

## Contenuti

<b>1. CAMPO D'APPLICAZIONE, SCOPO E DESTINATARI .....</b>	<b>2</b>
<b>DEFINIZIONI .....</b>	<b>2</b>
<b>PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI .....</b>	<b>4</b>
LICEITÀ, CORRETTEZZA E TRASPARENZA .....	4
LIMITAZIONE DELLE FINALITÀ .....	4
MINIMIZZAZIONE DEI DATI .....	4
ESATTEZZA.....	4
LIMITAZIONE DEL PERIODO DI CONSERVAZIONE .....	4
<b>INTEGRITÀ E RISERVATEZZA .....</b>	<b>4</b>
<b>RESPONSABILIZZAZIONE .....</b>	<b>5</b>
RACCOLTA.....	5
USO, CONSERVAZIONE E SMALTIMENTO .....	5
DIVULGAZIONE A TERZI.....	5
TRASFERIMENTO TRANSFRONTALIERO DEI DATI PERSONALI.....	5
DIRITTO D'ACCESSO DA PARTE DEGLI INTERESSATI .....	6
PORTABILITÀ DEI DATI.....	6
DIRITTO ALL'OBLIO.....	6
<b>LINEE GUIDA SUL CORRETTO TRATTAMENTO .....</b>	<b>6</b>
COMUNICAZIONI AGLI INTERESSATI .....	6
OTTENERE I CONSENSI .....	6
<b>ORGANIZZAZIONE E RESPONSABILITÀ .....</b>	<b>7</b>
<b>RISPOSTA AGLI INCIDENTI DI VIOLAZIONE DEI DATI PERSONALI .....</b>	<b>8</b>
<b>AUDIT E RESPONSABILIZZAZIONE.....</b>	<b>8</b>
<b>CONFLITTI CON LA LEGGE.....</b>	<b>9</b>
<b>GESTIONE DELLE REGISTRAZIONI SULLA BASE DI QUESTO DOCUMENTO.....</b>	<b>9</b>
<b>VALIDITÀ E GESTIONE DEL DOCUMENTO .....</b>	<b>9</b>

---

## 1. Campo d'applicazione, scopo e destinatari

Atex Industries S.r.l., in seguito denominata "Azienda", si impegna a rispettare le leggi e i regolamenti applicabili relativi alla protezione dei dati personali nei paesi in cui l'Azienda opera. Questa Politica stabilisce i principi di base con cui l'Azienda tratta i dati personali di clienti, fornitori, partner commerciali, dipendenti e altre persone e indica le responsabilità dei propri enti aziendali e dipendenti durante il trattamento dei dati personali.

I destinatari di questo documento sono tutti i dipendenti, permanenti o temporanei, e tutti i collaboratori che lavorano per conto dell'Azienda.

### Documenti di Riferimento

- Il GDPR dell'UE 2016/679 (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo 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)
- D.Lgs. 196/03 (Codice in materia di Protezione dei Dati Personali)
- Politica di Conservazione dei Dati
- Mappatura delle Attività di Trattamento
- Procedura di Comunicazione di una Violazione di Dati

### Definizioni

#### Enti aziendali coinvolti

AMM = Amministrazione

RU = Risorse Umane

SS = Salute Sicurezza ed Ambiente

COM = Commerciale e Marketing

ACQ = Acquisti

DIR = Direzione (Legale Rappresentante)

Le seguenti definizioni di termini utilizzati in questo documento sono tratte dall'articolo 4 del Regolamento Generale sulla Protezione dei Dati dell'Unione Europea (o GDPR):

**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.

**Dati personali sensibili:** Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Tra tali dati personali dovrebbero essere compresi anche i dati personali che rivelano 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.

**Titolare del trattamento o Controllore dei Dati (le due espressioni saranno utilizzate in maniera equivalente):** 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. Nel caso specifico, il titolare del trattamento è ATEX INDUSTRIES SRL.

**Responsabile del Trattamento o Processore dei Dati (le due espressioni saranno utilizzate in maniera equivalente):** una persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento o Controllore. Nel caso specifico, il responsabile del trattamento è il legale rappresentante di ATEX INDUSTRIES SRL. Possono esserci anche Responsabili esterni del trattamento.

