Delibera del Garante n.12 del 26 marzo 2026

Oggetto: Regolamento per il "*trattamento dei dati personali e sulla tutela delle persone fisiche con riguardo ai trattamenti effettuati dall'Autorità Garante nazionale dei diritti delle persone con disabilità*". ***ADOZIONE***.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

Oggetto: Regolamento per il "*trattamento dei dati personali e sulla tutela delle persone fisiche con riguardo ai trattamenti effettuati dall'Autorità Garante nazionale dei diritti delle persone con disabilità*".
***ADOZIONE*.**

IL GARANTE

Il giorno **26** del mese di marzo dell'anno 2026, in Roma, presso la sede legale dell'Autorità Garante nazionale dei diritti delle persone con disabilità, presenti l'avv. Maurizio Borgo, il prof. Francesco Vaia e l'ing. Antonio Pelagatti, Collegio del Garante regolarmente costituito;

vista la legge 22 dicembre 2021, n. 227, recante «Delega al Governo in materia di disabilità» e, in particolare, l'articolo 2, comma 2, lettera f), che prevede l'istituzione del Garante nazionale delle disabilità, al fine di assicurare la piena attuazione e la tutela dei diritti e degli interessi delle persone con disabilità;

visto il decreto legislativo 5 febbraio 2024, n. 20, recante "Istituzione dell'Autorità Garante Nazionale dei diritti delle persone con disabilità" (in seguito denominata "Autorità");

visto inoltre
- il regolamento (UE) 2016/679 del parlamento Europeo e del Consiglio del 27 aprile 2016 (regolamento generale sulla protezione dei dati);
- il decreto legislativo n. 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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», che ha modificato il d.lgs. 30 giugno 2003, n. 196, recante il «Codice in materia di protezione dei dati personali»;

visto altresì
- il regolamento concernente l'organizzazione e il funzionamento dell'Autorità Garante nazionale dei diritti delle persone con disabilità, approvato con deliberazione n. 1 del 4 febbraio 2025 e ss.mm.ii.;
- che con determina n.10 del 16 marzo 2026 del Direttore generale dell'Ufficio del Garante, è stato affidato il servizio di Responsabile della Protezione dei Dati (RPD/DPO) ai sensi del d.lgs. 36/2023 e la contestuale designazione per il predetto incarico all'ing. Maurizio Giacci;

tenuto conto
- che l'Autorità Garante nazionale dei diritti delle persone con disabilità esercita funzioni di tutela, promozione e monitoraggio dei diritti delle persone con disabilità;
- che nello svolgimento delle proprie funzioni istituzionali l'Autorità può trattare dati personali, anche appartenenti a categorie particolari ai sensi dell'articolo 9 del Regolamento (UE) 2016/679, con particolare riferimento a dati relativi alla salute e alla condizione di disabilità;

- che tali trattamenti devono essere effettuati nel pieno rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza;
- che il Regolamento (UE) 2016/679 attribuisce al titolare del trattamento la responsabilità di adottare misure tecniche e organizzative adeguate al fine di garantire e dimostrare la conformità dei trattamenti alla normativa vigente;
- che, ai fini dell'attuazione del principio di responsabilizzazione (accountability), risulta necessario definire in modo organico:
  - i ruoli e le responsabilità dei soggetti coinvolti nei trattamenti;
  - le modalità di gestione dei dati personali nell'ambito delle attività istituzionali dell'Autorità;
  - le misure di sicurezza tecniche e organizzative;
  - le procedure di gestione dei diritti degli interessati;
  - le modalità di gestione delle violazioni dei dati personali;
- che l'adozione di un regolamento interno in materia di protezione dei dati personali costituisce strumento essenziale per garantire la conformità dell'azione amministrativa ai principi e alle disposizioni in materia di trattamento dei dati personali di cui al citato Regolamento (UE) 2016/679;

considerato

- che l'adozione del Regolamento per il trattamento dei dati personali e sulla tutela delle persone fisiche, con riguardo ai trattamenti effettuati dall'Autorità, costituisce una misura organizzativa necessaria per assicurare la conformità delle attività dell'Autorità alla normativa europea e nazionale in materia di protezione dei dati personali;
- che il Regolamento consente inoltre di rafforzare le garanzie di tutela dei diritti degli interessati e di assicurare un quadro chiaro e organico delle responsabilità e delle procedure interne relative al trattamento dei dati personali;

preso atto

- che l'Ufficio, con il supporto del Responsabile della protezione dei dati, ha predisposto una proposta di Regolamento al fine di disciplinare in modo organico le modalità di trattamento dei dati personali effettuati dall'Autorità nello svolgimento delle proprie funzioni istituzionali;
- che il Regolamento è articolato in più capi e articoli, che disciplinano in modo organico i diversi profili relativi al trattamento dei dati personali. In particolare:
  - una prima parte contiene le definizioni e i principi generali applicabili ai trattamenti di dati personali effettuati dall'Autorità;
  - una seconda parte disciplina i ruoli e le responsabilità dei soggetti coinvolti nei trattamenti, con particolare riferimento al titolare del trattamento, ai soggetti autorizzati, al trattamento e al Responsabile della protezione dei dati;
  - una ulteriore sezione definisce le misure tecniche e organizzative adottate dall'Autorità per garantire la sicurezza dei dati personali, anche con riferimento alla gestione delle infrastrutture informatiche e alla figura degli amministratori di sistema;
  - specifiche disposizioni sono inoltre dedicate alla conservazione dei dati personali nonché alla gestione delle violazioni dei dati personali e all'esercizio dei diritti degli interessati;

ravvisata l'esigenza di adottare il Regolamento per il "*trattamento dei dati personali e sulla tutela delle persone fisiche con riguardo ai trattamenti effettuati dall'Autorità Garante nazionale dei diritti delle persone con disabilità*";

ritenuto, quindi, di adottare il Regolamento per il "*trattamento dei dati personali e sulla tutela delle persone fisiche con riguardo ai trattamenti effettuati dall'Autorità Garante nazionale dei diritti delle persone con disabilità*";

dichiarata
- la regolarità giuridico-amministrativa del presente provvedimento;

considerato
- che non sussistono motivi ostativi a procedere, attesa la piena conformità dell'atto alle disposizioni di legge ed ai regolamenti dell'Autorità;
- che in merito al trattamento dei dati ed in osservanza a quanto previsto dal d.lgs. n. 196/2003 e nel Regolamento (UE) 2016/679 (GDPR) circa il rispetto dei principi e delle prescrizioni per il trattamento e diffusione dei dati personali, con la firma del presente Atto si attesta la rispondenza del testo del provvedimento e degli eventuali allegati alle suddette prescrizioni, ai fini della pubblicazione nei modi di legge sul sito web istituzionale dell'Autorità, nelle apposite sezioni

