

## Allegato A – Diritti degli interessati

### Diritto di accesso dell'interessato (art. 15 GDPR)

L'interessato ha il diritto di ottenere dal Titolare la conferma se sia o non sia in corso un trattamento di propri dati personali e in caso di trattamento in corso, ha diritto di ottenere l'accesso ai dati personali e alle seguenti informazioni:

- le finalità del trattamento;
- le categorie dei dati personali di cui il Titolare è in possesso;
- i destinatari cui i dati sono stati o saranno comunicati, specificando in particolare se si tratta di soggetti che si trovano in paesi terzi rispetto all'Unione Europea o se si tratta di organizzazioni internazionali. In particolare, qualora ricorra una di queste ultime ipotesi, l'interessato ha anche il diritto di essere informato sull'esistenza di adeguate garanzie concernenti il trasferimento dei suoi dati personali come precisato nel Capo V del GDPR, dedicato proprio ai trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali;
- se possibile, la durata prestabilita del periodo di conservazione dei dati o quanto meno i criteri cui il Titolare fa riferimento per determinare tale durata;
- l'esistenza del suo diritto:
  - ✓ a chiedere la rettifica o la cancellazione dei dati;
  - ✓ a chiedere la limitazione del trattamento dei dati personali;
  - ✓ di opporsi al loro trattamento, perché ritenuto illegittimo;
- il diritto di proporre un reclamo al Garante per la protezione dei dati personali quando ritiene che vi sia stata violazione dei propri diritti o delle proprie libertà;
- tutte le informazioni disponibili sull'origine dei dati nel caso in cui non siano stati raccolti presso l'interessato, ma ricevuti da soggetti terzi (ai quali l'interessato potrebbe aver dato il consenso anche a tal fine) oppure ottenuti tramite elenchi pubblici;
- infine, la logica su cui è basato un **processo automatizzato**, come ad esempio la profilazione, il funzionamento di tali meccanismi e le possibili conseguenze del loro utilizzo (ovvero in cosa consistono sostanzialmente, quali dati e come vengono elaborati).

Si tratta di un diritto assoluto, non soggetto a motivazione da parte dell'interessato né ad alcuna limitazione specifica, ad esclusione di quelle generali di cui all'art. 23 del GDPR.

Ove si tratti una notevole quantità d'informazioni riguardanti l'interessato, il Titolare dovrebbe poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, a quali dati o attività di trattamento la richiesta si riferisca.

Il diritto d'accesso può essere esercitato anche più volte e con una cadenza periodica, perché solo mediante un controllo costante l'interessato sarà davvero consapevole delle attività che riguardano i propri dati personali, sempre che le richieste non assumano un carattere vessatorio (pluralità di domande identiche, seriali o onerose da parte di uno stesso soggetto).

Il Titolare è tenuto ad adottare tutte le misure ritenute adeguate, prime tra tutte quelle atte a verificare l'identità di chi chiede l'accesso, con particolare attenzione ai casi in cui ciò avvenga direttamente online. Inoltre, l'esercizio del diritto in esame non dovrebbe pregiudicare i diritti e le libertà degli altri interessati. Il Considerando n. 63, al riguardo, fa riferimento ai segreti industriali e ai diritti di proprietà industriale (si pensi alla tutela dei diritti d'autore relativi a

software).

### Diritto di rettifica (art. 16 GDPR)

L'interessato ha diritto di rettifica in caso di necessità di **correggere, modificare** od **integrare** i dati poiché **errati, non aggiornati** o **insufficienti**. La correzione dei dati da parte del Titolare deve avvenire senza ingiustificato ritardo.

Per la propria natura, si ritiene che il diritto possa essere esercitato solo su dati elementari, ma non in riferimento ad informazioni di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tiposoggettivo.

È opportuno che anche per l'esercizio di questo diritto siano predisposti strumenti e sistemi in grado di facilitare l'accesso diretto dell'interessato alle informazioni che lo riguardano, così da permettergli di intervenire prontamente e, per quanto possibile, autonomamente per modificare i dati inesatti.

