Privacy policy

During S.p.A.

DURING S.p.A. – Agenzia per il Lavoro
Sede Legale – Via Giovanni Carlo Cavalli 42, 10138 Torino – tel 011.4335224 – fax 011.4301294
Sede amministrativa – Via Francesco Brioschi 62, 20141 Milano – tel 02.897561 – fax 02.89756188
C.F. e P.IVA 13434210152 REA 959395 TO
Autorizzazione definitiva del Ministero del Lavoro Prot.n.1180 SG del 13/12/2004, Capitale Sociale € 724.011,00 i.v.

Indice

DURING S.p.A. – Agenzia per il Lavoro
Sede Legale – Via Giovanni Carlo Cavalli 42, 10138 Torino – tel 011.4335224 – fax 011.4301294
Sede amministrativa – Via Francesco Brioschi 62, 20141 Milano – tel 02.897561 – fax 02.89756188
C.F. e P.IVA 13434210152 REA 959395 TO
Autorizzazione definitiva del Ministero del Lavoro Prot.n.1180 SG del 13/12/2004, Capitale Sociale € 724.011,00 i.v.

1. PREMESSA

La società During S.p.A. (di seguito, l'"**Organizzazione**") attribuisce grande rilevanza al rispetto della privacy e delle normative sulla protezione dei dati personali al fine del corretto sviluppo delle proprie operazioni, degli affari e della sua immagine sul mercato. La protezione dei dati personali che raccoglie ed archivia, con sistemi elettronici o con modalità tradizionali, rappresenta un valore rilevante e strategico e per lo sviluppo degli affari.

In quest'ottica il Regolamento (UE) 2016/679 (di seguito anche "**GDPR**") rappresenta il fulcro della nuova normativa europea sulla protezione dei dati personali e costituisce la principale base di riferimento per le attività che coinvolgono dati personali nell'ambito dell'UE. La disciplina sulla privacy è poi integrata dalla normativa nazionale e dai provvedimenti dell'Autorità Garante. Per brevità menzioneremo solo il GDPR, intendendo comunque tutta la normativa privacy.

Per questo motivo si rende indispensabile adottare una Privacy Policy (di seguito la "**Policy**") e portare a conoscenza di tutti i dipendenti e di coloro che operano in nome e per conto dell'Organizzazione, i principi e le regole essa intende attenersi allo scopo di garantire un omogeneo ed elevato livello di protezione delle informazioni personali.

Alla luce della complessità della normativa da un lato e dei processi aziendali che coinvolgono i dati personali dall'altro, è preliminarmente necessario dotarsi di una struttura di governance della privacy nell'ambito dell'Organizzazione, definendo l'assetto dei ruoli, delle responsabilità, dei compiti attinenti alla protezione dei dati personali

2. SCOPO

La presente Policy intende descrivere:

(i). i principi e le modalità che l'Organizzazione deve seguire nelle attività di trattamento dei dati personali,
(ii). La gestione privacy e la governance in materia di dati personali, e
(iii). l'attribuzione di compiti e responsabilità dei vari livelli operativi.

Per questo motivo la Policy deve essere portata a conoscenza di tutte le persone che effettuano trattamenti di dati personali nell'Organizzazione.

3. AMBITO DI APPLICAZIONE

La presente Policy deve essere rispettata da parte di tutti i soggetti coinvolti nei trattamenti di dati personali all'interno dell'Organizzazione, a prescindere dal tipo di contratto di lavoro applicabile.
Ogni soggetto autorizzato all'interno dell'Organizzazione deve attenersi alla seguente policy, e deve ovviamente rispettare il GDPR e le normative integrative locali in materia di privacy e protezione dei dati personali, secondo la formazione svolta e, se in dubbio, contattare il DPO.

DURING S.p.A. – Agenzia per il Lavoro
Sede Legale – Via Giovanni Carlo Cavalli 42, 10138 Torino – tel 011.4335224 – fax 011.4301294
Sede amministrativa – Via Francesco Brioschi 62, 20141 Milano – tel 02.897561 – fax 02.89756188
C.F. e P.IVA 13434210152 REA 959395 TO
Autorizzazione definitiva del Ministero del Lavoro Prot.n.1180 SG del 13/12/2004, Capitale Sociale € 724.011,00 i.v.