**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.

**Anonimizzazione:** Deidentificazione irreversibile dei dati personali in modo tale che la persona non possa essere identificata utilizzando tempi, costi e tecnologie ragionevoli da parte del Titolare del trattamento (controllore) o di qualsiasi altra persona per identificare l'interessato. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile.

**Pseudonimizzazione:** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile. La pseudonimizzazione riduce, ma non elimina completamente, la possibilità di collegare il dato personale all'interessato. Poiché i dati pseudonimizzati sono comunque dati personali, il trattamento dei dati pseudonimizzati dovrebbe essere conforme ai principi del Trattamento dei Dati Personali.

**Trattamento transfrontaliero:** trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un Titolare del trattamento o Responsabile del Trattamento dei dati nell'Unione ove il Titolare o il Responsabile del Trattamento siano stabiliti in più di uno Stato membro; oppure il trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare o Responsabile del Trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

**Autorità di Controllo:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR dell'UE; per l'Italia il **Garante per la protezione dei dati personali** - Piazza di Monte Citorio, 121 00186 Roma.

**Autorità di Controllo Capofila:** L'autorità di controllo con la responsabilità primaria di gestire un'attività di trattamento di dati transfrontaliera, ad esempio quando un interessato presenta un reclamo in merito al trattamento dei propri dati personali; è responsabile, tra l'altro, di ricevere le notifiche di violazione dei dati, di essere notificato su attività di trattamento rischiose e avrà piena autorità per quanto riguarda le sue funzioni per garantire l'osservanza delle disposizioni del GDPR dell'UE;

Ogni **“autorità di controllo locale”** manterrà comunque nel proprio territorio e monitorerà qualsiasi trattamento di dati locale che incide sugli interessati o che viene effettuato da un Titolare del trattamento o controllore o un Responsabile del Trattamento o processore all’interno dell’Unione oppure all’esterno dell’Unione in caso il loro trattamento si rivolge a interessati residenti sul proprio territorio. I loro compiti e poteri comprendono lo svolgimento di indagini e l'applicazione di misure amministrative e sanzioni, la promozione della consapevolezza da parte del pubblico dei rischi, delle norme, della sicurezza e dei diritti in relazione al trattamento dei dati personali, nonché l'accesso a qualsiasi sede del Titolare del trattamento o controllore e del Responsabile del Trattamento o processore dei dati, compresi eventuali strumenti e mezzi per il trattamento.

**“Gruppo imprenditoriale”**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate.

## Principi Applicabili al Trattamento dei Dati Personali

I principi applicabili alla protezione dei dati delineano le responsabilità delle organizzazioni nella gestione dei dati personali. L'articolo 5(2) del GDPR enuncia che *“il controllore è competente per il rispetto dei principi, e in grado di provarlo.”*

### Liceità, Correttezza e Trasparenza

I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

### Limitazione delle Finalità

I dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.

### Minimizzazione dei Dati

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per cui sono trattati. L'azienda deve applicare l'anonimizzazione o la pseudonimizzazione ai dati personali, se possibile, per ridurre il rischio per gli interessati.

### Esattezza

I dati personali devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

### Limitazione del Periodo di Conservazione

I dati personali devono essere conservati per un arco di tempo sufficiente al conseguimento delle finalità per le quali sono trattati; in particolare, se sussistono rischi concreti per i diritti degli interessati, i dati vanno distrutti una volta raggiunte le finalità del trattamento.

## Integrità e riservatezza

Tenendo conto delle tecnologie e di altre misure di sicurezza disponibili, dei costi di attuazione e la probabilità e gravità dei rischi per i dati personali, l'Azienda deve mettere in atto misure tecniche

e organizzative per garantire un livello di sicurezza adeguato per i dati personali , inclusa la protezione dalla distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati.

## Responsabilizzazione

I Titolari del trattamento o controllori dei dati sono competenti per il rispetto dei principi sopra descritti e devono essere in grado di provarlo.

### Raccolta

L'Azienda deve raccogliere il minor numero di dati personali possibili. Se i dati personali sono raccolti da terzi, l'ente aziendale interessato deve garantire che i dati personali siano raccolti legalmente (RU e/o SS per eventuali dati dei dipendenti o di candidati ad assunzioni, COM per eventuali dati personali dei clienti, ACQ per eventuali dati personali dei fornitori, AMM per i dati che appartengono a tutte le categorie sopra elencate e che sono trattati dal proprio ufficio).