Nel caso in cui i dati personali oggetto di rettifica siano stati **comunicati** ad altri soggetti (o **pubblicati**), è onere del Titolare darne comunicazione e richiedere la rettifica a ciascuno dei destinatari, a meno che ciò sia impossibile o implichi uno sforzo sproporzionato (art. 19 del GDPR).

### Diritto alla cancellazione (c.d. "diritto all'oblio" - art. 17 GDPR)

L'interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo nei seguenti casi:

- a) i dati personali **non sono più necessari** rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- b) l'interessato **revoca il consenso** su cui si basa il trattamento (rilasciato a sensi dell'art. 6, par. 1, lett. a), o dell'art. 9, par. 2, lett. a), se non esiste nessun'altra base giuridica che lo legittimi (in questo caso particolare assume rilevanza l'acquisizione del consenso da un minore, considerato non pienamente consapevole dei rischi derivanti dal trattamento: vedasi art. 8, par. 1 e 2).
- c) l'interessato si **oppone al trattamento** e non sussiste alcun ulteriore motivo legittimo per procedere al trattamento, oppure si oppone al trattamento dei propri dati per finalità di marketing diretto (compresa la profilazione nella misura in cui sia connessa a tale marketing diretto); in questo caso quindi la cancellazione è diritto susseguente a quello di cui all'art. 21
- d) i dati personali sono stati trattati **illecitamente**;
- e) i dati personali **devono essere cancellati per adempiere un obbligo legale** previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento
- f) i dati personali sono stati raccolti relativamente **all'offerta di servizi della società dell'informazione ai minori**.

Il Titolare del trattamento nei casi indicati è obbligato a procedere alla cancellazione dei dati e – se li ha resi pubblici - ad adottare le misure ragionevoli per informare altri Titolari del trattamento che stanno trattando i dati (compreso "qualsiasi link, copia o riproduzione") di procedere alla loro cancellazione (art. 19 del GDPR).

Il diritto in argomento trova naturalmente alcune limitazioni che si fondano sulla base giuridica

a fondamento del trattamento e che legittimano quindi sia la conservazione dei dati che l'ulteriore trattamento; il Titolare può quindi rigettare la richiesta di cancellazione se il trattamento si basa:

- sull'esercizio del diritto alla libertà di espressione e di informazione;
- su un adempimento di un obbligo legale, per l'esecuzione di un compito di pubblico interesse oppure nell'esercizio di pubblici poteri;
- su motivi di interesse pubblico nel settore della sanità pubblica;
- su finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui la cancellazione rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
- sull'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

### Diritto di limitazione del trattamento (art. 18 GDPR)

Si tratta di una **sospensione** temporanea (ma che può anche diventare permanente) del trattamento in corso.

Il diritto è esercitabile ove ricorra almeno una delle seguenti ipotesi:

- 1) l'interessato ha contestato l'esattezza dei dati personali, in attesa della eventuale rettifica degli stessi;
- 2) il trattamento è illecito e l'interessato non richiama o si oppone alla cancellazione dei dati personali;
- 3) i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, mentre al Titolare del trattamento non servono più ai fini del trattamento;
- 4) l'interessato si è opposto al trattamento (ai sensi dell'art. 21 del GDPR) e si è in attesa delle verifiche necessarie per determinare se i motivi legittimi del Titolare del trattamento prevalgano su quelli dell'interessato.

I dati il cui trattamento sia sottoposto a limitazione **possono essere conservati ma non più trattati negli ambiti per cui sia stata accordata la limitazione, a meno che:**

- a) il Titolare non ottenga contestualmente uno specifico consenso per una o più finalità diverse da quelle per cui sia disposta la sospensione (ove il trattamento si basi sul consenso);
- b) il trattamento non sia:
  - ✓ finalizzato all'esercizio o difesa di un diritto in sede giudiziaria;
  - ✓ finalizzato alla tutela dei diritti di un'altra persona fisica o giuridica;
  - ✓ effettuato per motivi di interesse pubblico rilevante.

