, attraverso un link o una segnalazione o come risposta a una domanda in linguaggio naturale.

In terzo luogo, il **linguaggio usato dal titolare del trattamento dovrebbe essere il più semplice possibile**. A tal fine, la pubblicazione della Commissione UE Claire's Clear Writing Tips e How to Write Clearly[159] potrebbe fornire strumenti per semplificare il messaggio da trasmettere. Tra le cose da evitare nella stesura di qualsiasi nota informativa ci sono:

- frasi complesse,
- le forme passive,
- qualsiasi gergo tecnico,
- verbi modali e
- nozioni astratte che potrebbero portare a interpretazioni divergenti.

I bambini e altri gruppi vulnerabili richiedono un'ulteriore considerazione. Anche qui, molto è stato scritto per affrontare questa spinosa questione[160]. L'articolo 12 afferma che l'informazione dovuta alla persona interessata deve essere particolarmente adattata ai bambini (come esempio di gruppo vulnerabile) se le attività di trattamento dei dati sono rivolte a loro. La lingua è fondamentale quando si tratta di individui vulnerabili, come sottolinea l'autorità di vigilanza spagnola[161], poiché la vulnerabilità potrebbe essere esacerbata se l'individuo non ha le conoscenze per comprendere le informazioni.

---

156 *Ibidem*

157 Gruppo di lavoro sulla protezione dei dati dell' articolo 29 (a cura di), "Linee guida sulla trasparenza ai sensi del regolamento n. 2016/679", 2018, WP260 rev.01, p. 7

158 Ibidem.

159 Come suggerisce il titolo, entrambi i documenti forniscono al lettore alcuni consigli per scrivere più chiaramente. Sono disponibili presso: https://ec.europa.eu/info/sites/info/files/clear_writing_tips_en.pdf; https://op.europa.eu/en/publication-detail/-/publication/725b7eb0-d92e-11e5-8fea-01aa75ed71a1/language-en [ultimo accesso: 30.10.2020]

160 Vedi per esempio, I. Milkaite & E. Lievens, "Child-Friendly Transparency of Data Processing in the EU: From Legal Requirements to Platform Policies', *Journal of Children and Media*, 2020, Vol. 14, No. 1, pp. 5-21.

161 Agencia Española de Protección de Datos Personales, El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles, p. 2. At: https://www.aepd.es/sites/default/files/2019-11/nota-tecnica-apps-moviles.pdf (accessed Nov. 6, 2020)

In quarto luogo, per essere più accessibile, qualsiasi informazione scritta dovrebbe essere **fornita in un unico luogo o in un documento completo** (sia in formato digitale che cartaceo). Oltre al formato cartaceo, il titolare del trattamento può fare uso di altri mezzi elettronici e non elettronici che saranno trattati di seguito, come una dichiarazione di protezione dei dati a strati, avvisi pop-up, infografiche, diagrammi di flusso, video, avvisi vocali, animazioni e così via. Per contro, le informazioni potrebbero essere fornite anche oralmente, da persona a persona e attraverso mezzi automatizzati, a condizione che l'identità della persona interessata sia provata con altri mezzi.

Gli articoli 13 e 14 del GDPR specificano le informazioni da fornire, a seconda che i dati personali siano stati raccolti direttamente dalla persona interessata o meno.

Quando i **dati personali sono raccolti direttamente dall'interessato** (articolo 13, GDPR), il titolare del trattamento deve fornire al momento della raccolta le seguenti informazioni:

- L'identità e i dati di contatto del titolare del trattamento (cioè l'istituto di ricerca) e i contatti del suo responsabile della protezione dei dati (DPO);
- Gli scopi e la base giuridica del trattamento, incluso l'interesse legittimo, se applicabile;
- L'identità dei destinatari (o categorie di destinatari) dei dati personali, se presenti;
- Se i dati saranno trasferiti al di fuori dell'UE, così come i dettagli sulla base legale e le garanzie per il trattamento all'estero;
- Il periodo di conservazione dei dati. Se non è possibile stabilire tale periodo, devono essere stabiliti i criteri utilizzati per determinarlo;
- Tutti i diritti dell'interessato, compreso il diritto di presentare un reclamo a un'autorità di controllo. Inoltre, se il trattamento si basa sul consenso dell'interessato, deve essere incluso il diritto di ritirare il consenso;
- Se la fornitura di dati personali è prevista dalla legge o dal contratto e se la persona interessata deve fornire i dati personali, insieme alle potenziali conseguenze derivanti dalla mancata fornitura degli stessi;
- L'esistenza di un processo decisionale automatizzato; vale a dire, decisioni prese utilizzando dati personali trattati esclusivamente con mezzi automatici senza intervento umano.

Inoltre, nel suo documento sulla risposta alla richiesta della Commissione europea di chiarimenti sull'applicazione coerente del GDPR incentrato sulla ricerca sanitaria (2021), il Comitato europeo per la protezione dei dati raccomanda che *se un titolare del trattamento intende utilizzare i dati ottenuti dagli interessati anche per altri scopi, tale titolare dovrebbe, al momento della raccolta dei dati, adottare misure adeguate per essere in grado di soddisfare gli obblighi di informazione relativi a tale ulteriore trattamento*.[162]

L'articolo 13 del GDPR **esonera il titolare del trattamento** dal suo obbligo quando l'interessato ha già queste informazioni. Mentre il titolare del trattamento deve provare queste circostanze (relative, per esempio, a come e quando tali informazioni sono state fornite, così come in che misura non sono cambiate nel frattempo), c'è ancora un obbligo di completare potenzialmente la conoscenza dell'interessato.

162 Comitato europeo per la protezione dei dati, Documento sulla risposta alla richiesta della Commissione europea di chiarimenti sull'applicazione coerente del GDPR incentrata sulla ricerca sanitaria, adottato il 2 febbraio 2021, pag. 9, disponibile all'indirizzo: https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf [ultimo accesso: 28.06.2021]

Quando i **dati personali non sono raccolti direttamente dall'interessato** (articolo 14, GDPR), il titolare del trattamento deve anche **informare la persona sulla fonte dei dati personali e sulle categorie specifiche di dati che intende trattare.** Tutte le informazioni devono essere fornite *entro un periodo ragionevole [di tempo] dopo aver ottenuto i dati personali, ma al più tardi entro un mese, tenendo conto delle circostanze specifiche in cui i dati personali sono trattati.*

Infine, l'articolo 14.5(b) GDPR stabilisce tre **esenzioni per gli istituti di ricerca dall'obbligo del titolare del trattamento di informare gli interessati** sul trattamento dei dati personali che non sono stati raccolti da loro:

- tale disposizione *si rivela impossibile*
- *o comporterebbe uno sforzo sproporzionato*
- *[...] o nella misura in cui l'obbligo [...] possa rendere impossibile o compromettere gravemente il raggiungimento degli obiettivi di tale trattamento*.

Questo significa innanzitutto che i titolari del trattamento devono mostrare ciò che ha impedito loro di fornire le informazioni, considerando anche che, ogni volta che qualsiasi ostacolo è temporaneo, la fornitura di informazioni deve essere fatta il più presto possibile[163]. Per esempio, i ricercatori ottengono dati da un social network attraverso un'interfaccia di programmazione di applicazioni e, prima che possano conformarsi all'articolo 14 GDPR, il social network subisce un diniego di servizio che rende impossibile qualsiasi comunicazione con gli interessati.

Per quanto riguarda lo **sforzo sproporzionato**, il considerando 62 del GDPR si riferisce alla quantità di persone interessate, all'età dei dati e all'esistenza di misure di salvaguardia. Anche in questo caso, lo sforzo sproporzionato deve essere valutato e dimostrato, **bilanciando i costi e i benefici** in gioco. In ogni caso, il titolare del trattamento deve adottare misure adeguate per proteggere i diritti e le libertà e gli interessi legittimi degli interessati, compresa la messa a disposizione del pubblico delle informazioni. La disponibilità pubblica può derivare, ad esempio, dal caricamento delle informazioni su un sito web e/o dalla loro pubblicazione su un giornale. Altre misure appropriate vanno dall'esecuzione di una valutazione d'impatto, alla pseudonimizzazione e anonimizzazione dei dati personali (si veda la sezione "Identificazione, pseudonimizzazione e anonimizzazione" della Parte II "Concetti principali" delle presenti Linee guida), l'adozione di misure organizzative e tecniche in grado di migliorare il livello di sicurezza e così via.

In definitiva, la **grave compromissione degli obiettivi di tale trattamento richiede la prova che la fornitura di informazioni sancite dall'articolo 14.1 GDPR annullerebbe tali obiettivi. Ad** esempio, una ricerca condotta su come l'interazione umana nei social network è influenzata durante uno scenario di blocco derivante da una pandemia globale può richiedere che i ricercatori eseguano la loro analisi nel modo più segreto possibile per non disturbare tali interazioni. In tali casi, il titolare del trattamento adotta misure adeguate per proteggere i diritti e le libertà dell'interessato e gli interessi legittimi, compresa la messa a disposizione del pubblico delle informazioni ai sensi dell'articolo 14.5 (b) GDPR.