4. DEFINIZIONI

Ai fini della presente policy, si forniscono le seguenti definizioni derivate dal GDPR in ordine di rilevanza:

- **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.
  Inoltre, in caso di attività di marketing, non richieste dal destinatario (es: invio spontaneo di materiale pubblicitario, vendita diretta, compimento di ricerche di mercato o di comunicazione commerciale), anche qualunque informazione relativa a una persona giuridica - inclusi gli enti o le associazioni -.
  Sono tali ad esempio: dati anagrafici, indirizzi postali, telefonici, telematici, codici identificativi, ordini, fatturato, immagine, voce, curriculum, abitudini di acquisto, log di accesso ai sistemi e, più in generale, tutto quanto risulti registrato su supporto cartaceo o informatico e possa essere associato ad un interessato identificato o identificabile.

- **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.
  Sono tali ad esempio: la gestione delle paghe e delle presenze dei dipendenti, la gestione dei contratti, l'invio di comunicazioni di marketing, la profilazione, la videosorveglianza, etc.

- **Categorie particolari di dati personali**: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o 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 Si tratta di un sottoinsieme dei dati personali.
  Sono tali ad esempio: i certificati di malattia, le iscrizioni al sindacato, i permessi sindacali, le disabilità, gli infortuni, l'appartenenza a un partito, lo stato di salute ecc.

- **Dati personali relativi a condanne penali e reati**: (di seguito "**Dati penali**") dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza. Si tratta di un sottoinsieme dei dati personali.

- **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, come definito dall'art. 4, n.7) del GDPR.
  Ad esempio, se il sito web è gestito interamente dall'Organizzazione, i trattamenti di dati relativi ad esso saranno in capo alla stessa in qualità di titolare.
  Esempio di cattiva prassi: indicare nei documenti il nome del direttore generale o dell'Amministratore delegato come titolare anziché la ragione sociale dell'Organizzazione.

DURING S.p.A. – Agenzia per il Lavoro
Sede Legale – Via Giovanni Carlo Cavalli 42, 10138 Torino – tel 011.4335224 – fax 011.4301294
Sede amministrativa – Via Francesco Brioschi 62, 20141 Milano – tel 02.897561 – fax 02.89756188
C.F. e P.IVA 13434210152 REA 959395 TO
Autorizzazione definitiva del Ministero del Lavoro Prot.n.1180 SG del 13/12/2004, Capitale Sociale € 724.011,00 i.v.

- **Responsabile del trattamento**: come definito dall'art. 4, n. 8) del GDPR, è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento, in conformità all'art. 28 del GDPR.

- **Persona Autorizzata al trattamento**: (anche detta Incaricato) la persona fisica che tratta dati personali sotto l'autorità diretta del titolare o del responsabile, ai sensi dell'art. 29 del GDPR;

- **Interessato**. La persona fisica identificata o identificabile cui si riferiscono i dati personali ai sensi dell'art. 4, n. 1), del GDPR. Inoltre, per le ipotesi di attività di marketing non richieste dal destinatario (es: invio spontaneo di materiale pubblicitario, vendita diretta, compimento di ricerche di mercato o di comunicazione commerciale), interessato è anche la persona giuridica - inclusi enti od associazioni -, come previsto dalla Direttiva (UE) e-privacy 2002/58, e successive integrazioni e modifiche.
  Sono tali ad esempio: i clienti, anche potenziali, i dipendenti, i candidati all'assunzione, i consulenti, i fornitori, i visitatori, gli utenti web dei siti del Titolare, etc..

5. MODELLO ORGANIZZATIVO PRIVACY DELL'ORGANIZZAZIONE

Allo scopo di rendere omogeneo al suo interno le attività di protezione dei dati personali, L'Organizzazione ha deciso di dotarsi del seguente modello organizzativo:

- **Referente privacy**: sinteticamente, ha il compito di coordinare la materia a livello dell'intera Organizzazione e di dare guida funzionale a tutti i soggetti coinvolti nei trattamenti e nella gestione dei dati personali. Un dettaglio delle responsabilità e dei compiti assegnati è riportato nel documento "Nomina a Referente privacy" reperibile **su richiesta al DPO o al Referente privacy stesso** e accessibile dai soggetti apicali coinvolti.