### Uso, Conservazione e Smaltimento

Le finalità, i metodi, il limite di registrazione e il periodo di conservazione dei dati personali devono essere coerenti con le informazioni contenute nell'Informativa sulla Privacy. L'azienda deve mantenere l'esattezza, l'integrità, la riservatezza e la rilevanza dei dati personali in base allo scopo del trattamento. Sono utilizzati adeguati meccanismi di sicurezza volti a proteggere i dati personali per impedire che vengano rubati, utilizzati in modo improprio o abusati e prevenire le violazioni dei dati personali. Gli stessi enti citati al paragrafo precedente sono responsabili della conformità con i requisiti elencati in questa sezione.

### Divulgazione a terzi

Ogni volta che la Società utilizza un fornitore o un partner terzo per il trattamento dei dati personali per suo conto, il Responsabile del Trattamento dei Dati deve garantire che questo processore fornisca misure di sicurezza per salvaguardare i dati personali adeguate ai rischi associati.

In ogni caso, la Società richiede contrattualmente al fornitore o partner commerciale di fornire lo stesso livello di protezione dei dati. Il fornitore o il partner deve trattare i dati personali solo per adempiere ai propri obblighi contrattuali nei confronti dell'Azienda o dietro istruzioni dell'Azienda e non per altri scopi. Quando l'Azienda tratta i dati personali congiuntamente con un terzo indipendente, l'Azienda specifica esplicitamente le responsabilità proprie e quelle del terzo nel relativo contratto o qualsiasi in altro documento legale vincolante, come l' *Accordo con il Fornitore del Trattamento dei Dati*.

### Trasferimento Transfrontaliero dei Dati Personali

Prima dell'eventuale trasferimento di dati personali dallo Spazio Economico Europeo (SEE) devono essere utilizzate misure di protezione adeguate , compresa la firma di un accordo sul trasferimento dei dati, come richiesto dall'Unione Europea e, se necessario, deve essere ottenuta l'autorizzazione della relativa Autorità per la Protezione dei Dati. L'entità che riceve i dati personali deve rispettare i principi del trattamento dei dati personali stabiliti nella Procedura di Trasferimento Transfrontaliero di Dati Personali.

## Diritto d'Accesso da parte degli Interessati

Quando agisce come processore dei dati, l'Ente aziendale coinvolto (RU e/o SS per eventuali dati dei dipendenti o di candidati ad assunzioni, COM per eventuali dati personali dei clienti, ACQ per eventuali dati personali dei fornitori, AMM per i dati che appartengono a tutte le categorie sopra elencate e che sono archiviati dal proprio ufficio) è responsabile di fornire agli interessati un ragionevole meccanismo di accesso per consentire loro di accedere ai propri dati personali e deve consentire loro di far aggiornare, rettificare, cancellare o trasmettere i propri dati personali, se del caso o richiesto dalla legge.

### Portabilità dei Dati

Gli interessati hanno il diritto di ricevere, su richiesta, una copia dei dati che ci hanno fornito in un formato strutturato e di trasmettere tali dati a un altro Titolare del trattamento o controllore, gratuitamente. Il Responsabile del trattamento in collaborazione con il responsabile SI (Sistemi Informativi) garantisce che tali richieste vengano elaborate entro un mese, a patto che non siano eccessive (ad esempio, formulate con alta frequenza di richiesta) e non incidano sui diritti relativi ai dati personali di altre persone.

### Diritto all'oblio

Su richiesta, gli interessati hanno il diritto di ottenere dall'Azienda la cancellazione dei propri dati personali, qualora non siano indispensabili per adempiere agli obblighi di legge o contrattuali. Quando l'Azienda agisce come Titolare del trattamento o Controllore, il Responsabile del trattamento in collaborazione con il responsabile SI (Sistemi Informativi) deve intraprendere le azioni necessarie (comprese le misure tecniche) per informare i terzi che utilizzano o trattano tali dati per conformarsi alla richiesta.