DELIBERA

per le motivazioni espresse in narrativa, che qui si intendono integralmente riportate,

1) di adottare il Regolamento per il "*trattamento dei dati personali e sulla tutela delle persone fisiche con riguardo ai trattamenti effettuati dall'Autorità Garante nazionale dei diritti delle persone con disabilità*" (cfr. **allegato "A"**, *composto da 25 (venticinque) pagine formato A4 e stampate su unica facciata*);

2) di disporre la pubblicazione del presente provvedimento, unitamente al "*Regolamento per il trattamento dei dati personali e sulla tutela delle persone fisiche con riguardo ai trattamenti effettuati dall'Autorità Garante nazionale dei diritti delle persone con disabilità*", sul sito web istituzionale dell'Autorità, nelle apposite sezioni.

Il Collegio:

- avv. Maurizio Borgo _____

- prof. Francesco Vaia _____

- ing. Antonio Pelagatti _____

- il segretario verbalizzante
Direttore Generale Ufficio del Garante
ing. Ciro Verdoliva _____

ALLEGATO"A"

REGOLAMENTO

sul TRATTAMENTO dei DATI PERSONALI e sulla TUTELA delle PERSONE FISICHE con riguardo ai TRATTAMENTI EFFETTUATI dall'AUTORITÀ GARANTE nazionale dei diritti delle persone con disabilità.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

TITOLO I
PRINCIPI, DIRITTI, RUOLI.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

CAPO I
DISPOSIZIONI GENERALI

Art. 1 - Oggetto

1. Il presente Regolamento disciplina i trattamenti di dati personali effettuati dall'Autorità Garante nazionale dei diritti delle persone con disabilità, di seguito per brevità anche "***Autorità***", in attuazione del Regolamento (UE) 2016/679 e della normativa nazionale vigente in materia di protezione dei dati personali.

2. L'Autorità assicura che i trattamenti di dati personali siano effettuati nel rispetto dei principi e delle disposizioni normative applicabili, adottando misure tecniche e organizzative adeguate a garantire la tutela dei diritti e delle libertà degli interessati.

3. L'Autorità promuove, nell'ambito della propria organizzazione, la conoscenza e l'osservanza della disciplina in materia di protezione dei dati personali da parte del personale e di tutti i soggetti che, a qualunque titolo, operano per conto della stessa.

4. Il presente Regolamento è portato a conoscenza di tutto il personale dipendente e degli altri soggetti autorizzati o comunque legittimati a trattare dati personali per conto dell'Autorità, che sono tenuti a conformarsi alle relative disposizioni.

Art. 2 - Ambito di applicazione

Il presente Regolamento si applica a tutti i trattamenti di dati personali effettuati dall'Autorità con strumenti automatizzati e non automatizzati, nell'ambito dello svolgimento delle proprie funzioni istituzionali, nonché ai trattamenti effettuati da soggetti terzi per conto della stessa.

Art. 3 - Definizioni

Ai fini del presente Regolamento si intende per:

- **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;
- **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.
- **Dati Particolari**
  categoria di dati personali che rivela l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

- **Dato Personale**
  qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere individuata, 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.

- **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.

- **Informativa**
  l'insieme delle informazioni che il Titolare e/o l'eventuale Responsabile rendono all'interessato ai sensi degli artt. 13 e/o 14 GDPR.

- **Normativa applicabile**
  l'insieme delle norme applicabili in materia di protezione dei dati personali, incluso il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (General Data Protection Regulation, "GDPR"), il D.Lgs. 196/2003 (c.d. "Codice Privacy"), come modificato dal D.Lgs. 101/2018, nonché in ogni tempo, ogni linea guida, norma di legge, codice o provvedimento rilasciato o emesso dagli organi competenti o da altre autorità di controllo, ivi inclusi i Provvedimenti del Garante per la protezione dei dati personali che resteranno in vigore.

- **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.

- **Responsabile della protezione dei dati** o **DPO**
  il soggetto, disciplinato dagli artt. 37 e seguenti del GDPR, che svolge funzioni consultive, formative e le altre funzioni ivi previste; tale soggetto è ontologicamente diverso dal Responsabile del trattamento dei dati e non deve essere confuso con tale figura.

- **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.

- **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.

- **Trattamento dei dati personali**

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

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.

- **Violazione dei dati personali** (***data breach***)
  una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato a dati personali trasmessi, conservati o comunque trattati. Rientrano, a titolo esemplificativo e non esaustivo, le ipotesi di phishing con compromissione di credenziali/account, infezione da malware, smarrimento o furto di dispositivi o documenti, invio errato a destinatari non corretti.

Art. 4 - Principi da applicare al trattamento dei dati personali

1. Il trattamento di dati personali deve osservare i seguenti principi:

a) liceità, correttezza e trasparenza: i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
b) limitazione della finalità: i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo compatibile con tali finalità;
c) minimizzazione dei dati: i dati personali raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
d) esattezza: i dati personali raccolti devono essere esatti e, se necessario, aggiornati. Devono essere, inoltre, adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
e) limitazione della conservazione: i dati personali raccolti devono essere conservati in una forma che consenta l'identificazione degli Interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
f) integrità e riservatezza: i dati personali raccolti devono essere trattati in maniera da garantire un'adeguata sicurezza ivi compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti, dalla perdita, dalla distruzione e dal danno accidentale.

2. Con riferimento al principio di limitazione della finalità, l'ulteriore trattamento dei dati personali ai fini dell'archiviazione nel pubblico interesse, per la ricerca scientifica o storica o ai fini statistici non è considerato incompatibile con le finalità iniziali.

3. Con riferimento al principio di limitazione della conservazione, i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente ai fini dell'archiviazione nel pubblico interesse, per la ricerca scientifica o storica o ai fini statistici.