Indipendentemente dalla fonte dei dati personali, i titolari del trattamento devono informare l'interessato della loro intenzione di trattare ulteriormente i dati personali per uno scopo diverso da quello per cui sono stati raccolti, prima di tale ulteriore trattamento. Nel complesso, il principio di limitazione delle finalità (vedi "Principio di limitazione delle

163 Gruppo di lavoro " Articolo 29 per la protezione dei dati", "Linee guida sulla trasparenza ai sensi del regolamento n. 2016/679", *op. cit.,* p. 29

finalità" nella Parte II sezione "Principi" delle presenti Linee guida) prevede che **i dati personali debbano essere trattati per finalità determinate, esplicite e legittime, in modo che qualsiasi ulteriore trattamento incompatibile con esse debba essere vietato**. Tuttavia, secondo l'articolo 5.1(b) GDPR, qualsiasi ulteriore trattamento per scopi di archiviazione nel pubblico interesse, scopi di ricerca scientifica o storica o per scopi statistici non deve essere considerato incompatibile con lo scopo originario. In ogni caso, l'obbligo del titolare del trattamento di informare l'interessato sull'ulteriore trattamento comporta il test di compatibilità (cfr. "Protezione dei dati e ricerca scientifica" all'interno della Parte II sezione "Principali concetti" delle presenti Linee guida) effettuato sulla base dell'articolo 6.4 GDPR, al fine di spiegare perché il trattamento per finalità aggiuntive è coerente con quelle originarie. Come sottolineato dal Gruppo di Lavoro Articolo 29 (2013), l'esecuzione del test di compatibilità è della massima importanza per garantire la trasparenza e la limitazione delle finalità. [164] Ma, quando ci si affida alla presunzione di compatibilità sancita dall'articolo 5, paragrafo 1, lettera b) del GDPR per l'ulteriore trattamento dei dati personali a fini di ricerca scientifica, occorre tenere conto che tale presunzione può essere utilizzata solo a condizione che il trattamento ulteriore rispetti garanzie adeguate come richiesto dall'articolo 89, paragrafo 1, del GDPR.[165]

Sulla base di tali disposizioni, gli istituti di ricerca possono adottare tutte le misure che ritengono appropriate per rispettare questo obbligo. Il GDPR, infatti, non prescrive alcuna forma su come devono essere fornite le informazioni. Generalmente, il diritto all'informazione viene soddisfatto adottando una politica di protezione dei dati, una dichiarazione sulla privacy o un avviso di trattamento equo; la loro efficacia, tuttavia, ha portato a un dibattito polarizzato tra gli studiosi e i responsabili politici[166]. Di conseguenza, sono stati sviluppati nuovi metodi che potrebbero essere utilizzati per fornire informazioni agli interessati in modo chiaro e accessibile, come ad esempio:

- Un **approccio stratificato**: piuttosto che mostrare tutte le informazioni richieste in un unico avviso e quindi rischiare di sopraffare la persona interessata, un primo avviso sulla privacy può collegarsi alle altre categorie di informazioni, in modo che il livello di dettagli aumenti progressivamente. In questo contesto, il primo livello dovrebbe includere l'identità del titolare del trattamento, lo scopo del trattamento e i diritti[167] dell'interessato, insieme alle potenziali conseguenze derivanti dal trattamento[168]. È importante sottolineare che l'approccio a strati può essere adottato sia nello scenario online che in quello offline. Per quanto riguarda quest'ultimo, il primo strato potrebbe essere fornito oralmente, mentre in seguito si potrebbe inviare una copia della politica

164 Per ulteriori dettagli sul test di compatibilità, si veda il Gruppo di lavoro articolo 29 sulla protezione dei dati (ed.), "Opinion 03/2013 on Purpose Limitation", 2013, p. 13 WP 203 00569/13/EN

165 Comitato europeo per la protezione dei dati, *op. cit.,* p. 6

166 M. Arcand, J. Nantel, M. Arles-Dufour & A. Vincent, 'The Impact of Reading a Web Site's Privacy Statement on Perceived Control over Privacy and Perceived Trust, *Online Information Review*, 2007, Vol. 31, No. 5, pp. 661-681; J. A. Obar & A. Oeldorf-Hirsch, 'The Clickwrap: A Political Economic Mechanism for Manufacturing Consent on Social Media', *Social Media + Society*, 2018, Vol. 4, No. 3, pp. 1-14; Y. Pan & G. M. Zinkhan, 'Exploring the Impact of Online Privacy Disclosures on Consumer Trust, *Journal of Retailing*, 2006, Vol. 82, No. 4, pp. 331-338; B. Custers, S. van der Hof & B. Schermer, 'Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies: Privacy Expectations of Social Media Users', *Policy & Internet*, 2014, Vol. 6, No. 3, pp. 268-295

167 Considerando 39, GDPR

168 Gruppo di lavoro " Articolo 29 per la protezione dei dati" (a cura di), "Linee guida sulla trasparenza ai sensi del regolamento n. 2016/679", *op. cit.* , p. 19

di protezione dei dati e/o condividere un link alla dichiarazione[169] sulla privacy online a strati

- Un **pannello di controllo della privacy**: questa interfaccia utente permette all'interessato di gestire manualmente le sue preferenze per il trattamento dei dati personali
- Icone, pop-up, codici QR e avvisi vocali che indicano l'esistenza di un particolare tipo di trattamento dei dati personali
- Fogli informativi, infografiche, diagrammi di flusso, informazioni incorporate nei contratti

Oltre alle Linee guida sulla trasparenza ai sensi del regolamento n. 2016/679 adottate dal gruppo di lavoro dell'articolo 29, diversi progetti di ricerca stanno esplorando come rendere le informazioni più accessibili agli interessati, come il GDPR by Legal Design Project[170] e il PROTECT ITN[171].

Infine, nel suo parere preliminare del 2020, il Garante europeo della protezione dei dati esamina l'intersezione tra inganno, consenso informato e diritto all'informazione. In generale, l'*inganno può includere il trattenere informazioni nelle istruzioni ai partecipanti alla ricerca, fornire solo informazioni limitate sullo scopo della ricerca o anche ingannare i partecipanti fornendo una "storia di copertura" dello studio per mascherare il vero argomento dello studio. In alcuni esperimenti di psicologia noti come ricerche coperte, i soggetti vengono ingannati su ciò che viene testato, e questo viene citato come un fattore chiave di successo perché la consapevolezza dell'esatta natura della ricerca altererebbe il comportamento delle persone. [...] Relazione dei partecipanti alla ricerca e consenso informato retrospettivo insieme all'approvazione etica specifica prima dell'inizio della ricerca sono tra le misure per garantire la conformità etica*. È tuttavia il caso che tali pratiche apparentemente si scontrano con il diritto all'informazione, ogni volta che i dati sono raccolti direttamente dalla persona interessata ai sensi dell'articolo 13 GDPR[172].

Lista di controllo per rispettare il diritto all'informazione

Cosa fornire:

- ❑ Se i dati personali sono stati forniti direttamente dall'interessato, fornire tutte le informazioni elencate nell'articolo 13.1 GDPR;
- ❑ Se i dati personali non sono stati forniti dall'interessato, fornire tutte le informazioni elencate nell'articolo 14.1 - 2 GDPR;
- ❑ Se le informazioni sono già state fornite completamente alla persona interessata, non c'è più bisogno di rispettare questo obbligo.

Quando fornire:

- ❑ Nel momento in cui le informazioni sono state raccolte dal soggetto interessato;
- ❑ Quando i dati non sono raccolti dal soggetto interessato:
  - ▫ entro un periodo ragionevole dopo aver ottenuto i dati personali, ma al più tardi entro un mese;

169 *Ibidem.,* p. 20

170 Per ulteriori informazioni: http://gdprbydesign.cirsfid.unibo.it/

171 Per ulteriori informazioni: https://protect-network.eu/research/

172 Garante europeo della protezione dei dati, "A Preliminary Opinion on Data Protection and Scientific Research", 2020 disponibile su: https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf [ultimo accesso: 30.10.2020]

- se i dati personali devono essere utilizzati per la comunicazione con la persona interessata, al più tardi al momento della prima comunicazione a tale persona;
- se è prevista una divulgazione a qualcun altro, al più tardi quando i dati personali vengono divulgati per la prima volta.

Come fornire:

- Concisamente;
- ❑ In modo trasparente;
- ❑ In modo intelligente;
- ❑ Facilmente accessibile;
- ❑ In un linguaggio chiaro e semplice.

Esenzioni:

- ❑ Quando la persona interessata dispone già di tutte le informazioni pertinenti;
- ❑ Se i dati personali non sono stati forniti dall'interessato:
  - Quando la fornitura di informazioni è impossibile o sproporzionata.