## Linee guida sul Corretto Trattamento

### Comunicazioni agli Interessati

Al momento della raccolta o prima della raccolta di dati personali per qualsiasi tipo di attività di trattamento, inclusa ma non limitata a, la vendita di prodotti, servizi o attività di marketing, l'ente coinvolto (RU e/o SS per eventuali dati dei dipendenti o di candidati ad assunzioni, COM per eventuali dati personali dei clienti, ACQ per eventuali dati personali dei fornitori) è responsabile di informare adeguatamente gli interessati di quanto segue: i tipi di dati personali raccolti, le finalità del trattamento, i metodi di trattamento, i diritti degli interessati riguardo ai loro dati personali, il periodo di conservazione, i potenziali trasferimenti internazionali di dati, se i dati saranno condivisi con terzi e le misure di sicurezza dell'Azienda per proteggere i dati personali. Queste informazioni sono fornite tramite un'Informativa sulla Privacy.

Laddove i dati personali siano condivisi con terzi, il Responsabile del trattamento deve garantire che gli interessati siano stati informati di ciò tramite un'Informativa sulla Privacy.

Nel caso in cui vengano raccolti dati personali sensibili, il Responsabile del trattamento dei Dati deve assicurarsi che l'Informativa sulla Privacy riporti esplicitamente lo scopo per il quale tali dati personali sensibili vengono raccolti.

### Ottenere i Consensi

Ogni volta che il trattamento dei dati personali si basa sul consenso dell'interessato, o su altri motivi legittimi, AMM è responsabile della conservazione di una registrazione di tale consenso. Oltre ad AMM, le seguenti funzioni: RU e/o SS per eventuali dati dei dipendenti o di candidati ad assunzioni, COM per eventuali dati personali dei clienti, ACQ per eventuali dati personali dei fornitori sono responsabili di fornire agli interessati le opzioni per dare il consenso e devono informarli e garantire che il loro consenso (ogni volta che il consenso venga utilizzato come base legale per il trattamento) possa essere revocato in qualsiasi momento.

Laddove la raccolta di dati personali si riferisca a un minore di età inferiore ai 16 anni, AMM/RU deve garantire che il consenso del titolare della responsabilità genitoriale sia fornito prima della raccolta utilizzando il modulo di consenso del titolare della responsabilità genitoriale.

Quando viene richiesto di correggere, modificare o distruggere le registrazioni dei dati personali il Responsabile del trattamento deve garantire che tali richieste siano gestite entro un ragionevole lasso di tempo. AMM deve anche registrare le richieste.

I dati personali devono essere trattati solo per le finalità per cui sono stati originariamente raccolti. Nel caso in cui l'Azienda desideri trattare i dati personali raccolti per un altro scopo, l'Azienda deve richiedere il consenso degli interessati in forma scritta chiara e concisa. Qualsiasi richiesta di questo tipo dovrà includere lo scopo originale per cui sono stati raccolti i dati e anche gli scopi nuovi o aggiuntivi. La richiesta deve includere anche il motivo del cambiamento di scopo / i. Il Responsabile del trattamento dei Dati è responsabile del rispetto delle regole in questo paragrafo.

Ora e in futuro, il Responsabile del trattamento deve garantire che i metodi di raccolta siano conformi alla legge e alle buone pratiche.

## **Organizzazione e Responsabilità**

La responsabilità di garantire un adeguato trattamento dei dati personali spetta a chiunque lavori per o con l'Azienda e abbia accesso ai dati personali trattati dall' Azienda.

Le principali aree di responsabilità per il trattamento dei dati personali sono i seguenti ruoli organizzativi:

**Il legale rappresentante** prende decisioni e approva le strategie generali della Società in materia di protezione dei dati personali.

**Il Responsabile del trattamento dei Dati, in collaborazione con il responsabile dei sistemi informativi**, è responsabile della gestione del programma di protezione dei dati personali ed è responsabile dello sviluppo e della promozione delle politiche di protezione dei dati personali dall'inizio alla fine;

**I Consulenti eventualmente coinvolti, insieme al Responsabile del trattamento dei Dati**, monitorano e analizzano le leggi sui dati personali e le modifiche alle normative, sviluppano i requisiti di conformità e assistono i reparti aziendali nel raggiungimento dei loro obiettivi relativi ai dati personali.

**Il responsabile del sistema informativo (SI)** è responsabile di:

- Garantire che tutti i sistemi, i servizi e le attrezzature utilizzati per la registrazione dei dati soddisfino standard di sicurezza accettabili.

- Condurre controlli e scansioni regolari per garantire che l'hardware e il software di sicurezza funzionino correttamente.