Privacy by design

L'Autorità garantisce che i trattamenti di dati personali siano progettati e realizzati nel rispetto dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita (privacy by design e privacy by default), ai sensi dell'art. 25 del Regolamento (UE) 2016/679.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

Art. 5 - Liceità del trattamento

1. Il trattamento dei dati è lecito, pur senza il consenso dell'Interessato, se esso è necessario:
a) all'esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
b) per adempiere un obbligo legale al quale è soggetto il Titolare del Trattamento;
c) per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;
d) per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
e) per il perseguimento del legittimo interesse del Titolare del Trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiedono la protezione dei dati personali, in particolare se l'Interessato è un minore.

2. È altresì lecito svolgere trattamenti di dati particolari, ex art. 9 GDPR, qualora essi riguardino dati personali resi manifestamente pubblici dall'interessato o qualora essi:
a) siano necessari per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del Trattamento o dell'Interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
b) siano necessari per tutelare un interesse vitale dell'Interessato o di un'altra persona fisica qualora l'Interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
c) siano effettuati, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'Interessato;
d) il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
e) siano necessari per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'Interessato;
f) siano necessari per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità;
g) siano necessari per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'Interessato, in particolare il segreto professionale;

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

h) siano necessari a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'Interessato

3. Qualora non ricorrano i presupposti previsti nei precedenti commi 1 e 2, il trattamento dei dati personali è autorizzato solo se l'Interessato ha prestato il proprio consenso.

4. Il consenso dovrà essere formulato mediante un atto positivo inequivocabile, con il quale l'Interessato manifesta l'intenzione libera, specifica e informata di accettare il trattamento dei dati personali che lo riguardano. Dovranno essere adottate misure tecniche e organizzative volte a garantirne la verificabilità.

5. L'Interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. Dovranno essere adottate misure tecniche e organizzative idonee a favorire la richiesta di revoca da parte dell'interessato.

6. Qualora il trattamento dei dati avvenga nella circostanza indicata al precedente punto h) del comma 2, dovranno essere adottate misure tecniche e organizzative, in particolare quelle finalizzate a garantire il rispetto del principio della minimizzazione dei dati, adeguate a tutelare i diritti e le libertà dell'interessato. Tali misure dovranno includere l'utilizzo della tecnica della pseudonimizzazione o di qualsiasi altra tecnica che non permetta più l'identificazione dell'interessato.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

CAPO II
DIRITTI DELL'INTERESSATO

Art. 6 - Diritti dell'interessato

1. Con riferimento ai dati personali trattati dall'Autorità, l'interessato può avvalersi del:

a) diritto di accesso, ossia avere conferma dell'esistenza o meno di un trattamento di dati personali che lo riguardano e, in caso affermativo, di venire a conoscenza delle caratteristiche del trattamento;
b) il diritto di rettifica, ossia la modifica di dati personali inesatti e/o l'integrazione di dati personali incompleti;
c) il diritto di cancellazione, ossia la richiesta di immediata cancellazione dei dati personali se ne ricorrono i presupposti normativi;
d) il diritto di limitazione, ossia ottenere una limitazione al trattamento dei suoi dati personali;
e) il diritto alla portabilità dei dati, ossia ottenere, in caso di trattamenti effettuati con mezzi automatizzati, in formato strutturato i dati personali che lo riguardano al fine di trasferirli presso un'altra organizzazione.
f) diritto di opposizione, ossia di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, a trattamenti di dati personali che lo riguardano e svolti per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri oppure per il perseguimento del legittimo interesse del titolare del trattamento o di terzi.
g) diritto di opposizione a processi decisionali automatizzati, ossia richiedere 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 in modo analogo significativamente sulla sua persona.

2. Per l'esercizio dei propri diritti, l'interessato può rivolgersi al Titolare del trattamento ovvero al Responsabile della protezione dei dati, ferma restando la possibilità di proporre reclamo al Garante per la protezione dei dati personali.

Art. 7 - Informativa

1. Ai sensi dell'art. 13 del GDPR è istituita un'area, all'interno del portale istituzionale dell'Autorità Garante nazionale dei diritti delle persone con disabilità e raggiungibile dalla pagina principale dello stesso, in cui saranno pubblicate le informative mediante le quali gli interessati potranno ottenere informazioni sui trattamenti di dati personali eseguiti dalla stessa.

2. Ogni informativa deve essere redatta in forma concisa, trasparente, intelligibile e facilmente accessibile, con linguaggio semplice e chiaro.

3. Qualora la raccolta dei dati personali avvenga presso l'Interessato, l'informativa dovrà contenere:

a) l'identità e i dati di contatto del titolare del trattamento;
b) i dati di contatto del Responsabile della Protezione dei Dati;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

d) i legittimi interessi perseguiti dal Titolare del Trattamento o da terzi, qualora il trattamento si basi sulle circostanze indicate all'Art. 5, comma 1, lettera e);
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) l'eventualità che i dati personali vengano trasferiti a un paese terzo o a un'organizzazione internazionale;
g) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
h) la possibilità da parte dell'interessato di avvalersi dei diritti di cui all'Art. 6 del presente Regolamento;
i) qualora il trattamento sia basato sul consenso espresso dall'interessato, l'esistenza del diritto di revocare il consenso in un qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
j) l'esistenza del diritto di proporre reclamo a un'autorità di controllo;
k) indicazioni sulla comunicazione dei propri dati personali, se è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto. Inoltre se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
l) l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

4. Qualora la raccolta dei dati personali non avvenga presso l'interessato, l'informativa dovrà contenere:
a) l'identità e dei dati di contatto del titolare del trattamento;
b) i dati di contatto del Responsabile della Protezione dei Dati;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) le categorie di dati personali trattati;
e) gli eventuali destinatari o delle eventuali categorie di destinatari dei dati personali;
f) l'eventualità che i dati personali vengano trasferiti a un paese terzo o a un'organizzazione internazionale;
g) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
h) i legittimi interessi perseguiti dal Titolare del Trattamento o da terzi, qualora il trattamento si basi sulle circostanze indicate all'Art. 5, comma 1, lettera e);
i) la possibilità da parte dell'interessato di avvalersi dei diritti di cui all'Art. 6 del presente Regolamento;
j) qualora il trattamento sia basato sul consenso espresso dall'interessato, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
k) il diritto di proporre reclamo a un'autorità di controllo;
l) la fonte da cui hanno origine i dati personali e, se del caso, dell'eventualità che i dati provengano da fonti accessibili al pubblico;
m) l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

CAPO III
TITOLARE DEL TRATTAMENTO, RESPONSABILE DEL TRATTAMENTO E RESPONSABILE DELLA PROTEZIONE DEI DATI

Art. 8 - Titolare del trattamento

1. L'Autorità Garante nazionale dei diritti delle persone con disabilità, nella persona del Direttore generale dell'Ufficio del Garante, opera quale Titolare del trattamento e determina le finalità e i mezzi dei trattamenti di dati personali effettuati nell'ambito delle proprie funzioni istituzionali.