4.2 Diritto di accesso

Secondo l'articolo 15 del GDPR e in conformità con l'articolo 8.2 della Carta dei diritti fondamentali dell'Unione europea, ogni persona interessata ha il diritto di *ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che la riguardano e, in tal caso, l'accesso ai dati personali e alle* ***seguenti informazioni:***

- Lo scopo del trattamento;
- Le categorie di dati personali interessate;
- I destinatari o le categorie di destinatari a cui sono stati o saranno comunicati i dati personali;
- Il periodo di conservazione dei dati. Se non è possibile stabilire tale periodo, devono essere stabiliti i criteri utilizzati per determinarlo;
- Tutti i diritti dell'interessato, compreso il diritto di presentare un reclamo a un'autorità di controllo;
- L'origine dei dati personali, se non sono raccolti direttamente dall'interessato;
- L'esistenza di un processo decisionale automatizzato; vale a dire, decisioni prese utilizzando dati personali trattati esclusivamente con mezzi automatici senza intervento umano.
- L'esistenza di tutte le garanzie prese per trasferire eventualmente i dati personali fuori dall'UE.

Su richiesta degli interessati, il titolare del trattamento deve fornire loro una copia dei dati personali trattati, senza alcun costo. Per eventuali copie aggiuntive richieste dagli interessati, l'articolo 15.3 GDPR consente al titolare del trattamento di addebitare potenzialmente *un costo ragionevole basato sui costi amministrativi.* In questo scenario, il titolare del trattamento dovrebbe mettersi in contatto con gli interessati tempestivamente, al fine di renderli consapevoli del costo.

Gli interessati hanno solo diritto ai loro dati personali, a meno che queste informazioni non siano intrecciate con quelle di altre persone. Se i dati personali includono informazioni su

altre persone, la successiva divulgazione **dipenderà dal bilanciamento tra il diritto di accesso degli interessati e i diritti fondamentali del terzo ai** sensi dell'articolo 15.4 GDPR. Ad esempio, qualsiasi obbligo di segreto professionale, la natura dei dati personali e così via dovrebbero essere presi in considerazione quando si effettua la ricerca. In questo scenario, il titolare del trattamento potrebbe nascondere i dati che potrebbero influenzare negativamente gli altri, come l'oscuramento di informazioni selezionate[173].

Il GDPR non impedisce a una persona di agire potenzialmente per conto degli interessati, pur dimostrandolo, ad esempio, attraverso una procura[174]. In caso di dubbio, il titolare del trattamento può chiedere agli interessati di identificarsi. Come già detto, però, tale processo dovrebbe essere proporzionato. Inoltre, il titolare del trattamento può chiedere agli interessati di specificare la loro richiesta, offrendo ulteriori dettagli che contribuiranno a identificare le informazioni richieste. Tuttavia, la richiesta di ulteriori chiarimenti da parte del titolare del trattamento non influisce sul termine di un mese.

Il GDPR non stabilisce una **procedura per esercitare il diritto di accesso**. Di conseguenza, il titolare del trattamento potrebbe fornire un modulo specifico che gli interessati potrebbero facilmente compilare e presentare. L'istituzione di qualsiasi procedura, tuttavia, non consente al titolare del trattamento di non accettare richieste che sono state presentate attraverso altri mezzi.

Allo stesso modo, il GDPR non dice nulla su **come il titolare del trattamento dovrebbe fornire le informazioni agli interessati. In** generale, la fornitura di qualsiasi informazione dovrebbe essere fatta in un formato elettronico comunemente usato (ad esempio, e-mail in cui è allegato un file PDF), se la richiesta è stata fatta elettronicamente e gli interessati non hanno richiesto diversamente. Tuttavia, il considerando 63 del GDPR suggerisce al titolare del trattamento di fornire agli interessati un accesso remoto a un sistema auto-sicuro, in modo che essi siano in grado di accedere direttamente ai loro dati personali; per esempio, accedendo al database del titolare del trattamento attraverso una VPN.

Lista di controllo per soddisfare una richiesta di accesso:

L'esercizio del diritto di accesso è conforme al GDPR?

- Avete ricevuto una richiesta di accesso da una persona giuridica? Se sì, indicate che la richiesta non è stata presentata da una persona fisica e negate la richiesta;
- L'interessato si è identificato correttamente? In caso contrario, chiedete ulteriori informazioni per confermare l'identità;
- La richiesta può essere soddisfatta entro un mese? Se no, si prega di informare il motivo e quanto tempo ci vorrà per elaborare la richiesta (senza superare i limiti di tempo previsti dal GDPR, vedi sezione 6);
- La richiesta deve essere soddisfatta.

Come rispettare ulteriormente tutti gli obblighi del GDPR:

- ☐ Fornire tutte le informazioni elencate nell'articolo 15.1-2 GDPR;

173 P. Voigt & A. von dem Bussche, *Il regolamento generale sulla protezione dei dati dell'UE (GDPR). Una guida pratica,* Cham: Springer, 2017, p. 153

174 Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)*, 2019, p. 108, disponibile su: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ [ultimo accesso: 30.10.2020]

- ☐ Se l'informazione si intreccia con quella di altri individui, eseguite un test di bilanciamento per vedere se la divulgazione all'individuo che ha presentato la richiesta non influisce sui dati personali dell'altro individuo;
- ☐ Fornire all'interessato una copia dei dati personali trattati. Per qualsiasi copia aggiuntiva richiesta dalla persona interessata, il titolare del trattamento può addebitare una tassa ragionevole.

Le migliori pratiche:

- ☐ Fornire un modulo specifico che il soggetto dei dati possa facilmente compilare e presentare;
- ☐ Fornire tutte le informazioni in un formato elettronico di uso comune, a meno che l'interessato non richieda diversamente.

4.3 Diritto alla rettifica

Come stabilito dall'articolo 16 del GDPR, gli interessati hanno il diritto di far rettificare i loro dati personali. Tale diritto deriva dalla necessità di garantire l'accuratezza dei dati personali e, di conseguenza, un livello di protezione più elevato per gli interessati[175]. I **dati personali sono inesatti nella misura in cui sono errati, incompleti e/o fuorvianti**[176]. In altre parole, travisano la realtà. Di conseguenza, il diritto di rettifica riguarda solo i dati oggettivi e reali, compresa l'ortografia del nome del partecipante alla ricerca.

Quando si tratta di giudizi di valore che sono legati ai fatti (*ad esempio,* la valutazione personale di un partecipante alla ricerca basata sulle sue condizioni di vita), i **titolari del trattamento devono eseguire un test di bilanciamento** tra la loro libertà di espressione e il diritto degli interessati sotto esame. **Lo scopo del bilanciamento è quello di capire se una rettifica è ragionevole per il titolare del trattamento e necessaria per gli interessati.** Per esempio, quando il giudizio di valore si traduce in un'impressione errata degli interessati che può essere provata, l'interesse degli interessati prevarrà[177].

La **richiesta può essere fatta per iscritto o oralmente**. Per quanto riguarda la sua essenza, a volte sarà sufficiente che l'interessato chieda semplicemente la rettifica, come nel caso di un errore di ortografia. È tuttavia possibile che il titolare del trattamento richieda la prova dell'inesattezza, senza che ciò comporti un onere di prova irragionevole per la persona interessata e le impedisca quindi di esercitare il diritto in esame[178]. Inoltre, è importante sottolineare che qualsiasi aggiunta di informazioni deve essere necessaria per lo scopo o gli scopi del trattamento e lo sforzo del titolare del trattamento deve essere proporzionato alla situazione specifica del contesto[179]. Come una questione di buona pratica, **il titolare del trattamento dovrebbe limitare il trattamento dei dati, pur verificando l'accuratezza delle informazioni**[180].

175 Considerando 65, GDPR e articolo 5.1 (d) GDPR

176 Information Commissioner's Office (ed.), *op. cit.*, pp. 115-116

177 P. Voigt & A. von dem Bussche, *op. cit.*, p. 155

178 Agenzia dei diritti fondamentali (a cura di), *op. cit.*, p. 220

179 P. Voigt & A. von dem Bussche, *op. cit*., p. 156

180 Information Commissioner's Office (ed.), *op. cit.*, p. 115

Una persona interessata può esercitare il diritto di rettifica solo per i propri dati, dato che l'articolo 16 GDPR **non concede un diritto relativo alla rettifica dei dati personali di un terzo.** Ciò significa che la portata del diritto dell'interessato è limitata, ogni volta che i dati personali si riferiscono anche ad altri individui (ad esempio, la relazione con un'altra persona)[181].

Lista di controllo per conformarsi a una richiesta di rettifica: L'esercizio del diritto di rettifica è conforme al GDPR?

- Avete ricevuto una richiesta di rettifica da una persona giuridica? Se sì, indicare che la richiesta non è stata presentata da una persona fisica;
- L'interessato si è identificato correttamente? Se no, chiedete ulteriori informazioni per confermare l'identità;
- La richiesta può essere soddisfatta entro un mese? Se no, si prega di informare perché e quanto tempo ci vorrà per elaborare la richiesta?
- Avete bisogno di una prova di inesattezza o di informazioni aggiuntive per rettificare i dati? Se sì, chiedete ulteriori informazioni alla persona interessata. Ricordate di non porre un irragionevole onere della prova sulla persona interessata
- La richiesta deve essere soddisfatta.