**Il Responsabile del Marketing (COM)**, è responsabile di:

- Approvare qualsiasi dichiarazione sulla protezione dei dati allegata a comunicazioni di marketing commerciale quali e-mail e lettere.
- Se necessario, collaborare con il Responsabile del trattamento dei Dati per garantire che le iniziative di marketing rispettino i principi di protezione dei dati.

**Il Responsabile delle Risorse Umane (RU) e della sicurezza interno (SS)**, ognuno nel proprio ambito, sono responsabili di:

- Migliorare la consapevolezza di tutti i dipendenti sulla protezione dei dati personali degli utenti.
- Organizzare la formazione per la competenza e la sensibilizzazione sulla protezione dei dati personali per i dipendenti che lavorano con dati personali.
- Proteggere i dati personali dei dipendenti dall'inizio alla fine. Deve garantire che i dati personali dei dipendenti vengano trattati in base alle legittime finalità e necessità aziendali del datore di lavoro.

**Il Responsabile del Trattamento** è responsabile del trasferimento delle responsabilità di protezione dei dati personali ai processori esterni e del miglioramento dei livelli di consapevolezza dei processori esterni in materia di protezione dei dati personali, nonché del flusso verso il basso dei dati personali richiesti a qualsiasi processore esterno che l'azienda utilizzi. L'Azienda si riserva il diritto di svolgere un audit presso i processori esterni.

## **Risposta agli incidenti di Violazione dei Dati Personali**

Quando l'Azienda viene a conoscenza di una presunta o effettiva violazione dei dati personali, il Responsabile del trattamento, in collaborazione con il Gruppo di Risposta alle violazioni dei dati, deve eseguire un'indagine interna e adottare misure correttive appropriate in modo tempestivo, in base alla Procedura sulla violazione dei dati. Laddove sussistano rischi per i diritti e le libertà degli interessati, l'Azienda deve informare l'autorità di controllo competente in materia di protezione dei dati senza indebiti ritardi e, ove possibile, entro 72 ore.

## **Audit e Responsabilizzazione**

I responsabili SI e RU sono responsabili di verificare in che modo i reparti aziendali implementino questa politica.

Qualsiasi dipendente che violi questa Politica sarà soggetto ad azioni disciplinari e potrebbe anche essere soggetto a responsabilità civili o penali qualora la sua condotta violasse leggi o regolamenti.



## Conflitti con la Legge

Questa politica è intesa a rispettare le leggi e i regolamenti del luogo di stabilimento e dei paesi in cui Atex Industries S.r.l. opera. In caso di conflitto tra questa Politica e le leggi e i regolamenti applicabili, prevarranno questi ultimi.

### Gestione delle registrazioni sulla base di questo documento

Nome del documento	Luogo di archiviazione	Persona responsabile dell'archiviazione	Controlli per la protezione del documento	Tempo di archiviazione
Modulo di Consenso dell'Interessato	cartella "AMM" nella rete intranet aziendale	Il Responsabile e AMM	Soltanto le persone autorizzate possono avere accesso a cartella e moduli	permanente
Documenti di Recesso dell'Interessato	cartella "AMM" nella rete intranet aziendale	Il Responsabile e AMM	Soltanto le persone autorizzate possono avere accesso a cartella e moduli	permanente
Modulo di Consenso dei Titolari della Responsabilità Genitoriale	cartella "AMM" nella rete intranet aziendale, raccoglitore "Privacy"	Il Responsabile e AMM	Soltanto le persone autorizzate possono avere accesso a cartella e moduli	10 anni
Documenti di Recesso dei Titolari della Responsabilità Genitoriale	cartella "AMM" nella rete intranet aziendale, raccoglitore "Privacy"	Il Responsabile e AMM	Soltanto le persone autorizzate possono avere accesso a cartella e moduli	10 anni
Accordi con i Fornitori del Trattamento dei Dati	cartella "AMM" nella rete intranet aziendale, raccoglitore "Contratti"	Il Responsabile e AMM	Soltanto le persone autorizzate possono avere accesso a cartella e moduli	10 anni dopo la scadenza del contratto

### Validità e gestione del documento

Questo documento ha effetto dal 25/05/2018.

Il responsabile per questo documento è AMM, il quale deve controllare e, se necessario, aggiornare il documento con frequenza almeno annuale. Gli Enti in esso citati hanno la responsabilità di segnalare ad AMM qualsiasi necessità di aggiornamento derivi dai trattamenti di propria competenza.

AMM - Laura Benvenuto

DIR - Enzo Zanchetta