

**PROTOCOLLO PER LA GESTIONE DELLE RICHIESTE RELATIVE
ALL’ESERCIZIO DEI DIRITTI DEGLI INTERESSATI
di cui agli artt. 15 ss. Reg. UE 2016/679**

INDICE

1. Premessa;
2. Diritto di accesso ai dati personali;
3. Diritto di rettifica dei dati personali;
4. Diritto alla cancellazione dei dati personali;
5. Diritto alla limitazione del trattamento dei dati personali;
6. Obbligo della notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento;
7. Diritto alla portabilità dei dati personali;
8. Diritto di opposizione al trattamento dei dati personali;
9. Diritto di non essere sottoposto ad una decisione automatizzata;
10. Altri diritti degli interessati;
11. Modalità di esercizio dei diritti degli interessati.
12. Definizioni;

Allegato A – “Modulo esercizio diritti degli interessati”

1. Premessa

Come è noto, il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati, "GDPR") ed il d. lgs. 196/2003 ("Codice Privacy"), come modificato dal d. lgs. 101/2018, sono fonti normative tese a garantire la protezione dei dati personali e la tutela dei diritti e delle libertà dei soggetti interessati dal trattamento dei dati personali.

Tra gli strumenti forniti direttamente agli interessati, il GDPR riconosce la possibilità di esercitare i seguenti diritti:

- a) diritto di accesso ai dati personali;
- b) diritto di rettifica dei dati personali;
- c) diritto alla cancellazione dei dati personali;
- d) diritto alla limitazione di trattamento dei dati personali;
- e) diritto alla portabilità dei dati personali;
- f) diritto di opposizione al trattamento dei dati personali;
- g) diritto di non essere sottoposto ad una decisione automatizzata;
- h) diritto di proporre reclamo ad una autorità di controllo, di proporre ricorso in sede giudiziale e diritto a che una violazione di dati personali sia notificata all'autorità di controllo e notificata agli interessati.

Oltre che dalla fonte normativa euro unitaria ed interna, gli interessati prendono contezza della sussistenza dei propri diritti mediante l'informativa sul trattamento loro resa dai titolari del trattamento ai sensi degli artt. 13 e 14 GDPR.

In sintesi, rispetto alla normativa antecedente al GDPR, il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), di 1 mese, estendibile fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

Ed è proprio al titolare che spetta valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (art. 12, par. 5 GDPR), ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti.

Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, par. 1 GDPR; si veda anche art. 15, par. 3 GDPR). La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

Rimane invariato, invece, l'onere del titolare del trattamento di agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea; benché sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti (artt. 15-22 GDPR), il responsabile del trattamento eventualmente nominato è tenuto a collaborare con il titolare del trattamento ai fini dell'esercizio dei diritti degli interessati (art. 28, par. 3, lett. e GDPR).

Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee (si vedano, in particolare, art. 11, par. 2 e art. 12, par. 6, GDPR).

Sono ammesse deroghe ai diritti riconosciuti dal GDPR, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'art. 23 GDPR nonché di altri articoli relativi ad ambiti specifici (si vedano, in particolare, art. 17, par. 3 GDPR, per quanto riguarda il diritto alla cancellazione, art. 83 GDPR - trattamenti di natura giornalistica e art. 89 GDPR - trattamenti per finalità di ricerca scientifica o storica o di statistica).

Tutto ciò premesso, il presente protocollo è stato redatto al fine di consentire al titolare del trattamento di implementare le misure tecniche e organizzative eventualmente necessarie a favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati dal trattamento dei dati personali realizzato.

Nondimeno, il presente protocollo vuole sensibilizzare il personale dipendente ed i soggetti che collaborano a vario titolo con il titolare del trattamento sulle responsabilità in tema di protezione dei dati personali e sull'importanza della collaborazione per una efficiente ed efficace gestione dei diritti esercitati dai soggetti interessati dal trattamento.

Quanto descritto è applicabile a tutti i trattamenti realizzati dal titolare del trattamento o per conto del medesimo, come descritti nel registro dei trattamenti redatto ai sensi dell'art. 30 GDPR.