Come rispettare ulteriormente tutti gli obblighi del GDPR:

- Comunicare i dati ad ogni destinatario a cui sono stati divulgati i dati personali, a meno che ciò non si riveli impossibile o comporti uno sforzo sproporzionato.

4.4 Diritto alla cancellazione ("Diritto all'oblio")

L'articolo 17 del GDPR garantisce all'interessato il diritto alla cancellazione dei suoi dati personali senza indebito ritardo. Questo diritto riflette il principio di minimizzazione dei dati (vedi "Principio di minimizzazione dei dati" nella parte II sezione "Principi" di queste Linee guida) e il principio di accuratezza (vedi "Principio di accuratezza" nella parte II sezione "Principi" di queste Linee guida), secondo il quale i dati personali devono essere limitati a quanto necessario per le finalità per cui tali dati sono trattati, così come devono essere accurati e aggiornati (articolo 5.1(c) e (d)).

Ai sensi dell'articolo 17.1 GDPR, il diritto alla cancellazione **si applica nei seguenti scenari:**

a) I dati personali non sono più necessari per gli scopi per i quali sono stati trattati;
b) L'interessato ritira il consenso su cui si basa il trattamento e non c'è un altro motivo legale applicabile;
c) La persona interessata si oppone al trattamento e non ci sono motivi legittimi prevalenti per il trattamento;
d) I dati personali sono stati trattati illegalmente;
e) I dati personali devono essere cancellati, al fine di rispettare un obbligo legale previsto dalla legge dell'UE o dello Stato membro a cui il titolare del trattamento è vincolato;

181 P. Voigt & A. von dem Bussche, *op. cit*., p. 155

f) I dati personali sono stati raccolti per quanto riguarda l'offerta di servizi della società dell'informazione ai bambini secondo l'articolo 8.1 GDPR.

Da un punto di vista pratico, il diritto alla cancellazione implica **rendere i dati inutilizzabili in qualsiasi modo,** che impedisca al titolare del trattamento e a qualsiasi altra parte di (ri)accedere e (ri)elaborare i dati[182]. Sia distruggendo il supporto fisico (ad esempio documenti cartacei) o cancellando i dati dai sistemi informatici. Il processo di cancellazione è riuscito, **nella misura in cui non è più possibile ripristinare i dati senza uno sforzo eccessivo**. Voigt e von dem Bussche, per esempio, considerano ragionevole[183] la possibilità teorica di ripristinare i dati attraverso un software specializzato.

Da un lato, ci sono **standard internazionali** specificamente creati per dichiarare come le informazioni su carta devono essere distrutte. In particolare, la carta deve essere distrutta da un trituratore appropriato. Un esempio di standard su questo argomento è lo standard[184] DIN 66399, che offre una guida sull'adeguatezza dei distruggidocumenti e la loro configurazione. La distruzione delle informazioni può essere eseguita internamente dal titolare del trattamento o da una società esterna**. Se esternalizzata, la società esterna deve essere considerata un responsabile del trattamento dei dati** in quanto l'articolo 4.2 GDPR considera anche la "cancellazione o la distruzione" come un'operazione di trattamento. Secondo l'articolo 28.3 GDPR, il titolare del trattamento deve scrivere un **contratto** che imponga tutti gli obblighi necessari al responsabile del trattamento per attuare garanzie adeguate (vedi articolo 28 GDPR per i dettagli).

D'altra parte, è il caso che la cancellazione dai sistemi live possa non avvenire immediatamente. Spostare i dati nel cestino del computer non è sufficiente. Per esempio, i dati potrebbero essere memorizzati in luoghi diversi, e anche in archivi di backup. In tali casi, agire su richiesta dell'interessato potrebbe essere più complicato e più lungo a causa dei meccanismi tecnici in vigore. Di conseguenza, il titolare del trattamento deve mettere i dati di back-up fuori uso (vale a dire, in modo che nessuno possa trattare i dati nel deposito di back-up per qualsiasi scopo), fino a quando il deposito viene aggiornato secondo il programma e i dati possono finalmente essere cancellati in modo permanente. Un esempio recente di norme applicabili a questo processo può essere trovato nella ISO 27701.

Inoltre, quando i dati personali sono pubblici e devono essere cancellati, **il titolare del trattamento deve prendere misure ragionevoli per informare gli altri titolari del trattamento che trattano gli stessi dati della richiesta del soggetto di cancellarli**. Tale ragionevolezza deriva dalle tecnologie disponibili e dai costi di attuazione, come spiegato nel considerando 66 GDPR. Analogamente, l'articolo 19 GDPR richiede che il titolare del trattamento comunichi la cancellazione a ciascun destinatario a cui sono stati comunicati i dati, a meno che ciò non si riveli impossibile o comporti uno sforzo sproporzionato (cfr. "Principio di accuratezza" nella Parte II, sezione "Principi", delle presenti Linee guida).

Una questione molto dibattuta riguarda l'onere della prova. Da un lato, secondo Voigt e von dem Bussche (2017), gli interessati devono dimostrare l'esistenza del loro diritto alla cancellazione; il titolare del trattamento sarà tuttavia obbligato a provare circostanze favorevoli per esso, come la produzione di una controprova per negare un trattamento illecito

182 P. Voigt & A. von dem Bussche, *op. cit*., p. 161

183 Ibidem, p. 161

184 Questo standard è stato sviluppato dal DIN, che è l'abbreviazione dell'Istituto Tedesco di Standardizzazione. Per ulteriori informazioni, vedere: https://din66399.de

ai sensi dell'articolo 17.1 (d) GDPR. Lo stesso vale anche per provare le eccezioni al diritto di cancellazione di cui all'articolo 17. 3 GDPR (vedi sotto)[185]. D'altra parte, l'Agenzia per i diritti fondamentali afferma che, su richiesta di cancellazione da parte dell'interessato, è solo responsabilità del titolare del trattamento indicare la liceità del trattamento.[186]

In questo contesto, infatti, l'articolo 17.3 GDPR prevede diverse **deroghe** al diritto alla cancellazione, tra cui quando il trattamento dei dati personali è necessario per:

- Esercitare il diritto alla libertà di espressione e di informazione;
- Adempimento di un obbligo legale che richiede il trattamento da parte della legge dell'UE o degli Stati membri a cui il titolare del trattamento è vincolato, o per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio dei poteri ufficiali conferiti al titolare del trattamento;
- Motivi di interesse pubblico nel settore della salute pubblica;
- Finalità di archiviazione nell'interesse pubblico, finalità di ricerca scientifica o storica o finalità statistiche;
- L'esercizio o la difesa di rivendicazioni legali.

Concentrandosi sulla limitazione posta al diritto alla cancellazione quando il suo esercizio renderebbe impossibile o pregiudicherebbe il raggiungimento degli scopi della ricerca, Ducato sottolinea che *tale limitazione [...] si giustifica alla luce delle specifiche esigenze del contesto di ricerca: la cancellazione di tutti o parte dei dati utilizzati per uno studio, anche quando tecnicamente possibile, rischierebbe di minare la validità scientifica della ricerca, impedendo la verifica dei suoi risultati e il processo*[187] *di peer-review*. La restrizione, riferisce l'autore, è quindi apparentemente limitata agli studi già conclusi, dato che il mancato avvio della ricerca e il successivo esercizio del diritto alla cancellazione non inciderebbe sugli obiettivi[188] della ricerca.

Lista di controllo per soddisfare una richiesta di cancellazione:

L'esercizio del diritto alla cancellazione è conforme al GDPR?

- Avete ricevuto una richiesta di cancellazione da una persona giuridica? Se sì, indicare che la richiesta non è stata presentata da una persona fisica;
- La persona si è identificata correttamente? Se no, chiedete ulteriori informazioni per confermare l'identità;
- La richiesta rientra in una delle ipotesi previste dall'articolo 17.1 GDPR? Se no, informare e spiegare all'interessato che la richiesta sarà negata;
- La richiesta soddisfa una delle esenzioni previste dall'articolo 17.3 GDPR? Se sì, informare e spiegare all'interessato che la richiesta sarà negata;
- La richiesta può essere soddisfatta entro un mese? Se no, si prega di informare il perché e quanto tempo ci vorrà per elaborare la richiesta.
- La richiesta deve essere soddisfatta.