- **Persona autorizzata o incaricato**: è la persona fisica, che esegue materialmente le operazioni di trattamento dei dati, con l'ausilio di strumenti informatici e/o mediante supporti cartacei nell'ambito del reparto aziendale a cui risulta assegnato (questa figura è altresì nota come incaricato del trattamento). L'Organizzazione deve designare Persona autorizzata al trattamento ciascuno dei propri dipendenti che tratti dati personali nell'esecuzione delle sue mansioni. Il documento di designazione a Persona Autorizzata (o Incaricato) con la definizione dell'ambito dei trattamenti consentiti, le istruzioni impartite ed i compiti affidati verrà fornito in modalità cartacea e/o via mail ed è reperibile su richiesta al Referente privacy.

6. ALTRI SOGGETTI COINVOLTI

Nell'ambito della gestione dei dati personali possono essere coinvolti altri soggetti, tra cui:

- **Responsabile del trattamento**: come già visto, è il soggetto esterno che esegue trattamenti di dati personali per conto del titolare. Tali trattamenti devono avvenire sulla base di un contratto scritto che

DURING S.p.A. – Agenzia per il Lavoro
Sede Legale – Via Giovanni Carlo Cavalli 42, 10138 Torino – tel 011.4335224 – fax 011.4301294
Sede amministrativa – Via Francesco Brioschi 62, 20141 Milano – tel 02.897561 – fax 02.89756188
C.F. e P.IVA 13434210152 REA 959395 TO
Autorizzazione definitiva del Ministero del Lavoro Prot.n.1180 SG del 13/12/2004, Capitale Sociale € 724.011,00 i.v.

stipuli la materia disciplinata, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali, le categorie di interessati, gli obblighi e i diritti del titolare. In ambito UE tale contratto deve anche contenere gli elementi essenziali prescritti dall'art. 28, comma 3 del GDPR.
I servizi che tipicamente possono essere esternalizzati a Responsabili sono, ad esempio, la gestione delle paghe, la gestione del sito internet, la gestione del supporto IT, etc.

- **DPO**: il Data Protection Officer (in italiano Responsabile per la protezione dei dati), è una figura prevista dal GDPR all'art. 37 e ss, che una società deve designare ogniqualvolta:
  - le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
  - le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 del GDPR o di dati relativi a condanne penali e a reati di cui all'articolo 10 del GDPR.

  Il DPO ha vari compiti, tra cui quelli di:
  1. informare e fornire consulenza all'Organizzazione nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonché da altre norme nazionali relative alla protezione dei dati;
  2. sorvegliare l'osservanza del GDPR e delle altre norme nazionali relative alla protezione dei dati nonché delle politiche dell'Organizzazione in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
  3. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
  4. cooperare con l'autorità di controllo;
  5. fungere da punto di contatto per l'autorità di controllo.

  L'Organizzazione ha ritenuto necessario nominare un DPO in quanto, vista la sua attività tipica, che per sua natura può comportare rischi in ambito di protezione dei dati personali, data l'attività di trattamento di dati personali potenzialmente su larga scala, e dato il fatto che il trattamento di categorie particolari va ben oltre la semplice gestione del rapporto di lavoro con i propri dipendenti, risulta che sussistano le condizioni di obbligatorietà di nomina cui sopra.

- **Amministratori di sistema**: in Italia è prevista la figura degli Amministratori di Sistema che sono le persone fisiche incaricate della gestione tecnica dell'intero sistema informativo o anche solamente di una sua componente oppure di attività correlate. Tali persone devono ricevere una specifica designazione ad Amministratore di Sistema e specifiche istruzioni.

7. PRINCIPI GENERALI

In relazione al trattamento dei dati personali, l'Organizzazione intende adottare tutte le misure tecnologiche, organizzative e logistiche più adeguate a garantire l'effettivo rispetto delle garanzie di tutela dei dati personali.

DURING S.p.A. – Agenzia per il Lavoro
Sede Legale – Via Giovanni Carlo Cavalli 42, 10138 Torino – tel 011.4335224 – fax 011.4301294
Sede amministrativa – Via Francesco Brioschi 62, 20141 Milano – tel 02.897561 – fax 02.89756188
C.F. e P.IVA 13434210152 REA 959395 TO
Autorizzazione definitiva del Ministero del Lavoro Prot.n.1180 SG del 13/12/2004, Capitale Sociale € 724.011,00 i.v.