Nel caso in cui i dati personali oggetto di limitazione siano stati **comunicati** ad altri soggetti (o **pubblicati**) e sia accordata la limitazione, è onere del Titolare darne comunicazione a ciascuno dei destinatari, a meno che ciò sia impossibile o implichi uno sforzo sproporzionato (art. 19 del GDPR). In un secondo momento la limitazione può essere revocata (ad es., a seguito dell'avvenuta rettifica); prima che la revoca sia efficace però, il Titolare del trattamento deve avvisare l'interessato.

Il Considerando 67 illustra alcune modalità pratiche per attuare il diritto alla limitazione; questo potrebbe essere garantito ad es.:

- trasferendo temporaneamente i dati selezionati in un altro sistema di trattamento (così

- da nonrenderli disponibili per le normali attività di trattamento);
- rendendo i dati personali selezionati inaccessibili agli utenti (ove il trattamento sia così configurato);
- rimuovendo temporaneamente i dati pubblicati da un sito web.

Lo stesso considerando, poi, evidenzia che “negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe, in linea di massima, essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati (ove l’interessato non ne richieda la cancellazione). Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato”. In questo senso, **il dato personale soggetto a limitazione dovrebbe essere "contrassegnato"** in attesa di determinazioni ulteriori.

#### **Diritto alla portabilità dei dati (art. 20 GDPR)**

Il diritto alla portabilità consente all’interessato di ricevere i dati personali forniti a un Titolare, in un **formato strutturato, di uso comune** e **leggibile da dispositivo automatico**, e di trasmetterli a un altro Titolare.

Non si applica ai trattamenti **non automatizzati** (quindi ad es., ai dati detenuti in archivi o registri cartacei) ed è esercitabile solo nel caso in cui i dati:

- ✓ siano stati **forniti direttamente dall’interessato** (consapevolmente e in modo attivo);
- ✓ siano acquisiti e trattati sulla base del **consenso** dell’interessato o per **l’esecuzione di un contratto** di cui è parte l’interessato (artt. 6, par. 1, lett. a), o 9, par. 2, lett. a);
- ✓ siano **chiaramente riferibili all’interessato**; sono quindi ad esempio esclusi i dati relativi a terzepersone ovvero quelli anonimi; siano trattati attraverso **strumenti automatizzati**, ossia ad esclusione di qualsivoglia dato inferenziale o derivati, sia sulla base di un intervento umano nel trattamento medesimo sia che ciò derivi ad es., dall’applicazione di un algoritmo;

L’interessato può quindi richiedere:

- di **ricevere i dati personali** trattati e conservarli su un supporto personale in vista di un utilizzo ulteriore per scopi personali, senza trasmetterli necessariamente a un altro Titolare;
- di **trasmettere i dati personali** da un Titolare del trattamento a un altro Titolare del trattamento, se è tecnicamente fattibile.

Il Titolare del trattamento può consentire di esercitare il diritto o fornendo uno strumento per il download dei dati, o garantendo la trasmissione diretta dei dati ad altro Titolare (anche il titolare ricevente i dati è soggetto a specifici obblighi, in particolare diventa il nuovo Titolare e quindi deve garantire che i dati non siano eccessivi rispetto al servizio che fornisce).

L’esercizio del diritto alla portabilità non deve né ledere i diritti e le libertà altrui né pregiudicare nessuno degli altri diritti dell’interessato, che può, per esempio: continuare a fruire del servizio offertodal Titolare anche dopo un’operazione di portabilità; esercitare il diritto di cancellazione o di limitazione del trattamento.

**NB Tale diritto non si applica al trattamento necessario per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri di cui è investito il titolare del trattamento**

Si veda considerando n. 68 del Regolamento per maggiori dettagli.