Come rispettare ulteriormente tutti gli obblighi del GDPR:

☐ Rendere i dati inutilizzabili in modo da impedire a voi e a qualsiasi altra parte di

185 P. Voigt & A. von dem Bussche, *op. cit*., p. 159

186 Agenzia dei diritti fondamentali (a cura di), *op. cit.*, p. 223

187 R. Ducato, *op. cit.*, p. 6

188 Ibidem.

(ri)accedere e (ri)elaborare i dati;

- ☐ Comunicare la cancellazione ad ogni destinatario a cui sono stati divulgati i dati personali, a meno che ciò si riveli impossibile o comporti uno sforzo sproporzionato;

4.5 Diritto alla restrizione del trattamento

L'articolo 18 del GDPR permette all'interessato di limitare temporaneamente il trattamento dei suoi dati personali da parte del titolare del trattamento. Tale diritto sancisce una conciliazione di interessi tra l'interesse dell'interessato a una rettifica o cancellazione dei suoi dati e l'interesse del titolare del trattamento a continuare il trattamento[189] dei dati. Il GDPR **non definisce come la richiesta dovrebbe essere fatta: è comunque una questione di buona pratica che sia fatta in modo sufficientemente chiaro.**

Ai sensi dell'articolo 18.1 GDPR, la richiesta dell'interessato **può essere fatta, quando:**

a) L'esattezza dei dati personali è contestata (vedi sezione 6.3);
b) Il trattamento è illegale e l'interessato opta per la limitazione del trattamento, piuttosto che per la cancellazione dei dati personali;
c) I dati devono essere conservati per l'esercizio o la difesa di diritti legali;
d) Una decisione è pendente per il prevalere dei legittimi interessi del titolare del trattamento sugli interessi dell'interessato.

Come previsto dal considerando 67 del GDPR, i **metodi** con cui il titolare del trattamento può limitare il trattamento dei dati personali possono includere, ad esempio, lo spostamento temporaneo dei dati selezionati in un altro sistema di trattamento, rendendo i dati non disponibili agli utenti o la rimozione dei dati personali su base temporanea. Nel complesso, l'obiettivo è quello di impedire il trattamento dei dati, ad eccezione della conservazione (articolo 18.2 GDPR).

Mentre la restrizione è in corso, i dati personali possono ancora essere trattati:

- sulla base del consenso dell'interessato;
- per l'istituzione, l'esercizio o la difesa di rivendicazioni legali;
- per la protezione dei diritti di un'altra persona fisica o giuridica;
- per motivi di importante interesse pubblico dell'UE/di uno Stato membro dell'UE.

Sulla base dell'articolo 19 GDPR, il titolare del trattamento deve **comunicare** la limitazione del trattamento a ciascun destinatario a cui sono stati divulgati i dati personali, a meno che ciò si riveli impossibile o comporti uno sforzo sproporzionato. Lo **sforzo sproporzionato** dipende dalle circostanze specifiche e potrebbe coinvolgere, ad esempio, il vasto numero di destinatari e le successive notifiche, o la difficoltà di identificare il destinatario.

Infine, il titolare del trattamento **deve informare la persona interessata prima che la restrizione del trattamento sia revocata.** In effetti, la restrizione potrebbe essere temporanea, soprattutto quando l'interessato esercita i suoi diritti di rettifica e di opposizione.

Passando ora al trattamento dei dati a fini di archiviazione nel pubblico interesse, a fini di ricerca scientifica o storica o a fini statistici, l'articolo 89 GDPR e il considerando 156 GDPR

189 Ibidem, p. 164

consentono agli *Stati membri di prevedere, a condizioni specifiche e fatte salve le opportune garanzie per gli interessati, specifiche e deroghe per quanto riguarda il diritto [...] di opposizione*. A questo proposito, il Garante europeo della protezione dei dati (2020) riconosce che l'obiezione di un gran numero di persone a tutto o parte del progetto potrebbe influire negativamente sulla rappresentatività e l'affidabilità dei dati della ricerca. Secondo l'autorità UE, la portata di questa deroga dovrebbe quindi rimanere limitata ai casi in cui l'integrità della ricerca sarebbe compromessa dall'esercizio dei diritti degli interessati. [190]

Lista di controllo per conformarsi a una richiesta di restrizione di trattamento

L'esercizio del diritto alla limitazione del trattamento è conforme al GDPR?

- Avete ricevuto una richiesta di limitare il trattamento dei dati da una persona giuridica? Se sì, indicare che la richiesta non è stata presentata da una persona fisica;
- La persona si è identificata correttamente? In caso contrario, chiedete ulteriori informazioni per confermare l'identità;
- La richiesta rientra in una delle ipotesi previste dall'articolo 18.1 GDPR? In caso contrario, si prega di informare l'interessato che la richiesta sarà rifiutata;
- La richiesta può essere soddisfatta entro un mese? Se no, si prega di informare perché e quanto tempo ci vorrà per elaborare la richiesta?
- La richiesta deve essere soddisfatta.

Come rispettare ulteriormente tutti gli obblighi del GDPR:

- ☐ Ricordate che la restrizione non comprende la conservazione dei dati;
- ☐ Quando la restrizione è in corso, i dati personali possono ancora essere trattati nelle circostanze previste dall'articolo 18.2 GDPR;
- ☐ Comunicare la limitazione del trattamento a ciascun destinatario a cui sono stati comunicati i dati personali in conformità con l'articolo 19 GDPR, a meno che ciò si riveli impossibile o comporti uno sforzo sproporzionato.

4.6 Diritto alla portabilità dei dati

Sulla base dell'articolo 20 GDPR, l'interessato ha il *diritto di ricevere i dati personali che lo riguardano, che ha fornito a un titolare del trattamento, in un formato strutturato, di uso comune e leggibile a macchina e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento a cui sono stati forniti i dati personali.* In questo modo, gli interessati sono responsabilizzati, in quanto hanno un migliore controllo sui loro dati personali e quindi spostarli, copiarli o trasferirli come desiderato. Secondo l'articolo 20.1 GDPR il diritto alla portabilità dei dati, tuttavia, può essere esercitato solo **quando i dati personali sono trattati con mezzi automatizzati, per motivi di consenso o per l'esecuzione di un contratto.**

Come sottolineato nelle Linee guida sul diritto alla portabilità dei dati elaborate dal Gruppo di lavoro "Articolo 29" sulla protezione dei dati (2017), il diritto alla portabilità dei dati **non si**

190 GEPD, "Un parere preliminare sulla protezione dei dati e la ricerca scientifica", gennaio 2020, p. 21-22

limita alla possibilità di trasmettere i dati personali dell'interessato da un titolare del trattamento a un altro, ma comprende anche il diritto dell'interessato di ricevere un sottoinsieme dei dati personali trattati e conservarli per uso personale. Per dirla diversamente, la trasmissione dei dati a un altro titolare del trattamento non è un elemento costitutivo obbligatorio del diritto alla portabilità dei dati, dato che una delle sue specificità sta nel fatto che *offre un modo semplice per l'interessato di gestire e riutilizzare i dati personali*[191]. Tutto sommato, la portabilità dei dati riguarda i dati personali che riguardano la sola persona interessata, sia che siano forniti attivamente dalla persona interessata, sia che siano forniti in virtù dell'utilizzo del servizio del dispositivo. In quest'ultimo caso, il gruppo di lavoro dell'articolo 29 sulla protezione dei dati sottolinea che il titolare del trattamento non dovrebbe adottare un'interpretazione troppo restrittiva di ciò che conta come "dati personali riguardanti la persona interessata"[192].

Il diritto alla portabilità è soddisfatto nella misura in cui i titolari del trattamento trasmettono direttamente le informazioni richieste agli interessati o forniscono l'accesso a uno strumento automatizzato che consente loro di estrarre le informazioni richieste per conto proprio. Quest'ultimo metodo non implica che i titolari del trattamento debbano fornire un accesso più generale e di routine al proprio sistema; piuttosto, deve essere limitato all'estrazione delle informazioni in seguito alla richiestadi portabilità[193].

Il trasferimento dei dati personali da un titolare del trattamento a un altro dipende dalla sua fattibilità giuridica, tecnica e finanziaria. Tra i potenziali ostacoli, il Gruppo di lavoro per la protezione dei dati dell'articolo 29 identifica: *tasse richieste per la consegna dei dati, mancanza di interoperabilità o di accesso a un formato di dati o API o al formato fornito, eccessivo ritardo o complessità per recuperare l'intero set di dati, offuscamento deliberato del set di dati, o specifica e indebita o eccessiva standardizzazione settoriale o richiesta*[194] *di accreditamento*. A tal fine, il considerando 68 del GDPR prevede che il titolare del trattamento dovrebbe sviluppare formati interoperabili, vale a dire, la capacità del sistema di informazioni di scambiare dati e consentire la condivisione delle informazioni. Tuttavia, non vi è alcun obbligo per il titolare del trattamento di supportare questi formati, con la conseguenza che la trasmissione diretta può avvenire, nella misura in cui la comunicazione tra i due sistemi è possibile e sicura. Esempi di formati interoperabili sono: un server SFTP, una WebAPI protetta o un WebPortal.