Il protocollo è destinato alla consultazione da parte del personale dipendente e dei soggetti facenti parte dell'organigramma del titolare del trattamento, nonché – ove necessario - a coloro che realizzano trattamenti per conto del titolare del trattamento.

La responsabilità della concreta attuazione del protocollo risiede in seno al titolare del trattamento, in persona del Presidente *p.t.*, previa consultazione del Responsabile della Protezione Dati dal medesimo nominato ai sensi dell'art. 37 ss. GDPR.

Per l'attuazione del protocollo si suggerisce di nominare un referente ovvero un comitato.

2. Diritto di accesso ai dati personali.

L'art. 15 GDPR consente agli interessati di ottenere dal titolare del trattamento, in qualsiasi momento e senza ingiustificato ritardo, la conferma che sia o meno in corso un trattamento di dati personali che li riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

- a) le finalità del trattamento;
- b) le categorie di dati personali in questione;
- c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- e) l'esistenza del diritto degli interessati di chiedere al titolare del trattamento del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- f) il diritto di proporre reclamo all'Autorità di controllo (Garante per la protezione dei dati personali);

- g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, paragrafi 1 e 4 GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Nell'ipotesi in cui i dati personali oggetto del trattamento siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'art. 46 GDPR relative al trasferimento.

Su richiesta dell'interessato, il titolare del trattamento deve fornire una copia dei dati personali oggetto di trattamento; in caso di ulteriori copie richieste dall'interessato, ovvero nelle altre ipotesi eventualmente indicate dal titolare del trattamento, potrebbe addebitarsi un contributo spese alla risposta, sempre che lo stesso sia ragionevole e basato sui costi amministrativi.

Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa del medesimo, le informazioni devono essere fornite in un formato elettronico di uso comune. Ove possibile, inoltre, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali.

Il diritto di accesso include tutti i dati personali dell'interessato, siano essi dati comuni o dati particolari, ovvero dati relativi a condanne penali o reati (cfr. artt. 9 e 10 GDPR). Rimane fermo che il diritto di ottenere una copia dei dati non deve ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale, i diritti di proprietà intellettuale o altre informazioni comunque riservate. Tuttavia, tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni. Se il titolare del trattamento tratta una notevole quantità d'informazioni riguardanti l'interessato, l'interessato dovrebbe precisare, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce. Risultano, altresì, escluse le informazioni relative alle modalità del trattamento.

Infine, il titolare del trattamento non dovrebbe conservare dati personali al solo scopo di poter rispondere a potenziali richieste, di talché una volta esauritosi il periodo di conservazione dei dati, gli stessi dovranno essere oggetto di cancellazione.

3. Diritto di rettifica dei dati personali.

Ai sensi dell'art. 16 GDPR gli interessati hanno il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo, qualora gli stessi risultino errati, incompleti o non aggiornati.

In particolare, tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

4. Diritto alla cancellazione dei dati personali¹.

Secondo l'art. 17 GDPR, c.d. "diritto all'oblio", gli interessati hanno il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che li riguardano, senza ingiustificato ritardo, e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

- a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

¹Cfr. Linee guida 5/2019 sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca, ai sensi del RGPD (parte 1) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_it.

- b) l'interessato revoca il consenso su cui si basa il trattamento conformemente agli artt. 6, par. 1, lett. a), o 9, par. 2, lett. a), GDPR e se non sussiste altro fondamento giuridico per il trattamento;
- c) l'interessato si oppone al trattamento ai sensi dell'art. 21, par. 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'art. 21, par. 2;
- d) i dati personali sono stati trattati illecitamente;
- e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento (il diritto italiano);
- f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'art. 8, par. 1.

Il diritto alla cancellazione è, in particolare, rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet. In tale ipotesi, l'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore. Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

La cancellazione dovrebbe essere estesa in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali. Nel fare ciò, sarebbe opportuno che il titolare del trattamento adotti misure ragionevoli tenendo conto della tecnologia disponibile e dei mezzi a sua disposizione, comprese misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali.