## Diritto di opposizione (art. 21 GDPR)

Il diritto di opposizione è esercitabile ove il trattamento:

- a) si fondi sull'esecuzione di un compito di **interesse pubblico** o connesso all'esercizio di **pubblici poteri** (in ambito pubblico);
- b) sia posto in essere nell'esercizio di un **legittimo interesse** del Titolare del trattamento o di terzi (in ambito privato<sup>6</sup>);
- c) sia effettuato a fini di **ricerca scientifica o storica o a fini statistici** a norma dell'articolo 89, par.1 del GDPR, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

In questi casi, l'interessato può opporsi in qualsiasi momento, per motivi connessi alla **sua situazione particolare**, e quindi **motivando la sua richiesta**. Spetta dunque al Titolare l'onere di dimostrare che la base giuridica su cui si fonda il trattamento (compresa la necessità di accertamento, esercizio o difesa di un proprio diritto in sede giudiziaria) prevalgano sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato; ove accordi l'esercizio del diritto, il Titolare deve astenersi dal trattare ulteriormente i dati, anche se può comunque conservarli; in caso contrario, l'interessato deve comunque essere informato della possibilità di esercitare reclamo davanti al Garante per la protezione dei dati personali.

- d) è finalizzato ad **attività di marketing diretto** (compresa la profilazione connessa al marketing diretto).

In questo caso, l'interessato può opporsi in qualsiasi momento. Si tratta quindi di un **diritto assoluto**, poiché non soggetto a motivazione e ad alcuna valutazione da parte del Titolare. Anche in questo caso, se l'interessato esercita tale diritto, il Titolare deve esimersi dal procedere con il trattamento per finalità di marketing, potendo ben continuare eventuali diversi trattamenti che fondino il proprio presupposto su diverse basi (ad es., obbligazione contrattuale, l'interesse legittimo del titolare stesso, finalità che devono comunque essere rese esplicite all'interessato).

Nel contesto dell'**utilizzo di servizi della società dell'informazione**<sup>7</sup> e fatta salva la direttiva 2002/58/CE (relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche), l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

## Processo decisionale relativo alle persone fisiche, compresa la profilazione (art. 22 GDPR)

Il Regolamento definisce la **profilazione** all'art. 4, n. 4), come: *"qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi ad una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica"*.

Il WP 29 specifica che la profilazione è integrata allorché concorrano le seguenti **tre** caratteristiche:

- il trattamento sia svolto in forma automatizzata;
- esso abbia ad oggetto dati personali;
- il suo obiettivo sia quello di valutare aspetti personali di una persona fisica.

Mediante la profilazione, infatti, si raccolgono informazioni su un individuo (o gruppo di

individui), si analizzano le sue caratteristiche o modelli di comportamento e si inserisce il profilo individuale in una certa “categoria” o “segmento” per dar luogo ad ulteriori valutazioni o previsioni riguardanti, ad esempio, la sua capacità di eseguire un’attività, i suoi interessi o comportamento probabile.

Il **processo decisionale automatizzato** induce a prendere decisioni solo attraverso mezzi tecnologici, (ossia senza il coinvolgimento umano) e può basarsi su dati forniti direttamente dall’interessato (ad es. tramite *form* o un questionario), oppure su dati ricavati da programmi traccianti (ad es. la geolocalizzazione individuale fornita da un *app*) o dati derivanti da profili precedentemente creati (ad es. l’affidabilità finanziaria in ambito creditizio).

La decisione automatizzata e la profilazione a volte sono separate, altre volte no: infatti può succedere che una decisione automatizzata venga presa senza aver creato un profilo dell’individuo e, al contrario, una decisione automatizzata possa trasformarsi in profilazione a seconda del modo in cui i dati vengono utilizzati.