Inoltre, i dati dovrebbero essere *in un formato strutturato, comunemente usato e leggibile dalla macchina.* Per capire questa caratteristica, l'Open Data Handbook pubblicato da Open Knowledge International può essere una fonte[195] utile. Nello specifico, i dati strutturati possono essere definiti come *dati in cui la relazione strutturale tra gli elementi è esplicita nel modo in cui i dati sono memorizzati su un disco del computer.* Questo significa che il software può estrarre elementi specifici dei dati. Un esempio di formato strutturato è un file di foglio elettronico, dove i dati sono organizzati in righe e colonne. I dati leggibili dalla macchina sono invece quei dati che possono essere letti ed elaborati automaticamente da un computer. I

191 Gruppo di lavoro articolo 29 sulla protezione dei dati (a cura di), "Linee guida sul diritto alla portabilità dei dati", 2017, WP 242 rev.01, pp. 4-5. All'indirizzo: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

192 Per un altro esempio vedi: *ibid*., p. 9

193 Information Commissioner's Office (ed.), *op. cit.* , p. 140

194 Gruppo di lavoro articolo 29 per la protezione dei dati (a cura di), "Linee guida sul diritto alla portabilità dei dati", *op. cit.,* p. 15

195 Il manuale è disponibile su: https://opendatahandbook.org/ [ultimo accesso: 30.10.2020]

dati leggibili dalla macchina possono essere resi direttamente disponibili alle applicazioni che richiedono quei dati sul web[196]. Questo avviene per mezzo di un'interfaccia di programmazione delle applicazioni ("API"). Infine, è importante sottolineare che, anche se il requisito "di uso comune" potrebbe essere soddisfatto utilizzando applicazioni software comuni, tali applicazioni devono anche soddisfare gli standard strutturati e leggibili a macchina per rispettare il diritto alla portabilità. In ogni caso, i formati aperti come CSV, XML, JSON e RDF sono un buon esempio di modi per rispondere a una richiesta di portabilità.

Considerando che la portabilità dei dati implica il trasferimento di dati personali, tale atto potrebbe diventare una potenziale fonte di **rischio** per i dati personali in quanto tali. Di conseguenza, il titolare del trattamento è tenuto a **prendere tutte le misure necessarie per garantire un trasferimento sicuro** al giusto destinatario. Questo obiettivo potrebbe essere raggiunto attraverso la crittografia dei dati, password monouso e così via.

Si nota anche che quando un titolare del trattamento risponde a una richiesta di portabilità dei dati, agisce su istruzioni dell'interessato e, di conseguenza, non è responsabile del rispetto del quadro di protezione dei dati da parte del destinatario. Inoltre, il titolare del trattamento che trasferisce i dati non è tenuto a verificare l'esattezza dei dati[197] personali; tuttavia, la **portabilità dei dati non comporta automaticamente la cancellazione dei dati personali dal sistema, né influisce sul periodo[198] di conservazione originale**.

Se la richiesta dell'interessato riguarda **informazioni su altre persone,** il titolare del trattamento deve considerare se ci sarà un effetto negativo sui loro diritti e libertà. Al contrario, se la richiesta di portabilità è fatta da più interessati, il titolare del trattamento deve assicurarsi che tutti siano d'accordo sulla richiesta[199].

Infine, bisogna sottolineare che non esiste un diritto di accesso ai dati dedotti, poiché questi NON sono forniti dagli interessati. Tuttavia, gli interessati possono ancora avvalersi del loro "diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che li riguardano e, in tal caso, l'accesso ai dati personali", nonché informazioni sull'"esistenza di un processo decisionale automatizzato, compresa la profilazione, di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica applicata, nonché sul significato e le conseguenze previste di tale

196 Il termine è definito nel considerando 21 della direttiva 2013/37/UE17 come (...) *un formato di file strutturato in modo che le applicazioni software possano facilmente identificare, riconoscere ed estrarre dati specifici, comprese singole dichiarazioni di fatti, e la loro struttura interna. I dati codificati in file strutturati in un formato leggibile a macchina sono dati leggibili a macchina. I formati leggibili dalla macchina possono essere aperti o proprietari; possono essere standard formali o meno. I documenti codificati in un formato di file che limita l'elaborazione automatica, perché i dati non possono, o non possono essere facilmente estratti da essi, non dovrebbero essere considerati in un formato leggibile a macchina. Gli Stati membri dovrebbero, eventualmente, incoraggiare l'uso di formati aperti e leggibili a macchina*.

197 Gruppo di lavoro articolo 29 per la protezione dei dati, "Linee guida sul diritto alla portabilità dei dati", *op. cit.* , p. 6

198 Ibidem. , p. 7

199 Information Commissioner's Office (ed.), *op. cit*., p. 139

trattamento per l'interessato", secondo l'articolo 15 del GDPR (che si riferisce al diritto di accesso)[200].

Passando al regno della ricerca, la portabilità dei dati potrebbe consentire lo sviluppo di "piattaforme sempre più centrate sull'utente per la gestione dei dati personali"[201], fornendo anche agli interessati un controllo effettivo sulle loro informazioni personali. In particolare, la portabilità dei dati potrebbe essere utile per la creazione di un'ampia rete di ricerca, la facilitazione dell'uso secondario, e la realizzazione della *citizen science* (vale a dire, che gli individui dovrebbero essere in grado di trasferire i loro dati da varie risorse alle istituzioni di ricerca)[202].

Lista di controllo per conformarsi a una richiesta di portabilità

L'esercizio del diritto alla portabilità dei dati è conforme al GDPR?

- ☐ Avete ricevuto una richiesta di portabilità dei dati da un individuo? In caso contrario, indicare che la richiesta non è stata presentata da un individuo e indicare che la richiesta dovrebbe essere fatta seguendo la legislazione pertinente;
- ☐ La richiesta di portabilità è fatta da diversi interessati? Se sì, assicuratevi che tutti siano d'accordo sulla richiesta;
- ☐ L'interessato si è identificato correttamente? In caso contrario, chiedete ulteriori informazioni per confermare l'identità;
- ☐ I dati sono trattati su una delle basi legali previste dall'articolo 20.1 GDPR? In caso contrario, si prega di informare l'interessato che la sua richiesta sarà respinta;
- ☐ Il trattamento dei dati è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio dei pubblici poteri di cui è investito il titolare del trattamento? In caso affermativo, informare l'interessato che la sua richiesta sarà respinta;
- ☐ La richiesta può essere soddisfatta entro un mese? Se no, si prega di informare perché e quanto tempo ci vorrà per elaborare la richiesta?
- ☐ La richiesta deve essere soddisfatta.

Come rispettare ulteriormente tutti gli obblighi del GDPR:

- ☐ Se le informazioni si intrecciano con quelle di altri individui, fate un test di bilanciamento;
- ☐ Trasmettere dati in formati strutturati, comunemente usati e leggibili dalla macchina;
- ☐ Trasmettere dati in modo sicuro.

200 Gruppo di lavoro articolo 29 per la protezione dei dati (a cura di), "Linee guida sul diritto alla portabilità dei dati", *op. cit.,* pag. 15.

201 P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, I. Sanchez, "Il diritto alla portabilità dei dati nel GDPR: Towards User-Centric Interoperability of Digital Services", Computer Law and Security Review, Vol. 34, No. 2, 2018, p. 203.

202 P. Quinn P., "Is the GDPR and its Right to Data Portability a Major Enabler of Citizen Science? ", Global Jurist, giugno 2018, pp. 8-9

4.7 Diritto di opposizione

L'articolo 21 GDPR attribuisce all'interessato *il diritto di opporsi, per motivi legati alla sua situazione particolare, in qualsiasi momento al trattamento dei dati personali che lo riguardano*. Il blocco dei cookie su una pagina web, per esempio, è un esempio di obiezione.

Questa disposizione e il suo riferimento alla situazione particolare dell'interessato mirano a bilanciare i suoi diritti con quelli legittimi di altri nel trattamento dei loro dati. Ciò è esemplificato dall'interesse professionale dell'interessato alla riservatezza. È importante sottolineare che il diritto di opposizione è **applicabile quando la base giuridica del trattamento è l'esecuzione da parte del titolare del trattamento di un compito di interesse pubblico, o quando il trattamento è basato su interessi legittimi del titolare del trattamento.** In ogni caso, l'**onere della prova spetta al titolare del trattamento**, che deve dimostrare motivi convincenti per continuare il trattamento.

L'obiezione accolta, infatti, porta all'impossibilità di trattare i dati in questione, mentre, secondo l'Agenzia dei diritti fondamentali (2018) i trattamenti effettuati prima dell'obiezione rimangono legittimi[203]. Voigt e von dem Bussche, invece, sostengono che non è chiaro se l'obiezione accolta comporti la cancellazione obbligatoria dei dati[204]. In ogni caso, un'obiezione accolta consente all'interessato di esercitare il diritto alla cancellazione ai sensi dell'articolo 17.1(c) GDPR.

Al più tardi al momento della prima comunicazione con la persona interessata, il diritto di opposizione deve essere esplicitamente portato all'attenzione della persona interessata e presentato chiaramente e separatamente da qualsiasi altra informazione.

Tuttavia, l'articolo 21.6 GDPR impedisce all'interessato di opporsi al trattamento dei dati, a condizione che quest'ultimo sia effettuato a fini di ricerca scientifica o storica e a fini statistici e sia necessario per l'esecuzione di un compito di interesse pubblico. L'onere della prova della necessità ricade sul titolare del trattamento, il quale, tuttavia, non deve dimostrare l'esistenza di motivi legittimi cogenti, come nel caso del primo paragrafo dell'articolo 21 GDPR.[205] A questo proposito, è importante ricordare che, secondo l'EDPB (2020), la portata di questa deroga dovrebbe essere limitata ai casi in cui l'integrità della ricerca sarebbe compromessa dall'esercizio dei diritti dell'interessato.[206] Infatti, l'obiezione a tutta o parte di una ricerca scientifica da parte di diversi interessati può influenzare negativamente la rappresentatività e l'affidabilità dei dati della ricerca.