L'esercizio del diritto alla cancellazione può essere legittimamente negato:

- g) per l'esercizio del diritto alla libertà di espressione e di informazione;
- h) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento (diritto italiano) o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- i) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'art. 9, par. 2, lettere h) e i), e dell'art. 9, par. 3;
- j) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'art. 89, par. 1, nella misura in cui il diritto di cui al par. 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;

k) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

5. Diritto alla limitazione del trattamento dei dati personali.

Secondo l'art. 18 GDPR, gli interessati hanno il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorra una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento ai sensi dell'art. 21, par. 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Nelle ipotesi in cui il trattamento dei dati sia limitato per le suesposte ragioni, tali dati possono essere trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

In ogni caso, gli interessati che abbiano ottenuto la limitazione del trattamento a norma dell'art. 18 GDPR sono informati dal titolare del trattamento prima che detta limitazione sia eventualmente revocata. In aggiunta, il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori; pertanto, sarebbe opportuno prevedere nei sistemi informativi (elettronici o meno) misure idonee a tale scopo.

Le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web.

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. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato.

6. Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento.

Il titolare del trattamento deve comunicare a ciascuno dei destinatari cui sono stati trasmessi i dati personali, ad esempio al fine di realizzare un trattamento quale responsabile *ex art. 28 GDPR*, le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma degli artt. 16, 17 e 18 GDPR, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

Qualora l'interessato lo richieda, il titolare del trattamento deve rendergli noti tali destinatari.

7. Diritto alla portabilità dei dati².

² Il Gruppo "Articolo 29" (EU) ha pubblicato linee-guida specifiche dove sono illustrati e spiegati i requisiti e le caratteristiche del diritto alla portabilità con particolare riguardo ai diritti di terzi interessati i cui dati siano potenzialmente compresi fra quelli "relativi

L'art. 20 GDPR attribuisce agli interessati il diritto di chiedere e ricevere i dati personali che lo riguardano dal titolare del trattamento a cui li ha forniti, in un formato strutturato, di uso comune e leggibile da dispositivo automatico (e, ove possibile, interoperabile).

Ove tecnicamente fattibile, l'interessato dovrebbe avere il diritto di ottenere che i dati personali siano trasmessi direttamente dal titolare del trattamento a un altro titolare del trattamento, senza impedimenti da parte del titolare del trattamento, se tecnicamente fattibile; purtuttavia, il diritto dell'interessato di trasmettere o ricevere dati personali che lo riguardano non comporta l'obbligo per il titolare del trattamento di adottare o mantenere sistemi di trattamento tecnicamente compatibili con quanti adottati da altri titolari del trattamento.

Il diritto alla portabilità trova applicazione esclusivamente qualora, al contempo, il trattamento si basi sul consenso dell'interessato ai sensi degli artt. 6, par. 1, lett. a), o 9, par. 2, lett. a), o su un contratto ai sensi dell'art. 6, par. 1, lett. b), e sia effettuato con mezzi automatizzati.

Qualora un certo insieme di dati personali riguardi più di un interessato, l'esercizio del diritto alla portabilità non può comportare una lesione dei diritti e delle libertà altrui; esso, inoltre, lascia impregiudicato il diritto alla cancellazione di cui all'art 17 GDPR e non dovrebbe implicare la cancellazione dei dati personali riguardanti l'interessato, forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e fintantoché i dati personali siano necessari all'esecuzione di tale contratto.

È d'interesse per il titolare del trattamento osservare che tale diritto non trova applicazione nei confronti dei titolari del trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche e, dunque, quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investita.

8. Diritto di opposizione al trattamento dei dati

Ai sensi dell'art. 21 GDPR, l'interessato ha il diritto di opporsi al trattamento dei dati personali che lo riguardano anche qualora i dati personali siano lecitamente trattati dal titolare del trattamento per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investita.