2. Il Titolare del Trattamento è responsabile delle misure tecniche e organizzative da porre in essere al fine di attuare, in modo efficace, i principi di protezione dei dati, e di integrare nel trattamento le necessarie garanzie finalizzate a soddisfare i requisiti della Normativa Applicabile e a tutelare i diritti degli Interessati.

3. Tramite verifiche periodiche, il Titolare del Trattamento vigila, su tutti i soggetti che a diverso titolo trattano dati per suo conto, circa l'osservanza delle disposizioni stabilite dalla Normativa Applicabile e dal presente Regolamento.

Art. 9 - Responsabile del trattamento

1. Il Responsabile del Trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto di questa Autorità.

2. Qualora l'affidamento di un servizio o la stipula di una convenzione preveda la presenza della figura del Responsabile del Trattamento dovranno essere individuati unicamente soggetti che presentino garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate a soddisfare il rispetto dei principi di cui all'art. 4 del presente regolamento e ogni disposizione stabilita dalla normativa vigente sulla protezione dei dati personali.

3. I rapporti tra il Titolare del Trattamento e i Responsabili del Trattamento dovranno essere stabiliti attraverso contratti o altri atti giuridici, stipulati in forma scritta.

4. Il contratto o altro atto giuridico dovrà identificare la materia disciplinata, la durata, la natura e la finalità, nonché il tipo di dati personali, le categorie di Interessati e gli obblighi del Responsabile del Trattamento. In particolare, dovrà obbligare quest'ultimo:

a) a garantire che le persone che operano per suo conto e autorizzate al trattamento dei dati personali siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
b) ad adottare le misure necessarie a garantire il trattamento in sicurezza di dati personali;
c) ad assistere il titolare del trattamento qualora quest'ultimo sia chiamato a dar seguito alle richieste per l'esercizio dei diritti dell'Interessato;
d) a cancellare o restituire tutti i dati personali al termine della prestazione dei servizi e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

e) mettere a disposizione del Titolare del Trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del Trattamento o da un altro soggetto da questi incaricato;
f) a informare immediatamente il Titolare del Trattamento su ogni circostanza che, a suo parere, comporti la violazione del presente regolamento e di ogni altra disposizione in materia di protezione dei dati personali;
g) ad assistere il Titolare del Trattamento nelle procedure finalizzate alla valutazione degli impatti sulla protezione dei dati, fornendo allo stesso ogni informazione di cui è in possesso;
h) a informare il Titolare del Trattamento, senza ingiustificato ritardo, su avvenuti casi di violazione dei dati personali e assistere il Titolare del Trattamento nello svolgimento di ogni procedura conseguenziale, quale ad esempio la notifica di violazione all'Autorità Garante per la Protezione dei Dati Personali.

Art. 10 - Responsabile della protezione dei dati

1. Ai sensi degli artt. 37 e seguenti del GDPR, l'Autorità designa il Responsabile della protezione dei dati (RPD/DPO).

2. Il Responsabile della Protezione dei Dati è la figura professionale incaricata almeno dei seguenti compiti:
a) informare e fornire consulenza al Titolare del Trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. In tal senso il Responsabile della Protezione dei Dati può indicare al Titolare del Trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
b) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare del Trattamento;
c) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;
d) cooperare con l'Autorità Garante per la Protezione dei Dati Personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento.

3. La figura del Responsabile della Protezione dei Dati è incompatibile con chi determina le finalità o i mezzi del trattamento. In particolare, risultano con la stessa incompatibili:
a) il responsabile per la prevenzione della corruzione e per la trasparenza;
b) la figura del responsabile del trattamento.

4. Il Responsabile della Protezione dei Dati opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti. In particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

5. Il Responsabile della Protezione dei Dati non può essere rimosso o penalizzato per l'adempimento dei propri compiti nel rispetto della normativa applicabile.

6. Ferma restando l'indipendenza nello svolgimento di detti compiti, il Responsabile della Protezione dei Dati riferisce direttamente al rappresentante legale pro tempore del Titolare del Trattamento o suo delegato.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

Art. 11 - Registro delle attività di trattamento

1. Ai sensi dell'art. 30 del GDPR è istituito il Registro delle Attività di Trattamento che identifica tutti i trattamenti di dati personali operati dall'Autorità Garante nazionale dei diritti delle persone con disabilità.

2. Il Registro delle Attività di Trattamento riporterà i dati di contatto del Titolare del Trattamento e del Responsabile della Protezione dei Dati. Inoltre, per ogni trattamento di dati personali le seguenti informazioni:

a) le finalità del trattamento;
b) i dati di contatto di un eventuale contitolare del trattamento;
c) la sintetica descrizione delle categorie di Interessati, nonché le categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) il richiamo alle misure di sicurezza tecniche e organizzative adottate.

3. Il Registro delle Attività di Trattamento sarà tenuto in formato digitale, acquisito al protocollo e posto in conservazione sostitutiva.

Art. 12 - Valutazione d'impatto della protezione dei dati

1. Qualora un trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche sarà predisposta, ai sensi dell'art. 35 del GDPR, la valutazione d'impatto della protezione dei dati (c.d. DPIA).

2. Fermo restando quanto indicato dall'art. 35 del GDPR, verrà condotta una DPIA nel caso in cui un trattamento ricada in almeno due delle seguenti circostanze:

a) trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su Interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli Interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
d) trattamenti di dati particolari;
e) trattamenti di dati su larga scala;
f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

g) dati relativi a Interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
i) tutti quei trattamenti che, di per sé, impediscono agli Interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

3. Qualora la DPIA evidenzi un rischio elevato residuo in assenza di misure idonee a mitigarlo, il Titolare del trattamento procede alla consultazione preventiva del Garante per la protezione dei dati personali ai sensi dell'art. 36 del GDPR.

4. Il Titolare del Trattamento consulta l'Autorità Garante per la Protezione dei Dati Personali anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale e alla sanità pubblica.