A tal fine i processi aziendali e le operazioni materiali di trattamento dei dati effettuati dai dipendenti, Persone autorizzate al trattamento, devono rispettare i seguenti principi.

7.1. **Liceità, correttezza e trasparenza**
Il trattamento dei dati personali deve essere effettuato solo se ricorre una delle condizioni previste dalla legge che lo consentano, solo se l'interessato ne è a conoscenza e corrisponda a quanto dichiaratogli.

7.2. **Limitazione delle finalità**
I dati personali devono essere trattati solo per finalità dichiarate all'interessato, e il trattamento non deve essere incompatibile con tali finalità.

7.3. **Minimizzazione**
L'uso dei dati personali deve essere ridotto al minimo e dunque, se le finalità possono essere raggiunte anche senza l'utilizzo di dati personali il trattamento deve essere effettuato con dati anonimi. I dati anonimi sono i dati che non possono in alcun modo essere associati ad un interessato identificato o identificabile. In particolare, i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

7.4. **Esattezza**
I dati trattati devono essere corretti e mantenuti aggiornati e l'interessato deve poterli verificare e rettificare.

7.5. **Limitazione della conservazione**
I dati personali trattati non vanno conservati per periodi di tempo indeterminati. Essi devono essere cancellati una volta raggiunta la finalità e quindi l'Organizzazione deve determinare dei tempi di conservazione compatibili con le finalità stesse e nel rispetto delle normative locali.

7.6. **Integrità e riservatezza**
L'Organizzazione deve trattare i dati personali in modo da garantire un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.

7.7. **Accountability**
L'Organizzazione deve garantire il rispetto dei principi sopra indicati e deve essere in grado di darne dimostrazione.

8. REGOLE OPERATIVE

In applicazione dei principi sopra descritti e delle ulteriori norme contemplate dal GDPR l'Organizzazione dovrà operare rispettando le seguenti regole operative.

DURING S.p.A. – Agenzia per il Lavoro
Sede Legale – Via Giovanni Carlo Cavalli 42, 10138 Torino – tel 011.4335224 – fax 011.4301294
Sede amministrativa – Via Francesco Brioschi 62, 20141 Milano – tel 02.897561 – fax 02.89756188
C.F. e P.IVA 13434210152 REA 959395 TO
Autorizzazione definitiva del Ministero del Lavoro Prot.n.1180 SG del 13/12/2004, Capitale Sociale € 724.011,00 i.v.

8.1. **Registri delle attività di trattamento**.

L'Organizzazione, tramite i propri Referenti, deve mantenere evidenza dei trattamenti, informatici e manuali, effettuati al suo interno dai vari reparti aziendali. L'Organizzazione deve adempiere a tale obbligo mediante la compilazione dei registri delle attività di trattamento di cui all'art. 30 del GDPR, rispettando le indicazioni fornite in merito dal Garante per la protezione dei dati personali.

La responsabilità di garantire che l'Organizzazione disponga dei registri prescritti dal GDPR e del loro costante aggiornamento è in capo al Referente privacy che, allo scopo, dovrà definire una apposita procedura di gestione, individuando responsabilità e compiti all'interno dell'Organizzazione eventualmente coinvolgendo i soggetti apicali necessari nelle singole funzioni.

In ogni caso, l'aggiornamento dei registri deve avvenire almeno su base annuale.

8.2. **Informativa e raccolta dei dati (*trasparenza e correttezza*).**

Di norma i dati personali sono conferiti direttamente dagli interessati nell'ambito dei normali contatti di lavoro e nell'esecuzione delle attività operative dell'Organizzazione, o tramite il sito Internet, ma possono essere acquisiti anche presso terzi. I dipendenti che raccolgano i dati personali di un interessato dovranno assicurarsi, in occasione della raccolta dei dati, che tale interessato sia adeguatamente informato sugli scopi per cui i dati vengono raccolti e successivamente trattati.

A questo fine devono fornire l'apposito documento di "informativa" predisposto dall'Organizzazione.

L'informativa è sempre dovuta, anche quando non è necessario richiedere all'interessato alcun consenso al trattamento dei suoi dati.