Una volta esercitato il diritto di opposizione, il titolare del trattamento dovrebbe astenersi dal trattare ulteriormente i dati personali, salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento, tali da prevalere sugli interessi, sui diritti e sulle libertà dell'interessato, ovvero per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Nel contesto dell'utilizzo di servizi della società dell'informazione (fatta salva la direttiva 2002/58/CE), l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche. Inoltre, qualora il trattamento sia realizzato per finalità di marketing diretto, gli interessati hanno il diritto di opporsi al trattamento realizzato per tale finalità (compresa la profilazione nella misura in cui sia connessa a tale marketing diretto), in qualsiasi momento e gratuitamente; qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'art. 89, par. 1 GDPR, gli interessati, per motivi connessi alla propria situazione particolare, hanno il diritto di opporsi al trattamento di dati personali che li riguardano, salvo se il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

all'interessato" di cui quest'ultimo chiede la portabilità (versione italiana con le relative FAQ disponibile qui: www.garanteprivacy.it/regolamentoue/portabilita). Al riguardo, inoltre, vi sono numerosi provvedimenti con cui il Garante per la Protezione dei dati personali ha indicato criteri per il bilanciamento fra i diritti e le libertà fondamentali di terzi e quelli degli interessati esercitanti i diritti di cui all'art. 7 del d. lgs. 196/2003 e ss.mm.ii.

Come gli altri diritti di cui al GDPR, il diritto all'opposizione deve essere portato all'attenzione degli interessati e presentato chiaramente e separatamente da qualsiasi altra informazione.

9. Altri diritti degli interessati

Oltre ai suesposti diritti, esercitabili su iniziativa degli interessati e obbligatoriamente resi noti agli stessi ai sensi degli artt. 13 e 14 GDPR, la normativa vigente in materia di protezione dei dati personali ne riconosce di ulteriori a garanzia di un'effettiva ed efficace tutela dei diritti e delle libertà delle persone fisiche.

a) Diritto a non essere sottoposti ad un processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione³.

Gli interessati hanno il diritto di non essere sottoposti a una decisione basata unicamente su di un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che li riguardi o che incida in modo analogo e significativamente sulla loro persona.

Tale diritto non si applicherebbe nel caso in cui la decisione fosse necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento, o sia basata sul consenso esplicito dell'interessato; il diritto in parola trova, altresì applicazione, qualora la decisione basata unicamente sul trattamento automatizzato sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento (il diritto italiano).

In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione.

Nel caso in cui si intendesse realizzare un trattamento automatizzato comprendente la profilazione a fini decisionali, al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali, secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero un trattamento che comporti misure aventi tali effetti.

Le decisioni basate unicamente sul trattamento automatizzato, infine, non possono fondarsi sulle categorie particolari di dati personali di cui all'art. 9, par. 1 GDPR, a meno che non trovino applicazione le basi giuridiche del consenso esplicito dell'interessato o del trattamento necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, e solo qualora siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

b) Diritto di proporre reclamo all'autorità di controllo.

Come per i diritti di cui agli artt. 15 ss., il titolare del trattamento deve informare gli interessati del diritto di proporre reclamo all'autorità di controllo italiana, il Garante per la protezione dei dati

³ Cfr. le linee guida (EU) sulle decisioni basate su un trattamento automatizzato e sulla profilazione https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

personali, ovvero all'autorità di controllo dello Stato membro in cui essi risiedono abitualmente, lavorano oppure del luogo ove si è verificata la presunta violazione.

Ai sensi dell'art. 77 GDPR tale diritto è esercitabile per questioni che concernono la violazione delle norme del GDPR, fatto salvo ogni altro ricorso amministrativo o giurisdizionale.

c) Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo.

Altra fonte di tutela giurisdizionale è concessa agli interessati dall'art. 79 GDPR, secondo il quale, in sintesi, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda o avverso l'omessa trattazione di un reclamo, fatto salvo ogni altro ricorso amministrativo o extragiudiziale.

d) Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento.

Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'art. 77 GDPR, gli interessati hanno il diritto di proporre un ricorso giurisdizionale effettivo qualora ritengano che i diritti di cui gode a norma del GDPR siano stati violati a seguito di un trattamento.

Se del caso, le eventuali azioni nei confronti del titolare del trattamento o dei responsabili del trattamento da essa nominati dovrebbero essere promosse dinanzi alle autorità giurisdizionali italiane.

e) Notifica di una violazione dei dati personali all'autorità di controllo e agli interessati⁴.