5. La valutazione d'impatto sulla protezione dei dati è effettuata dal Titolare del trattamento con il supporto delle strutture competenti, sentito il Responsabile della protezione dei dati, il quale fornisce il proprio parere ai sensi dell'art. 39 del GDPR e ne sorveglia lo svolgimento.

6. La documentazione prodotta a seguito di una DPIA sarà tenuta in formato digitale, acquisita al protocollo e posta in conservazione sostitutiva.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

TITOLO II
MISURE ORGANIZZATIVE E TECNICHE

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

CAPO I
MISURE ORGANIZZATIVE

Art. 13 - Principi generali

1. Il trattamento di dati personali è effettuato esclusivamente per finalità istituzionali, per l'adempimento di obblighi di legge, per l'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri, nonché per esigenze organizzative e gestionali strettamente connesse all'attività dell'Autorità.

2. Devono essere trattati esclusivamente i dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità perseguite.

3. Le informazioni trattate dovranno essere opportunamente cancellate o distrutte nei casi in cui:

a) non siano più utili al raggiungimento delle finalità istituzionali;
b) siano relative alla cessazione, per qualsiasi causa, di trattamenti di dati personali non più necessari o siano eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati;
c) gli scopi per le quali sono state raccolte e trattate non siano più determinati, espliciti e legittimi oppure siano diventate incompatibili con tali scopi
d) l'interessato ne richieda la cancellazione nell'esercizio dei propri diritti.

4. Il Responsabile della Protezione dei Dati sarà tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. In particolare egli:

a) deve essere invitato a partecipare alle riunioni di coordinamento che abbiano per oggetto questioni inerenti al trattamento di dati personali;
b) deve disporre tempestivamente di tutte le informazioni necessarie a rendere una idonea consulenza.

5. Al Responsabile della Protezione dei Dati sarà fornito il supporto necessario ad assolvere ai compiti attribuiti. In particolare, deve essergli assicurato il supporto attivo da parte dei dipendenti e degli organi di governo, nonché l'accesso ai settori funzionali di questa Autorità.

Art. 14 - Formazione del personale

L'Autorità promuove programmi periodici e documentati di formazione e aggiornamento in materia di protezione dei dati personali rivolti al personale dipendente e ai soggetti autorizzati al trattamento.

Art. 15 - Comunicazione e diffusione dei dati

1. La comunicazione e la diffusione dei dati personali da parte dell'Autorità sono consentite esclusivamente nei casi previsti dalla legge, dal regolamento o dalla normativa europea applicabile.

2. È in ogni caso esclusa la consultazione massiva o indiscriminata di banche dati in assenza di idoneo presupposto normativo o funzionale.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

Art. 16 - Soggetti delegati e designati al trattamento

1. I dirigenti e i responsabili dei procedimenti competenti sovrintendono ai trattamenti di dati personali effettuati nell'ambito degli uffici cui sono preposti, secondo le attribuzioni conferite dall'ordinamento interno dell'Autorità.

2. I soggetti che operano sotto l'autorità del Titolare del trattamento possono effettuare operazioni di trattamento solo se autorizzati e adeguatamente istruiti in ordine alle modalità del trattamento, ai limiti delle funzioni attribuite e alle misure di sicurezza da osservare.

3. I soggetti autorizzati al trattamento sono individuati sulla base delle effettive esigenze organizzative e operative connesse allo svolgimento delle mansioni loro assegnate.

4. I soggetti designati al trattamento devono garantire la massima riservatezza, nonché il rispetto delle disposizioni stabilite dalla Normativa Applicabile e dal presente regolamento e in particolare l'applicazione dei principi di cui all'Art. 4 del presente regolamento e dei diritti dell'interessato di cui all'Art. 6 del presente regolamento.

5. Il Titolare del trattamento, per il tramite dei dirigenti e i responsabili dei procedimenti, cura l'aggiornamento delle autorizzazioni al trattamento in caso di modifiche organizzative, mutamento delle mansioni, cessazione dell'incarico o variazione dell'ambito dei trattamenti effettuati.

Art. 17 - Sulla tenuta del Registro delle Attività di Trattamento

1. I dirigenti o responsabili delle strutture competenti collaborano alla predisposizione e all'aggiornamento del Registro delle attività di trattamento relativamente ai trattamenti di rispettiva competenza.

2. Il Registro, che dovrà essere revisionato almeno con cadenza annuale, individua i trattamenti di dati personali effettuati dall'Autorità e ne riporta gli elementi essenziali previsti dall'art. 30 del GDPR.

3. Il Responsabile della protezione dei dati fornisce supporto e consulenza in ordine alla corretta stesura e revisione del Registro delle Attività di Trattamento.

4. Il Titolare del Trattamento trasmette al Responsabile della Protezione dei Dati il Registro delle Attività dei Trattamenti che viene formato:
a) al termine del processo di iniziale stesura;
b) qualora si determini un nuovo aggiornamento;
c) al termine del processo di revisione annuale.

5. Il Registro delle Attività di Trattamento è tenuto in formato digitale, è acquisito al protocollo e posto in conservazione sostitutiva.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

Art. 18 - Sulla tenuta delle Informative

1. I dirigenti o responsabili dei procedimenti competenti collaborano alla predisposizione e all'aggiornamento delle informative relativamente ai trattamenti di rispettiva competenza.

2. I Dirigenti e i Responsabili dei Procedimenti sovrintendono, altresì, alla pubblicazione delle stesse nella corrispondente sezione istituita all'interno del portale istituzionale di questa Autorità.

3. Il Responsabile della protezione dei dati fornisce supporto e consulenza in ordine alla corretta tenuta delle informative.

Art. 19 - Rapporti con i Responsabili del Trattamento

1. Qualora l'affidamento di un servizio o la stipula di una convenzione preveda la presenza della figura del Responsabile del Trattamento, di cui all'Art. 9 del presente regolamento, ossia di un soggetto terzo che esegue un trattamento di dati per conto dell' Autorità Garante nazionale dei diritti delle persone con disabilità è obbligo dei Dirigenti e i Responsabili dei Procedimenti, ovvero di chiunque altro soggetto che per conto di questa Autorità ha facoltà di determinare l'affidamento o stipulare la convenzione, di individuare unicamente soggetti economici che presentino garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate a soddisfare il rispetto delle disposizioni della Normativa Applicabile e del presente Regolamento.