Le operazioni per le quali non sia stata rilasciata una informativa, o che non risultano descritte nell'informativa stessa, sono illecite e dunque non possono essere svolte.

L'informativa va fornita "una tantum" e deve precedere la prima raccolta dei dati di un interessato.

Una nuova informativa va fornita nel caso di variazione di taluni degli elementi indicati in quella precedentemente fornita.

8.3. **Condizioni di liceità del trattamento**

Per ogni finalità elencata nell'ambito dell'informativa deve essere individuata almeno una base giuridica che ne rende lecito il trattamento.

Le basi giuridiche sono quelle indicate all'art. 6 del GDPR per il dati personali "comuni", che consistono, in breve, nelle seguenti alternative:

- Consenso
- Esecuzione del contratto di cui l'interessato è parte
- Esecuzione di un obbligo di legge
- Salvaguardia di interessi vitali
- Esecuzione di un compito di interesse pubblico
- Legittimo interesse (che prevalga sui diritti dell'interessato)

Per quanto riguarda il trattamento di categorie particolari di dati, le basi giuridiche sono indicate all'art. 9 del GDPR, e all'art. 10 per i Dati penali, e sono più restrittive rispetto a quelle dei dati comuni.

Per le **categorie particolari di dati** le basi di liceità specificamente indicate dal GDPR sono le seguenti:

DURING S.p.A. – Agenzia per il Lavoro
Sede Legale – Via Giovanni Carlo Cavalli 42, 10138 Torino – tel 011.4335224 – fax 011.4301294
Sede amministrativa – Via Francesco Brioschi 62, 20141 Milano – tel 02.897561 – fax 02.89756188
C.F. e P.IVA 13434210152 REA 959395 TO
Autorizzazione definitiva del Ministero del Lavoro Prot.n.1180 SG del 13/12/2004, Capitale Sociale € 724.011,00 i.v.

- consenso;
- il trattamento è necessario 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…se autorizzato da diritto o contratto collettivo;
- tutela di un interesse vitale dell'interessato;
- il trattamento da parte di fondazione, associazione o org. senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali;
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario accertare, esercitare o difendere un diritto in sede giudiziaria;
- motivi di interesse pubblico rilevante;
- per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, sulla base del diritto o conformemente al contratto con un professionista della sanità;
- motivi di interesse pubblico nel settore della sanità pubblica;
- archiviazione nel pubblico interesse, di ricerca scientifica o storica.

Per i c.d. **Dati penali**, invece, il trattamento è ammesso soltanto se è autorizzato dal diritto che ne preveda garanzie appropriate per i diritti e le libertà degli interessati.

8.4. **Consenso dell'interessato (*liceità*).**

Tra le basi giuridiche di liceità, è menzionato il consenso dell'interessato. Il consenso non va raccolto se il trattamento si basa su una delle altre condizioni di liceità (come indicato al punto precedente). Tuttavia, taluni trattamenti richiedono necessariamente il consenso come condizione di liceità. Le operazioni di trattamento devono essere conformi a tale consenso rilasciato dall'interessato in risposta all'informativa. Il consenso deve essere liberamente prestato dall'interessato, deve essere raccolto solo a fronte di una idonea informativa e deve essere dimostrabile e non equivoco, e sempre revocabile.
Quando il consenso è necessario per effettuare il trattamento, non è consentito effettuarlo se non è stato ottenuto.

8.5. **Accessibilità ai dati e attività consentite al personale**.

L'accesso ai dati personali e lo svolgimento delle attività di trattamento è consentito solo alle persone che siano state debitamente autorizzate, e abbiano ricevuto debite istruzioni. Queste Persone Autorizzate potranno accedere ai dati solo sulla base di un criterio di 'need to know'. I dati devono essere utilizzati unicamente al fine dello svolgimento della mansione e dei compiti di volta in volta affidati.
Come già indicato in precedenza si sottolinea il fatto che:

- le operazioni per le quali non sia stata rilasciata una informativa, o che non risultano esplicitate nell'informativa stessa, non potranno essere svolte;
- non è consentito effettuare trattamenti per i quali non sia stato ottenuto il consenso, quando necessario.