Anche se non collegato agli scopi di ricerca, il GDPR fornisce altre due sfumature relative al diritto di opposizione. In primo luogo, l'articolo 21.2 del GDPR include anche un diritto specifico di opposizione relativo all'uso dei dati personali per il **marketing diretto**. Questo diritto può essere esercitato in qualsiasi momento e gratuitamente e l'interessato deve essere informato della sua esistenza in modo chiaro, separato da qualsiasi altra informazione.

---

203 Agenzia dei diritti fondamentali (a cura di), *op. cit.*, p. 231

204 P. Voigt & von dem Bussche, *op. cit.,* p. 179

205 G. Zanfir-Fortuna, "Articolo 21. Right to Object', in C. Kuner, L. A. Bygrave & C. Docksey (eds.), *The EU General Data Protection Regulation (GDPR) A Commentary*, Oxford: Oxford University Press, 2020, p. 519

206 EDPB, *op. cit.,* pp. 21-22

In secondo luogo, l'articolo 21.5 del GDPR disciplina il diritto di opposizione, quando il trattamento è effettuato dai servizi della società dell'informazione attraverso **mezzi automatizzati.** In questo contesto, che è particolarmente rilevante in termini di ricerca ICT, il titolare del trattamento deve sviluppare modalità e procedure tecniche adeguate per garantire che il diritto di opposizione possa essere esercitato in modo efficace, come nel caso del blocco dei cookie sulla pagina web e la disattivazione del tracciamento della navigazione in internet.

Lista di controllo per conformarsi a una richiesta di obiezione

L'esercizio del diritto di opposizione è conforme al GDPR?

- Ha ricevuto una richiesta di obiezione da una persona giuridica? Se no, indicare che la richiesta non è stata presentata da una persona fisica.
- La richiesta rientra in una delle eccezioni di cui all'articolo 21.2-6 GDPR? In caso affermativo, informare l'interessato che la richiesta sarà rifiutata.
- L'interessato si è identificato correttamente? In caso contrario, chiedete ulteriori informazioni per confermare l'identità.
- \
- La richiesta può essere soddisfatta entro un mese? Se no, si prega di informare il perché e quanto tempo ci vorrà per elaborare la richiesta.
- La richiesta deve essere soddisfatta.

Come rispettare ulteriormente tutti gli obblighi del GDPR:

- ☐ Verificare la situazione particolare dell'interessato per bilanciare i suoi diritti con quelli legittimi di altri nel trattamento dei suoi dati.

4.8 Diritto a non essere soggetti a un processo decisionale automatizzato

Ai sensi dell'articolo 22 GDPR, l'*interessato ha il diritto di non essere sottoposto a una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo in modo significativo*. Come spiegato da Bygrave (2021), la ratio di questa disposizione risiede nelle ripercussioni potenzialmente gravi che la profilazione e altri trattamenti automatizzati potrebbero avere sul processo decisionale dell'interessato.[207] I ricercatori, ad esempio, potrebbero sviluppare un software per elaborare una grande quantità di dati personali, classificare gli interessati in base ad essi, fare previsioni e determinare risultati che potrebbero causare una discriminazione dei dati, quando successivamente applicati nel contesto della pubblica amministrazione (ad *esempio*, fornitura di servizi di welfare e sanitari) o del settore privato (ad *esempio*, pubblicità mirata ed e-recruitment)

Una questione molto dibattuta è la natura dell'articolo 22 GDPR. Il gruppo di lavoro dell'articolo 29, da un lato, interpreta questa disposizione come un divieto generale e giustifica per lo più la sua lettura sulla base del considerando 71, che rende chiaro che il

207 L. A. Bygrave, "Articolo 22. Automated individual decision-making, including profiling, in C. Kuner, L. A. Bygrave & C. Docksey *The EU General Data Protection Regulation (GDPR) A Commentary*, Oxford: Oxford University Press, 2020, p. 526

trattamento ai sensi dell'articolo 22 GDPR non è consentito in generale.[208] Dall'altro lato, Bygrave e altri autori sostengono che questa interpretazione va contro la formulazione effettiva dell'articolo 22 GDPR, così come la sua collocazione nella struttura del regolamento (vale a dire, il capo III sui diritti dell'interessato) e la sua speciale considerazione negli articoli 13. 2(f), 14.2(g), 15.1(h), e 35.3(a).[209] Mentre l'interpretazione dell'articolo 22 GDPR come divieto impone al titolare del trattamento di applicarlo indipendentemente dall'azione dell'interessato a tal fine, la sua interpretazione come diritto comporta il suo esercizio seguendo i suddetti requisiti sanciti dall'articolo 12 GDPR che saranno anche menzionati di seguito.

Il **processo decisionale automatizzato** è la capacità di prendere decisioni con mezzi tecnologici senza il coinvolgimento umano. Le decisioni automatizzate possono essere basate su qualsiasi tipo di dati, per esempio, dati forniti direttamente dagli individui interessati (come le risposte a un questionario); dati osservati sugli individui (come i dati di localizzazione raccolti tramite un'applicazione); dati derivati o dedotti come un profilo dell'individuo che è già stato creato (per esempio un punteggio di credito)[210].

La profilazione è qualsiasi forma di trattamento automatizzato di dati personali che consiste nell'uso di dati personali per valutare alcuni aspetti personali relativi a una persona fisica, in particolare, per analizzare o prevedere aspetti riguardanti il rendimento sul lavoro, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o i movimenti di tale persona fisica (vedi articolo 4 GDPR).

Anche se il GDPR **non definisce gli "effetti legali" e "simili"** derivanti dal processo decisionale automatizzato, il Gruppo di lavoro dell'articolo 29 chiarisce che *un effetto legale richiede che la decisione, che è basata esclusivamente sul trattamento automatizzato, influenzi i diritti legali di qualcuno, come la libertà di associarsi con altri, votare alle elezioni o intraprendere un'azione legale. Un effetto legale può anche essere qualcosa che colpisce lo stato giuridico di una persona o i suoi diritti in un contratto*[211]. Esempi di effetti giuridici comprendono la risoluzione di un contratto, la negazione di un beneficio sociale concesso dalla legge, la negazione della cittadinanza o del permesso di soggiorno. Per quanto riguarda gli effetti simili, il gruppo di lavoro dell'articolo 29 li considera come la conseguenza di *decisioni che devono avere il potenziale per influenzare significativamente le circostanze, i comportamenti o le scelte della persona interessata: avere un impatto prolungato o permanente sulla persona interessata o; portare all'esclusione o alla discriminazione della persona*[212]. Questo è evidente in una pratica di e-recruitment che favorisce gli uomini bianchi rispetto alle donne o alle persone appartenenti a gruppi minoritari o vulnerabili.

Ai sensi dell'articolo 22.4 GDPR, quando si tratta di categorie speciali di dati personali, il processo decisionale automatizzato può avvenire, a **condizione che l'interessato vi abbia acconsentito esplicitamente o se è necessario per motivi di interesse pubblico sostanziale** previsti dal diritto dell'UE o degli Stati membri dell'UE. In questo contesto, il responsabile del

208 Gruppo di lavoro articolo 29 sulla protezione dei dati, "Linee guida sul processo decisionale individuale automatizzato e sulla profilazione ai fini del regolamento 2016/679", 2018, WP251rev.01, pp. 19-20

209 L. A. Bygrave, *op. cit.,* pp. 531-532

210 Gruppo di lavoro " Articolo 29 per la protezione dei dati", "Linee guida sul processo decisionale individuale automatizzato e sulla profilazione ai fini del regolamento 2016/679", *op. cit.*, p. 8

211 Gruppo di lavoro articolo 29 per la protezione dei dati, "Linee guida sul processo decisionale individuale automatizzato e sulla profilazione ai fini del regolamento n. 2016/679", *op. cit.,* pag. 21

212 Ibidem.

trattamento deve adottare tutte le misure appropriate per salvaguardare i diritti e le libertà dell'interessato.

Come già accennato, l'articolo 12 GDPR prevede l'obbligo del titolare del trattamento di informare l'interessato sull'esistenza del processo decisionale automatizzato. Inoltre, l'informazione non dovrebbe limitarsi al fatto che tale processo decisionale si verifica, ma dovrebbe anche spiegare **la logica coinvolta e le potenziali conseguenze** per l'interessato[213].

L'articolo 22.2 GDPR prevede tre eccezioni al divieto del processo decisionale automatizzato, vale a dire:

- La decisione è necessaria per stipulare o eseguire un contratto tra l'interessato e un titolare del trattamento;
- La decisione è autorizzata dal diritto dell'UE o degli Stati membri dell'UE a cui è soggetto il titolare del trattamento;
- La decisione si basa sul consenso esplicito della persona interessata.