2. E' obbligo altresì dei I Dirigenti e i Responsabili dei Procedimenti, ovvero di chiunque altro soggetto che per conto dell'Autorità Garante nazionale dei diritti delle persone con disabilità ha facoltà di determinare l'affidamento o stipulare la convenzione, di disciplinare i rapporti con i Responsabili del Trattamento attraverso contratti o altri atti giuridici così come indicato ai punti 3 e 4 dell'Art. 9 del presente regolamento.

Art. 20 - Violazione dei dati personali

1. Qualsiasi soggetto autorizzato al trattamento che venga a conoscenza di un evento suscettibile di integrare una violazione dei dati personali è tenuto a darne immediata comunicazione al Titolare del trattamento e al Responsabile della protezione dei dati, secondo le procedure interne adottate dall'Autorità.

2. Al verificarsi di ogni evento di violazione dei dati personali, Il Titolare del trattamento, con il supporto delle strutture competenti e sentito il Responsabile della protezione dei dati, valuta senza ritardo la natura dell'evento, le possibili conseguenze e la necessità di procedere alla notifica al Garante e alla comunicazione agli interessati ai sensi degli artt. 33 e 34 del GDPR.

3. La notifica, di cui al precedente comma, avviene entro le 72 ore dal momento in cui il Titolare del Trattamento è venuto a conoscenza dell'evento di violazione.

4. Se il rischio per i diritti e le libertà degli Interessati coinvolti dall'evento di violazione di dati personali è elevato, allora questi ultimi saranno informati, senza ingiustificato ritardo, circa la natura della violazione verificatasi.

5. I rischi per i diritti e le libertà degli Interessati saranno considerati "elevati" quando la violazione può:
a) coinvolgere un rilevante quantitativo di dati personali e/o di soggetti Interessati;
b) riguardare categorie particolari di dati personali;

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

c) comprendere dati che possono accrescere ulteriormente i potenziali rischi (dati di localizzazione, finanziari, relativi alle abitudini e preferenze, etc.);
d) comportare rischi imminenti e con un'elevata probabilità di accadimento (rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito, etc.);
e) impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (utenti deboli, minori, soggetti indagati, etc.).

6. Gli eventi di violazione dovranno essere documentati all'interno del Registro degli Eventi di Data Breach, che, oltre ai riferimenti temporali legati all'accaduto, dovrà riportare le circostanze a esso relative, le conseguenze e i provvedimenti adottati.

7. Il Registro degli Eventi di Data Breach sarà tenuto in formato digitale, acquisito al protocollo e posto in conservazione sostitutiva.

Art. 21 - Tempi di conservazione

L'Autorità definisce, nell'ambito del proprio piano di conservazione documentale, i tempi di conservazione delle diverse categorie di dati personali trattati, nel rispetto dei principi di limitazione della conservazione e minimizzazione dei dati.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

CAPO II
MISURE TECNICHE

Art. 22 - Trattamenti disgiunto dei dati particolari

1. I dati particolari devono essere trattati con gestione disgiunta, ossia:

a) l'insieme dei dati personali che identificano una persona dovrà essere trattato separatamente dall'insieme dei dati particolari a essa collegati;

b) il collegamento tra le due tipologie di insiemi avviene attraverso l'utilizzo di codici identificativi atti a impedire l'immediata riconducibilità.

2. L'adozione di tecniche di crittografia e di ogni altro strumento offerto dalla tecnologia corrente, che rendono l'intero insieme dei dati particolari non comprensibili/intelligibili a persone non autorizzate, sostituisce l'obbligo del trattamento disgiunto di cui al precedente punto.

3. Le regole di cui ai precedenti punti sono applicate a ogni trattamento di dati particolari, sia che esso avvenga su supporto cartaceo che digitale.

Art. 23 - Trattamenti eseguiti mediante l'utilizzo dei documenti in formato cartaceo

1. I documenti in formato cartaceo che contengono dati personali dovranno essere conservati in archivi ciechi e dotati di serratura.

2. I documenti in formato cartaceo che contengono dati personali dovranno essere consultati solo all'interno degli uffici di questa Autorità non accessibili al pubblico. In caso di allontanamento, anche temporaneo, dalla postazione di lavoro dovranno essere poste in essere tutte le misure necessarie a evitare che soggetti non autorizzati possano accedere ai dati personali contenuti nei documenti in consultazione.

3.Le attività di stampa, fotocopia o acquisizione ottica di documenti contenenti dati personali dovranno essere svolte nel rispetto del principio di riservatezza, ossia evitando che soggetti non autorizzati possano visualizzare il contenuto dei documenti oggetto di trattamento. Al termine dell'attività il documento oggetto di trattamento dovrà essere rimosso dai dispositivi di stampa, fotocopia o acquisizione ottica.

Art. 23 - Amministratori di sistema

1. L'Autorità individua formalmente gli amministratori di sistema incaricati della gestione e manutenzione delle infrastrutture informatiche.

2. Gli accessi logici degli amministratori di sistema sono registrati e conservati per un periodo non inferiore a sei mesi.

3. I relativi accessi ai sistemi sono registrati e conservati per un periodo non inferiore a sei mesi.

Art. 24 - Dispositivi tecnologici e dei software

1. È fatto divieto di installare, senza autorizzazione del Titolare del Trattamento, sulle postazioni di lavoro fornite in dotazione qualsiasi software, soggetto a tutela autoriale, contenuto in dischetti, DVD-ROM e altri dispositivi removibili, o direttamente scaricato da Internet, senza la licenza d'uso commerciale, shareware o open source.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

2. Il soggetto a cui fa capo la responsabilità dei sistemi informativi provvede alla rimozione dei dispositivi non autorizzati e dei software non autorizzati o comunque non necessari allo svolgimento delle funzioni istituzionali.

3. E' fatto divieto di utilizzare gli strumenti tecnologici forniti in dotazione, nelle componenti sia hardware che software, in modo improprio o per fini personali.

4. All'interno della struttura informatica di questa Autorità è consentito esclusivamente l'utilizzo di dispositivi tecnologici e software autorizzati.