8.6. **Accessibilità alle categorie particolari di dati ed ai Dati penali e attività consentite al personale.**

Tali dati devono essere trattati solo dalle Persone Autorizzate che ne abbiano stretta necessità, indispensabile per lo svolgimento della loro mansione e specificamente autorizzate a farlo.

DURING S.p.A. – Agenzia per il Lavoro
Sede Legale – Via Giovanni Carlo Cavalli 42, 10138 Torino – tel 011.4335224 – fax 011.4301294
Sede amministrativa – Via Francesco Brioschi 62, 20141 Milano – tel 02.897561 – fax 02.89756188
C.F. e P.IVA 13434210152 REA 959395 TO
Autorizzazione definitiva del Ministero del Lavoro Prot.n.1180 SG del 13/12/2004, Capitale Sociale € 724.011,00 i.v.

In aggiunta ai vincoli, descritti in precedenza, riguardanti la necessità di informativa e di eventuale consenso, si rammenta che le operazioni di trattamento di tali dati devono altresì rispettare anche le condizioni e i limiti fissati dalle normative secondarie.
Ad esempio, le condizioni ed i limiti di trattamento di tali dati sono stabiliti nelle Autorizzazioni Generali emesse dal Garante della privacy, reperibili sul sito del Garante (www.garanteprivacy.it).
Non è consentito quindi effettuare trattamenti in difformità da quanto prescritto nelle normative secondarie.

8.7. **Misure di sicurezza.**
Tutti gli incaricati sono tenuti al rispetto puntuale delle norme in materia di sicurezza predisposte dall'Organizzazione, la cui mancata osservanza può comportare conseguenze giuridiche rilevanti, talvolta anche di natura penale. Il rispetto di talune misure di sicurezza dipende esclusivamente dal comportamento degli incaricati.

8.8. **Circolazione dei dati e comunicazione dei dati a terzi all'interno dell'UE.**
I dati personali possono circolare regolarmente tra le Persone Autorizzate che abbiano la necessità di conoscerli per esigenze di lavoro (*need to know*) e che hanno ricevuto istruzioni in merito. Non devono invece essere trasmessi – o comunque resi accessibili – a terzi esterni all'Organizzazione, salvo che si ricada in una delle seguenti ipotesi:

- la trasmissione al terzo è necessaria per adempiere ad un obbligo di legge o ordine dell'autorità pubblica;
- la trasmissione al terzo è necessaria per eseguire obblighi derivanti da un contratto sottoscritto con l'interessato al quale sono riconducibili i dati personali ;
- qualora il terzo sia stato nominato Responsabile del trattamento, ai sensi dell'art. 28 del GDPR, e i dati siano necessari per l'esecuzione del servizio esternalizzato;
- la persona a cui sono riconducibili i dati abbia rilasciato, in modo esplicito, il proprio consenso alla trasmissione dei dati in questione, a tale Terzo.

Eventuali necessità di trasmissione di dati ad un terzo per ipotesi diverse da quelle appena elencate devono ottenere l'autorizzazione scritta da parte del Referente Privacy in carica.

In ogni caso non rientra nella politica dell'Organizzazione effettuare, a qualsiasi titolo o per qualsiasi finalità, cessione di elenchi, di liste o di indirizzi che si configurino come commercializzazione di dati personali.

8.9. **Trasferimenti di dati personali al di fuori dell'UE**
Il trasferimento dei dati personali al di fuori dell'UE è vietato, salvo che sussista una o più delle seguenti condizioni:

- il paese in questione garantisce un livello di protezione adeguato secondo le decisioni della Commissione Europea (vale a dire Andorra, Argentina, Canada, Isole Faroe, Guernsey, Israele, Isola di Man, Giappone, Jersey, Nuova Zelanda, Svizzera, Uruguay[1]);
- il trasferimento è basato sulle clausole contrattuali standard della Commissione Europea;

[1] Elenco aggiornato al 23.01.2020. Per un elenco più aggiornato consultare il sito della commissione europea (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)

DURING S.p.A. – Agenzia per il Lavoro
Sede Legale – Via Giovanni Carlo Cavalli 42, 10138 Torino – tel 011.4335224 – fax 011.4301294
Sede amministrativa – Via Francesco Brioschi 62, 20141 Milano – tel 02.897561 – fax 02.89756188
C.F. e P.IVA 13434210152 REA 959395 TO
Autorizzazione definitiva del Ministero del Lavoro Prot.n.1180 SG del 13/12/2004, Capitale Sociale € 724.011,00 i.v.