Nei casi in cui si applica una di queste eccezioni, il titolare del trattamento dovrà attuare garanzie specifiche diverse da quelle generalmente previste dall'articolo 12 GDPR. Sulla base dell'articolo 22.3 GDPR, nei casi di deroghe per il contratto e il consenso, l'interessato avrà ancora il diritto di chiedere il riesame umano della decisione completamente automatizzata, oltre alle garanzie generali che il titolare del trattamento dovrebbe attuare per proteggere i suoi diritti e libertà fondamentali, nonché gli interessi legittimi. Inoltre, al fine di garantire un trattamento dei dati equo e trasparente, il considerando 71 richiede che il titolare del trattamento dei dati *utilizzi procedure matematiche o statistiche appropriate per la profilazione, attui misure tecniche e organizzative adeguate per garantire, in particolare, che i fattori che determinano inesattezze nei dati personali siano corretti e che il rischio di errori sia ridotto al minimo, proteggere i dati personali in un modo che tenga conto dei potenziali rischi per gli interessi e i diritti della persona interessata ed evitare, tra l'altro, effetti discriminatori nei confronti delle persone fisiche sulla base dell'origine razziale o etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello stato genetico o di salute o dell'orientamento sessuale, oppure trattamenti che comportino misure aventi tale effetto.* Per questi scopi, l'attuazione del principio della protezione dei dati per progettazione e per impostazione predefinita sono della massima importanza. Inoltre, il considerando 91 chiarisce che una valutazione d'impatto sulla protezione dei dati dovrebbe essere fatta nel contesto dei processi decisionali automatizzati, ogni volta che il trattamento dei dati si traduce in *decisioni riguardanti specifiche persone fisiche a seguito di qualsiasi valutazione sistematica e approfondita di aspetti personali relativi a persone fisiche basata sulla profilazione di tali dati o a seguito del trattamento di categorie speciali di dati personali, dati biometrici, o dati su condanne penali e reati o misure di sicurezza correlate*. La disposizione continua dicendo che *[una] valutazione d'impatto sulla protezione dei dati è ugualmente richiesta per il monitoraggio su larga scala di aree accessibili al pubblico, in particolare quando si utilizzano dispositivi ottici elettronici o per qualsiasi altra operazione in cui l'autorità di controllo competente ritiene che il trattamento possa comportare un rischio elevato per i diritti e le libertà degli interessati, in particolare perché impedisce agli interessati di esercitare un diritto o di utilizzare un servizio o un contratto, o perché è effettuato sistematicamente su larga scala.*

213 Agenzia dei diritti fondamentali (a cura di), *op. cit.,* p. 234

Lista di controllo per conformarsi a una richiesta di non essere soggetti a un processo decisionale automatizzato

Come rispettare tutti gli obblighi del GDPR:

- ☐ Il processo decisionale automatizzato rientra in una delle deroghe previste dagli articoli 22.2 e 22.4? Se sì, potete procedere al trattamento dei dati;
- ☐ Informare la persona interessata dell'esistenza del processo decisionale automatizzato, includendo anche una spiegazione della logica coinvolta e le potenziali conseguenze per la persona interessata.

4.9 Restrizioni ai diritti degli interessati

Ai sensi dell'articolo 23 del GDPR, il diritto dell'UE o degli Stati membri può limitare la portata di alcuni diritti degli interessati al fine di salvaguardare alcuni obiettivi, in particolare:

a) Sicurezza nazionale
b) Difesa
c) Sicurezza pubblica
d) La prevenzione, l'investigazione, l'individuazione o il perseguimento di reati o l'esecuzione di sanzioni penali
e) Altri importanti obiettivi di interesse pubblico generale dell'UE o di uno Stato membro
f) La protezione dell'indipendenza giudiziaria e dei procedimenti
g) La prevenzione, l'investigazione, l'individuazione e il perseguimento delle violazioni dell'etica per le professioni regolamentate
h) Una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio dei poteri pubblici nei casi summenzionati (eccetto la protezione dell'indipendenza e dei procedimenti giudiziari)
i) La protezione della persona interessata o i diritti e le libertà di altri
j) L'esecuzione dei crediti di diritto civile

Affinché qualsiasi restrizione sia legittima, l'articolo 23(1) GDPR chiarisce che deve essere prevista da un provvedimento legislativo, riguardare i soli diritti dell'interessato e i corrispondenti obblighi sanciti dagli articoli 5, 12-22, e 34 GDPR, rispettare l'essenza dei diritti e delle libertà fondamentali, ed essere una misura necessaria e proporzionata in una società democratica.

Come spiegato dal GEPD, la condizione di rispettare l'essenza dei diritti e delle libertà fondamentali significa che le restrizioni non possono essere così estese e intrusive da privare tali diritti e libertà del loro contenuto fondamentale.[214] Per quanto riguarda i requisiti di necessità e proporzionalità, sottolinea il GEPD, il primo è soddisfatto nella misura in cui l'obiettivo di interesse generale è sufficientemente identificato in dettaglio. In questo modo sarà possibile valutare se la misura restrittiva è necessaria. Per quanto riguarda il carattere

214 Comitato europeo per la protezione dei dati, Linee guida 10/2020 sulle restrizioni ai sensi dell'articolo 23 GDPR, adottate il 15 dicembre 2020, p. 10, disponibile all'indirizzo: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-102020-restrictions-under-article-23_en [ultimo accesso: 15.09.2021]

proporzionale, ciò significa che la misura legislativa deve essere adeguata al raggiungimento degli obiettivi legittimi.[215]

In seguito, l'articolo 23(2) GDPR prevede che le misure legislative che limitano i diritti dell'interessato e gli obblighi del titolare del trattamento devono includere, eventualmente:

(a) Le finalità del trattamento o le categorie di trattamento
(b) Le categorie di dati personali
(c) La portata delle restrizioni introdotte
(d) Le salvaguardie per prevenire l'abuso o l'accesso o il trasferimento illegale
(e) La specificazione del titolare del trattamento o delle categorie di responsabili del trattamento
(f) I periodi di conservazione e le garanzie applicabili tenendo conto della natura, della portata e delle finalità del trattamento o delle categorie di trattamento
(g) I rischi per i diritti e le libertà degli interessati
(h) Il diritto delle persone interessate ad essere informate della restrizione, a meno che ciò possa pregiudicare lo scopo della restrizione

Nelle sue Linee guida, l'EDPB chiarisce anche che "il titolare del trattamento dovrebbe documentare l'applicazione delle restrizioni in casi concreti tenendo un registro della loro applicazione",[216] in conformità con il principio di responsabilità (vedi "Principio di accuratezza" nella Parte II sezione "Principi" di queste Linee guida). Questo registro dovrebbe contenere i motivi applicabili per le restrizioni, quali motivi tra quelli elencati nell'articolo 23(1) GDPR si applicano, la sua tempistica, nonché l'esito del test di necessità e proporzionalità.

4.10 **Osservazioni finali sui diritti dell'interessato**

Prima di concludere, è importante notare che questo documento ha solo fornito una breve panoramica dei diritti dell'interessato inclusi nel capo III del GDPR. Tuttavia, poiché questi diritti impongono contemporaneamente un obbligo reciproco per il titolare e il responsabile del trattamento, il capo IV del GDPR che regola gli obblighi del titolare e del responsabile del trattamento attribuisce anche ulteriori diritti all'interessato.

Più in generale, i diritti degli interessati si trovano in tutto il GDPR. I principi di base sanciti nel capo II, articoli 5-10, per esempio, forniscono anche una protezione aggiuntiva per la persona interessata. La ragione di questa salvaguardia diffusa risiede in una delle motivazioni del GDPR, cioè la necessità di garantire un livello coerente ed elevato di protezione delle persone fisiche nell'era digitale, dove il trattamento continuo e i flussi transfrontalieri di dati personali sono all'ordine del giorno.

Per completezza, il lettore deve quindi sapere che il GDPR include, *tra l'altro,* i seguenti diritti dell'interessato[217]:

- Il diritto di revocare il consenso (articolo 7.3 GDPR); l'interessato ha il diritto di revocare il suo consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basato sul consenso prima della sua revoca;

---

215 Ivi.
216 Ibidem, p. 14
217 Per ulteriori dettagli, si veda, ad esempio: Fundamental Rights Agency (ed.), *Handbook on European Data Protection Law,* Lussemburgo: Ufficio delle pubblicazioni dell'Unione europea, 2018, pp. 236-248

- Il diritto di presentare un reclamo a un'autorità di controllo (articolo 78 GDPR); in particolare, gli interessati possono presentare richieste e/o reclami all'autorità di controllo competente, se ritengono che il trattamento dei loro dati personali non sia stato effettuato in conformità con la legge;
- Il diritto a un ricorso giurisdizionale effettivo (articolo 79 GDPR); vale a dire, gli interessati possono presentare un reclamo davanti a un tribunale;
- Il diritto al risarcimento (articolo 82 GDPR); vale a dire, gli interessati possono chiedere il risarcimento di qualsiasi danno subito a causa del trattamento dei dati personali in violazione del GDPR.