In caso di violazione dei dati personali, il titolare del trattamento deve avvisare l'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è venuta a conoscenza della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche; qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, essa deve essere corredata dei motivi del ritardo.

Le violazioni subite dai responsabili del trattamento nominati dal titolare del trattamento soggiacciono agli stessi termini, sicché tali responsabili sono tenuti ad informare il titolare del trattamento della violazione senza ingiustificato ritardo.

Nell'ipotesi in cui la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe comunicarla all'interessato senza ingiustificato ritardo a meno che non ricorra una delle condizioni che escludono la cogenza di tale notifica.

Per informazioni aggiuntive sulla notifica di una violazione, si rinvia al "Protocollo *data breach*".

10. Modalità di esercizio dei diritti degli interessati.

Il titolare del trattamento rende noti agli interessati i diritti sin qui approfonditi mediante l'informativa resa ai sensi degli artt. 13 e 14 GDPR; tale documento, così come le comunicazioni relative ad eventuali richieste degli interessati, di esercizio dei propri diritti, deve essere caratterizzata da una forma concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro.

⁴ Cfr. le linee guida in materia di notifica delle violazioni di dati personali (*data breach notification*) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679, adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017 (Versione emendata e adottata il 6 febbraio 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052), nonché le Linee guida 01/2021 sugli esempi riguardanti la notifica di violazione dei dati, adottate da EDPB il 14 gennaio 2021 (https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_en)

Gli interessati possono esercitare i propri diritti mediante un'istanza o richiesta inviata con comunicazione elettronica o cartacea agli indirizzi di contatto del titolare del trattamento, come indicati nelle informative rese ai sensi degli artt. 13 e 14 GDPR, possibilmente adoperando il modello allegato al presente protocollo (cfr. allegato A).

Al momento della ricezione di una richiesta di esercizio dei diritti, il titolare del trattamento, in qualità di titolare del trattamento in persona del Presidente *p.t.*, con il supporto del Responsabile della Protezione dei dati, di eventuali altri soggetti all'uopo incaricati e di altri soggetti eventualmente competenti per il trattamento in esame (ad esempio, il referente del protocollo e/o il responsabile del trattamento nominato per i servizi IT), deve attivare la procedura che segue, **avendo cura di concluderla senza ingiustificato ritardo e comunque entro un mese dal ricevimento dalla richiesta** (cfr. punto VI):

- I. comunicare tempestivamente al Responsabile della Protezione dei dati e di eventuali altri soggetti all'uopo incaricati dal titolare del trattamento la richiesta dell'interessato;
- II. il Titolare, con il supporto Responsabile della Protezione dei dati e di eventuali altri soggetti all'uopo incaricati, valuta la richiesta e dispone la comunicazione all'interessato della presa in carico della richiesta, anche al fine di accertare con certezza l'identità del medesimo ed eventualmente del soggetto che presenta la richiesta per suo conto, anche mediante richiesta di invio di copia digitale del documento di riconoscimento valido;
- III. a) nel caso in cui le informazioni ricevute al fine di accertare l'identità del richiedente e dell'eventuale soggetto che presenta la richiesta per suo conto risultino insufficienti, la richiesta può essere respinta fino all'ottenimento della prova necessaria;
b) accertata l'identità del richiedente, il Titolare, con il supporto del Responsabile della Protezione dei dati, di eventuali altri soggetti all'uopo incaricati e di altri soggetti eventualmente competenti per il trattamento in esame, individua l'ambito operativo del diritto esercitato e l'eventuale sussistenza di condizioni che ostano all'esercizio di tale diritto. Ove necessario, chiedere chiarimenti all'interessato in merito alla richiesta (ad esempio, novero di dati oggetto della richiesta);
- IV. il Titolare, con il supporto del Responsabile della Protezione dei dati, di eventuali altri soggetti all'uopo incaricati e di altri soggetti eventualmente competenti per il trattamento in esame, seleziona i dati oggetto del diritto e individua al loro interno eventuali informazioni che potrebbero rivelare dati personali di terzi o che potrebbero ledere i diritti e le libertà di terzi, ovvero informazioni o beni oggetto di segreti industriali o aziendali, del diritto di proprietà intellettuale o comunque riservate, per valutarne l'esclusione dalla risposta inviata all'interessato e dal campo di applicazione del diritto esercitato (non sussiste, invece, alcun obbligo di verificare la qualità dei dati prima di trasmetterli, sebbene gli stessi debbano necessariamente essere esatti e aggiornati, conformemente alle disposizioni del GDPR);
- V. il Titolare, con il supporto del Responsabile della Protezione dei dati, di eventuali altri soggetti all'uopo incaricati e di altri soggetti eventualmente competenti per il trattamento in esame, individua lo strumento tecnico più opportuno per trasmettere i dati al richiedente o effettuare la diversa operazione oggetto del diritto esercitato, tenuto conto di quanto specificamente richiesto dall'interessato e delle misure tecniche e organizzative idonee a garantire la protezione dei dati.
Salvo che la richiesta non comporti oneri ingiustificati in seno al titolare del trattamento, la risposta alla richiesta di esercizio dei diritti deve essere fornita gratuitamente, senza