- il trasferimento è necessario all'esecuzione di un contratto concluso tra l'interessato ed il titolare del trattamento, ovvero per eseguire una misura precontrattuale adottata su istanza dell'interessato;
- l'interessato ha manifestato il proprio consenso esplicito, dopo essere stato informato dei possibili rischi collegati al trasferimento dovuti alla mancanza di adeguata protezione dei diritti nel paese di destinazione, e dopo aver preventivamente consultato il Referente Privacy.

Qualora sorgesse la necessità di effettuare un trasferimento che non ricada nei casi sopra indicati, sarà obbligatorio consultare preventivamente il Referente Privacy ed attendere la sua decisione.

8.10. **Nuovi trattamenti e trattamenti con rischi elevati**.

Senza una preventiva autorizzazione, non possono essere iniziati nuovi trattamenti che presentino un rischio elevato, così come definito e disciplinato nella policy aziendale relativa alla valutazione di impatto dei trattamenti previsti sulla protezione dei dati personali (Valutazione di impatto o **DPIA**). I principali elementi da valutare che possono comportare rischi elevati per gli interessati, sono i seguenti:

- Valutazione, assegnazione di un punteggio o profilazione
- Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone fisiche
- Monitoraggio sistematico
- Trattamento di categorie particolari di dati
- Trattamento di dati su larga scala
- Creazione di corrispondenze o combinazione di insiemi di dati
- Trattamento di dati relativi a interessati vulnerabili
- Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative
- Trattamento che in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto"

Oltre a questi elementi, la normativa potrebbe prevedere ulteriori casi di rischio o casi in cui sia obbligatoria la DPIA. Il Garante della privacy ha imposto che la DPIA sia obbligatoria in una serie di casi tra cui, ad esempio, trattamenti non occasionali di dati relativi a soggetti vulnerabili, trattamenti sistematici di dati biometrici, etc. Questa lista aggiornata è disponibile al seguente link: https://www.garanteprivacy.it/documents/10160/0/ALLEGATO+1+Elenco+delle+tipologie+di+trattamenti+soggetti+al+meccanismo+di+coerenza+da+sottoporre+a+valutazione+di+impatto.pdf/b9ceefa9-dd65-df86-fed4-df3c3570f59d?version=1.11.

8.11. **Violazione dei dati personali (Data breach)**

Una violazione di dati personali è definita come "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" (di seguito anche "**Data Breach**").

In caso di Data Breach è fatto obbligo di notificarlo all'Autorità di controllo (Garante locale) entro 72 ore dalla conoscenza dell'avvenuta violazione.

L'Organizzazione si è dotata di una policy di gestione dei Data Breach che deve essere conosciuta e conoscibile da tutte le Persone Autorizzate le quali, al manifestarsi della situazione descritta, devono immediatamente segnalarla al Referente Privacy al fine di rispettare i termini di notifica.

DURING S.p.A. – Agenzia per il Lavoro
Sede Legale – Via Giovanni Carlo Cavalli 42, 10138 Torino – tel 011.4335224 – fax 011.4301294
Sede amministrativa – Via Francesco Brioschi 62, 20141 Milano – tel 02.897561 – fax 02.89756188
C.F. e P.IVA 13434210152 REA 959395 TO
Autorizzazione definitiva del Ministero del Lavoro Prot.n.1180 SG del 13/12/2004, Capitale Sociale € 724.011,00 i.v.

8.12. **Privacy by design e Privacy By Default**

L'Organizzazione si è dotata di una policy di privacy by design e privacy by default che deve essere seguita in caso di sviluppo di nuove applicazioni e nuovi trattamenti, e che dovrà essere resa nota a tutte le Persone Autorizzate coinvolte nella progettazione e nello sviluppo di tali applicazioni e trattamenti.