5. L'utilizzo dei dispositivi personali è ammesso esclusivamente per l'accesso a sistemi informativi erogati in modalità cloud o SaaS oppure attraverso l'uso di sistemi di crittografia del traffico, come VPN e ogni ulteriore sistema tecnicamente disponibile. Il proprietario del dispositivo garantisce, sotto la propria responsabilità, che i software e il sistema operativo installati sul sistema utilizzato siano conformi alla normativa e ogni altra disposizione di cui al comma 1 del presente articolo. L'organizzazione potrà unilateralmente stabilire i requisiti minimi hardware e software necessari per l'accesso alla rete sia da remoto che nei locali dell'organizzazione.

Art. 25 - Controllo degli accessi ai dispositivi e ai software

1. L'accesso a postazioni di lavoro, unità server, nodi di rete configurabili, software, risorse cloud e ogni altro dispositivo fornito in dotazione dall' Autorità Garante nazionale dei diritti delle persone con disabilità dovrà avvenire attraverso l'utilizzo di sistemi di identificazione, autenticazione e autorizzazione.

2. Le credenziali di autenticazione devono essere adeguatamente robuste, mantenute riservate e modificate senza ritardo in caso di sospetta compromissione, nonché modificate almeno semestralmente.

3. È vietato divulgare ad altri le credenziali personali di accesso. Il titolare delle credenziali è responsabile di tutte le azioni e le funzioni svolte per il tramite delle stesse.

4. In caso di allontanamento, anche temporaneo, dalla postazione di lavoro, l'utente è tenuto ad attivare il blocco della sessione o ad adottare ogni altra misura idonea a impedire accessi non autorizzati.

5. Le utenze dotate di privilegi di amministrazione devono essere utilizzate esclusivamente per dar luogo ad attività di gestione straordinaria del software. L'utilizzo ordinario di una postazione di lavoro o di una unità server deve essere effettuato mediante l'accesso con utenze dotate di privilegi limitati.

6. Le utenze dotate di privilegi di amministrazione definite per ogni postazione di lavoro, unità server, nodi di rete configurabili, software, risorse cloud e ogni altro dispositivo fornito in dotazione da questa Autorità dovranno essere riportate nel registro delle password che sarà custodito dal responsabile del sistema informativo.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

Art. 26 - Gestione delle postazioni di lavoro e delle unità server e delle risorse cloud

1. E' vietato l'utilizzo di postazioni di lavoro e unità server non dotati di software atti a rilevare la presenza e bloccare l'esecuzione di malware (c.d. antivirus), che dovranno essere automaticamente aggiornabili nella conoscenza delle impronte virali.

2. E' vietato l'utilizzo di sistemi operativi non aggiornati o non più aggiornabili. Laddove applicabile, l'aggiornamento degli stessi dovrà essere eseguito automaticamente.

3. Il soggetto a cui fa capo la responsabilità dei sistemi informativi, verifica trimestralmente la necessità di eseguire l'aggiornamento firmware dei dispositivi di rete e procede in tal senso quando necessario. Egli verifica, altresì, con la medesima periodicità e per ogni postazione di lavoro e unità server su cui operano sistemi operativi non aggiornabili automaticamente, la necessità di eseguire un aggiornamento.

4. In caso di malfunzionamento dell'elaboratore in uso, che possa far sospettare la presenza di un virus, malware, cryptolocker, keylogger o strumenti di controllo remoto, pur se legittimi ma non autorizzati direttamente dall'utente o dall'organizzazione stessa, è fatto obbligo di:

a) sospendere ogni operazione;
b) contattare immediatamente il soggetto a cui fa capo la responsabilità dei sistemi informativi;
c) chiudere il sistema e le relative applicazioni.
d) consegnare il dispositivo in uso al responsabile dei sistemi informativi;

5. La copia dei dati personali su supporti di memorizzazione di massa esterni e risorse cloud diverse da quelle poste a disposizione da questa Autorità, è consentita solo se necessaria per lo svolgimento delle funzioni istituzionali. In tal caso dovranno essere adottati sistemi per la crittografia dei dati oppure ogni altra misura che renda tali dati personali non comprensibili o intelligibili a persone non autorizzate.

6. Qualora venga meno la possibilità di adottare i sistemi per la criptazione dei dati di cui al comma precedente, i supporti di memorizzazione di massa esterni che contengono dati personali non potranno lasciare la sede ospitante gli uffici, dovranno essere utilizzati esclusivamente all'interno di quest'ultima e dovranno essere custoditi con diligenza e conservati in armadi o contenitori muniti di serratura.

Art. 27 - Comunicazioni mediante rete

1. L'utilizzo della rete Internet e dei servizi accessibili per il suo tramite è consentito solo se necessario per lo svolgimento delle funzioni istituzionali. Sono vietati comportamenti che possano arrecare danno alla reputazione e al patrimonio dell'Autorità Garante nazionale dei diritti delle persone con disabilità.

2. Il trattamento dei dati personali mediante reti di comunicazione elettronica deve avvenire mediante protocolli e canali sicuri, idonei a garantire la riservatezza, l'integrità e l'autenticità dei dati scambiati.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

3. L'accesso alle reti wireless dell'Autorità è consentito esclusivamente mediante sistemi di sicurezza e di controllo degli accessi coerenti con lo stato dell'arte e con le politiche di sicurezza adottate dall'Ente.

4. Le attività di accesso da remoto alle postazioni di lavoro, alle unità server e ai dispositivi di rete sono consentite solo se eseguite mediante l'utilizzo di connessioni protette e sotto il controllo e il monitoraggio del soggetto a cui fa capo la responsabilità dei sistemi informativi.

Art. 28 - Utilizzo del servizio di posta elettronica, dei servizi di messaggistica e delle risorse cloud

1. L'account istituzionale di posta elettronica è assegnato per lo svolgimento delle attività lavorative e deve essere utilizzato nel rispetto delle disposizioni normative, regolamentari e organizzative vigenti. E' pertanto vietato l'utilizzo per scopi personali.

2. Attraverso le caselle di posta elettronica si rappresenta pubblicamente l'Autorità Garante nazionale dei diritti delle persone con disabilità e per questo è fatto obbligo di utilizzare la posta elettronica in modo lecito, professionale e comunque tale da riflettere positivamente l'immagine di questa Autorità. Sono pertanto vietati comportamenti che possano arrecare danno alla reputazione e al patrimonio di quest'ultimo.

3. Ad uno stesso soggetto possono essere assegnate più caselle di posta elettronica, nonché indirizzi anche disgiunti dalla propria casella personale, che possono anche essere condivise con altri utenti dello stesso ufficio o di altri uffici, nei limiti del perseguimento di fini istituzionali e del miglioramento oggettivo dei servizi offerti all'utenza.

4. Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica affidata e devono:
- conservare la password nella massima riservatezza e con la massima diligenza;
- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
- verificare con particolare attenzione l'identità del mittente, l'attendibilità del contenuto, la correttezza dei collegamenti e degli allegati, evitando di aprire messaggi, file o link sospetti o non pertinenti.

5. Non è consentito l'invio automatico della posta ricevuta su account istituzionale verso un indirizzo di e-mail privato, anche durante i periodi di assenza.

6. In caso di assenza improvvisa o prolungata ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio ovvero per motivi di sicurezza del sistema informatico, il Titolare del Trattamento, per il tramite dell'amministratore di sistema, potrà accedere all'account di posta elettronica, prendendo visione dei messaggi, salvando o cancellando file. Di tale attività sarà redatto apposito verbale e informato il soggetto interessato alla prima occasione utile.

7. In caso di interruzione del rapporto di lavoro, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 (trenta) giorni da quella data ed entro 90 (novanta) giorni si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'Autorità Garante nazionale dei diritti delle persone con disabilità si riserva il diritto di

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

conservare i messaggi di posta elettronica ritenuti rilevanti per le proprie finalità istituzionali.

8. Salvo l'utilizzo di appositi strumenti di cifratura i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto è fatto obbligo di valutare con attenzione l'invio di informazioni contenenti dati personali che potranno essere trasmessi se:
a) il destinatario è certo;
b) il destinatario è autorizzato a entrare in possesso dei dati personali.

9. Fermo restando l'applicazione di quanto disposto al precedente punto, è fatto, altresì, obbligo di adottare sistemi per la cifratura dei contenuti qualora le informazioni trasmesse attraverso la posta elettronica contengano dati particolari.

10. L'utilizzo dei sistemi di messaggistica istantanea, di trasferimento dei dati o di ogni ulteriore sistema di trasferimento dei dati o di memorizzazione dei dati in cloud è regolamentato dalle medesime norme applicabili ai servizi di posta elettronica. E' fatto divieto di utilizzare detti sistemi ove non prevedano tecnologie di crittografia end-to-end per la trasmissione di documenti e dati dell'organizzazione, contenenti o meno dati ritenuti sensibili, senza preventiva autorizzazione espressa del Titolare del Trattamento.

11. L'utilizzo delle risorse cloud o dei servizi SaaS diversi da quelli ufficialmente messi a disposizione da parte dell'organizzazione deve essere espressamente autorizzato dal Titolare del Trattamento.

Art. 29 - Procedure di backup dei dati

1. Sono adottate procedure volte a eseguire le copie di backup dei dati contenuti all'interno delle unità server, delle singole postazioni di lavoro e di tutte le risorse cloud disponibili nell'organizzazione.

2. Le procedure di backup dovranno essere eseguite quotidianamente, mediante l'utilizzo di procedure/software che ne garantiscono l'automatizzazione.

3. Il responsabile del sistema informativo sovrintende sulla corretta esecuzione delle procedure di backup e in particolare verifica semestralmente il corretto funzionamento delle procedure di recovery.

Art. 30 - Distruzione dei dati

1. I supporti di memorizzazione di massa (hard disk, DVD, CD, etc.) destinati allo smaltimento dovranno essere oggetto di preventiva distruzione fisica attraverso sistemi di punzonatura, deformazione meccanica o apertura dell'involucro protettivo con danneggiamento delle superfici atte alla memorizzazione.

2. I supporti di memorizzazione di massa destinati al reimpiego dovranno essere oggetto di preventiva cancellazione dei dati che dovrà avvenire mediante l'utilizzo di software di wiping.

3. Le risorse memorizzate in cloud verranno cancellate definitivamente, compatibilmente con le tecnologie in essere al momento dell'esigenza e in tempi e modalità compatibili con le policy sottoscritte con il fornitore di servizi, nonché della vigente legislazione nazionale ed europea applicabile ai servizi cloud e SaaS.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

Art. 31 - Segnalazioni e reclami

I dati personali raccolti nell'ambito di segnalazioni, reclami o procedimenti istruttori sono trattati esclusivamente per le finalità connesse all'esercizio delle funzioni istituzionali dell'Autorità e nel rispetto delle garanzie previste dalla normativa vigente.

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*

CAPO III
RESPONSABILITÀ E PUBBLICITA'

Art. 32 - Responsabilità in caso di violazione delle disposizioni in materia di privacy

1. Il mancato rispetto delle disposizioni previste dal presente Regolamento comporta la violazione degli obblighi previsti dalla normativa sulla protezione dei dati personali ed espone il Titolare del Trattamento a rischi sul piano delle responsabilità e delle sanzioni a livello civile, amministrativo e, nei casi più gravi, anche penale.

2. La violazione delle disposizioni previste dal presente regolamento e dalla normativa sulla protezione dei dati personali da parte dei soggetti designati/autorizzati al trattamento dei dati per conto dell'Autorità Garante nazionale dei diritti delle persone con disabilità rende possibile contestare il fatto e infliggere i relativi provvedimenti disciplinari previsti dal C.C.N.L. applicato, nonché a fronte di danni economici, la richiesta del conseguente risarcimento.

Art. 33 - Rinvio

1. Per quanto non previsto nel presente regolamento, si applicano le disposizioni stabilite dalla Normativa Applicabile.

2. Il presente regolamento sarà aggiornato a seguito di ulteriori modifiche alla vigente normativa in materia di tutela delle persone fisiche con riguardo alla protezione dei dati personali.

Art. 34 - Entrata in vigore del regolamento e forme di pubblicità

1. Il presente Regolamento è approvato dal Garante nella seduta del 26 marzo 2026 con delibera n.___ del __ _____ ____.

2. Il presente Regolamento è reso pubblico mediante inserimento sul sito istituzionale dell'Autorità Garante nazionale dei diritti delle persone con disabilità ed entra in vigore dalla sua pubblicazione.

Il Collegio:

- avv. Maurizio Borgo _____

- prof. Francesco Vaia _____

- ing. Antonio Pelagatti _____

via Maia, 10 - 00175 Roma
C.F. 96615240585 - tel. 06-83941488
email *segreteria@garantedisabilita.it* PEC *garantedisabilita@pec.it*