commissioni o oneri di sorta (ad esempio, sarebbe legittimo chiedere all'interessato di sopportare i costi di spedizione di raccomandate o di copia su penna USB, ovvero chiedere un contributo qualora un interessato abbia già esercitato il diritto oggetto di ulteriore richiesta, o per richieste manifestamente infondate o eccessive);

VI. il Titolare, con il supporto del Responsabile della Protezione dei dati, di eventuali altri soggetti all'uopo incaricati e di altri soggetti eventualmente competenti per il trattamento in esame, fornisce all'interessato le informazioni relative all'esito dell'azione intrapresa, comprensive degli eventuali dati richiesti nonché delle ragioni dell'eventuale esclusione di alcuni dati o del rigetto della richiesta, senza ingiustificato ritardo e comunque entro un mese dal ricevimento dalla richiesta.

In casi di particolare complessità ovvero a fronte di particolari circostanze, il titolare del trattamento può prorogare il termine di risposta sino a un massimo di tre mesi, purché l'interessato venga informato delle motivazioni di tale proroga entro un mese dal ricevimento della richiesta iniziale (ad esempio, la quantità di dati trattati dal titolare del trattamento impone all'interessato di precisare specificamente l'informazione o le attività di trattamento cui la richiesta si riferisce, oppure i tempi di evasione della richiesta sono prorogati a causa del numero di richieste ricevute);

VII. il Titolare, con il supporto del Responsabile della Protezione dei dati, di eventuali altri soggetti all'uopo incaricati e di altri soggetti eventualmente competenti per il trattamento in esame, conserva quanto strettamente necessario a dar conto dell'avvenuto esercizio dei diritti da parte degli interessati e delle azioni intraprese, posto che se le finalità per cui il titolare del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligata a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il GDPR (cfr. art. 11, par. 1 GDPR).

Per quanto specificamente concerne il diritto di accesso, dovrebbe garantirsi agli interessati l'accesso remoto a un sistema sicuro che consente di consultare direttamente i propri dati personali (ad esempio, mediante l'accesso sulla piattaforma dei servizi informatici).

Rimane fermo che al fine di ottemperare alle richieste di esercizio dei diritti degli interessati sarà essenziale aggiornare con continuità la mappatura dei dati e delle informazioni inerenti al loro trattamento, così da poter individuare quelli su cui sono esercitabili i diritti degli interessati.

11. Definizioni (cfr. art. 4 GDPR)

- a. «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- b. «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- c. «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- d. «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a 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;
- e. «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- f. «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- g. «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- h. «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- i. «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- j. «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- k. «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- l. «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

- m. «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- n. «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- o. «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- p. «stabilimento principale»: a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del GDPR;
- q. «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'art. 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del GDPR;
- r. «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
- s. «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- t. «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
- u. «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51;
- v. «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello

Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;

- w. «trattamento transfrontaliero»: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
- x. «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del GDPR, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al GDPR, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
- y. «servizio della società dell'informazione»: il servizio definito all'art. 1, par. 1, lett. b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);
- z. «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.