8.13. **Gestione dei diritti degli interessati**

Il GDPR riconosce i seguenti diritti agli interessati:

- Diritto di accesso ai suoi dati personali (art. 15);
- Diritto di rettifica (art. 16);
- Diritto di cancellazione (diritto all'oblio) (art. 17);
- Diritto di limitazione di trattamento (art. 18);
- Diritto alla portabilità dei dati (art. 20);
- Diritto di opposizione (art. 21);
- Diritto di opporsi a una decisione basata unicamente sul trattamento automatizzato (art. 22);
- Diritto di revocare, in qualsiasi momento, il consenso rilasciato, senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca (art 7.3);

L'Organizzazione si è dotata di una policy per la gestione delle richieste di esercizio dei diritti di cui sopra, illustrandone il contenuto. La policy deve essere conosciuta e conoscibile da ciascuna Persona Autorizzata coinvolta nel processo di gestione di tali richieste. Si ricorda che in assenza di una corretta gestione delle richieste di cui alla policy, l'interessato ha il diritto di proporre reclamo al Garante o agire in sede giudiziale per la tutela dei propri diritti. Si ricorda inoltre che la risposta o riscontro all'interessato deve per forza essere fornito entro un mese.

9. FORMAZIONE

Il GDPR prescrive l'obbligo di rendere consapevoli le Persone Autorizzate dei rischi legati al trattamento di dati personali. L'Organizzazione deve pertanto provvedere a sensibilizzare le Persone Autorizzate fornendo loro una adeguata formazione coerente con la mansione attribuita.
La formazione non potrà essere una tantum ma andrà ripresa su base periodica in particolare in presenza di modifiche normative o nuovi orientamenti interpretativi.
Ai fini della formazione potranno anche essere resi disponibili documenti e presentazioni che illustrano i principali aspetti della normativa, programmi di e-learning, lezioni in aula e sessione di comunicazione etc.

Tale attività formativa deve essere obbligatoriamente documentata (in ossequio al principio dell'Accountability). Ciascun dipendente è tenuto a approfondire la propria conoscenza della materia, al fine di operare nel pieno rispetto della normativa, della presente Policy e delle istruzioni emesse in materia di trattamento dei dati. Eventuali ulteriori necessità di formazione devono essere fatte presenti al Referente Privacy, il quale dovrà provvedere a dare seguito alle richieste.

DURING S.p.A. – Agenzia per il Lavoro
Sede Legale – Via Giovanni Carlo Cavalli 42, 10138 Torino – tel 011.4335224 – fax 011.4301294
Sede amministrativa – Via Francesco Brioschi 62, 20141 Milano – tel 02.897561 – fax 02.89756188
C.F. e P.IVA 13434210152 REA 959395 TO
Autorizzazione definitiva del Ministero del Lavoro Prot.n.1180 SG del 13/12/2004, Capitale Sociale € 724.011,00 i.v.

10. VERIFICHE PERIODICHE

L'Organizzazione, in esecuzione degli obblighi derivanti dal GDPR, dovrà disporre verifiche periodiche**,** anche tramite il Referente Privacy, in merito all'osservanza delle disposizioni del GDPR, delle normative locali, e delle policy, nonché delle istruzioni emesse in materia di trattamento dei dati.
Le verifiche devono essere documentabili. Le Persone Autorizzate sono chiamate a prestare la massima collaborazione per facilitare le verifiche.

11. SANZIONI

La violazione parziale o totale delle disposizioni della normativa privacy può comportare sanzioni di natura penale, civile, e amministrativa previste per i trattamenti illeciti o non conformi alla normativa di riferimento.
Nei casi più gravi, si rammenta che la sanzione amministrativa pecuniaria applicabile ai sensi dell'art. 83 comma 5 del GDPR può arrivare fino a 20.000.000 di Euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Comportamenti illeciti o non conformi alla presente Policy, alle policy dell'Organizzazione ed alle istruzioni emesse in materia di trattamento di dati personali può comportare provvedimenti disciplinari commisurati alla gravità dei fatti.

*** *** ***

DURING S.p.A. – Agenzia per il Lavoro
Sede Legale – Via Giovanni Carlo Cavalli 42, 10138 Torino – tel 011.4335224 – fax 011.4301294
Sede amministrativa – Via Francesco Brioschi 62, 20141 Milano – tel 02.897561 – fax 02.89756188
C.F. e P.IVA 13434210152 REA 959395 TO
Autorizzazione definitiva del Ministero del Lavoro Prot.n.1180 SG del 13/12/2004, Capitale Sociale € 724.011,00 i.v.