L’art. 22, par. 1, del GDPR, prevede che l’interessato abbia il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida con effetti analoghi. Per **decisione basata unicamente sul trattamento automatizzato** si deve intendere una decisione presa senza il coinvolgimento di un essere umano che possa influenzare ed eventualmente cambiare il risultato attraverso la sua autorità competenza.

Perché sia riconosciuto il diritto dell’interessato è necessario che tale decisione “*produca effetti giuridici o incida in modo analogo significativamente sulla sua persona*”. Il riferimento agli “**effetti giuridici**” riguarda l’impatto che una decisione automatizzata può produrre sulla sfera giuridica dell’individuo (ad es. penalizzando il diritto di associazione, di voto, di libertà negoziale, di libera circolazione, etc.) ovvero tutte le circostanze che “in modo analogo” possano potenzialmente e significativamente influenzare i comportamenti e le scelte degli individui interessati. Il Considerando 71 del GDPR cita, come esempi di decisioni automatizzate che possono incidere sui diritti e le libertà degli individui in maniera rilevante, il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani.

L’art. 22 al par. 2 prevede che *il diritto non si applichi*:

1. quando la decisione è necessaria per la **conclusione o l’esecuzione di un contratto** tra l’interessato e un Titolare del trattamento; in questo caso, la *necessità* di utilizzare decisioni automatizzate per l’esecuzione o conclusione di un contratto deve essere interpretata in modo restrittivo, ossia che il Titolare deve essere in grado di dimostrare che la profilazione è necessaria e non sono disponibili mezzi alternativi meno invasivi;
2. quando la decisione è **autorizzata dal diritto** dell’Unione o dello Stato membro cui è soggetto il Titolare del trattamento; specifiche disposizioni di diritto comunitario o interno possono quindi, in casi specifici, autorizzare il ricorso ad un processo di decisione automatizzata (ad es., per il monitoraggio e la prevenzione delle frodi e dell’evasione fiscale o per garantire la sicurezza e l’affidabilità di un servizio fornito dal Titolare).
3. quando la decisione si basa sul **consenso esplicito** dell’interessato; il consenso deve consistere in una dichiarazione espressa e non desunto da *facta concludentia*.

In ambito di decisioni basate unicamente su un trattamento automatizzato, il Regolamento UE 2016/679 introduce la necessità di fornire all’interessato maggiori informazioni sulle modalità

di creazione ed utilizzo di questi processi. Infatti, l'art. 13, par. 2, lett. f) e l'art. 15, par. 1, lett. h), stabiliscono il diritto dell'interessato di conoscere l'esistenza del processo decisionale automatizzato, in particolare, di ottenere informazioni significative sulla logica utilizzata (i criteri assunti per raggiungere la decisione, senza che con ciò si debba necessariamente fornire una spiegazione complessa degli algoritmi utilizzati) e sulle conseguenze previste di tale trattamento (attraverso esempi bisognerà fornire informazioni su come il processo automatizzato potrebbe influenzare in futuro la persona interessata).

Tenuto conto dei rischi rilevanti sui diritti e libertà dell'interessato per queste tipologie di trattamento, il Regolamento UE 2016/679, da un lato obbliga il Titolare ad attuare misure appropriate e "rafforzate" di tutela (importante sarà anche prevedere modalità che verificano con regolarità la correttezza dei processi per limitare errori di classificazione o valutazione con impatto negativo sui soggetti profilati), dall'altro lato, all'art. 22, par. 3 riconosce il potere all'interessato di ottenere l'*intervento umano* da parte del Titolare, di esprimere la propria opinione e di contestare la decisione, nei casi in cui tale decisione sia prevista per contratto o consentita dall'interessato. L'Intervento umano deve essere "effettivo" ossia poter intervenire sul procedimento con autonome valutazioni.

Infine, un processo decisionale automatizzato che coinvolga categorie particolari di dati, di cui all'art.9, par. 1, è consentito solo in presenza del consenso esplicito dell'interessato o per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri