Politica aziendale sulla protezione dei dati personali

STATO DELLE REVISIONI

Rev.	Data	Descrizione delle modifiche	Approvazione
N. 1	12/11/2018	Prima emissione	Dott. Francesco Bizzini Presidente CdA
n.2	19/02/2019	Aggiornamento legale rappresentante	Dott. Fabio Rallo Presidente CdA

Indice

1. Scopo, campo di applicazione e destinatari

Asec S.p.a. (in seguito indicata come: "**Società**" o "**Asec**"), si impegna al puntuale rispetto delle leggi e dei regolamenti applicabili relativi alla protezione dei dati personali.
La presente procedura definisce i principi fondamentali secondo i quali la Società tratta i dati personali di clienti, fornitori, dipendenti ed altri soggetti, ed indica le responsabilità dei propri servizi e dei propri dipendenti nel trattamento dei dati personali.
I destinatari della presente procedura sono tutti i dipendenti e tutti i collaboratori che operano per conto della Società.

2. Riferimenti normativi

- Regolamento (UE) 2016/679 (in seguito indicato come: "**Regolamento**") 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.
- Leggi nazionali, decreto legislativo attuativo del 10.8.2018, n. 101 e Provvedimenti generali del *Garante per la protezione dei dati personali – Autorità di controllo*.

3. Definizioni

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 particolari: dati personali che, per loro natura, sono particolarmente sensibili in relazione ai diritti e alle libertà fondamentali e meritano una protezione specifica in quanto il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Questi dati personali includono dati personali che rivelano origine razziale o etnica, opinioni politiche, credenze religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici che identificano in modo univoco una persona fisica, dati sulla salute o dati relativi all'orientamento sessuale della persona.
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.
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.
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: de-identificazione irreversibile dei dati personali in modo tale che la persona non può essere identificata tramite tecnologie e in tempi e costi ragionevoli né dal titolare né da altra persona. I principi di trattamento dei dati personali non si applicano ai dati anonimi in quanto questi non sono considerati dati personali.

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 del tutto, la possibilità di collegare un dato personale a un interessato. Tenendo conto che i dati che hanno subito il processo di pseudonimizzazione sono ancora dati personali, tale processo deve essere conforme ai principi di 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 nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.

Autorità di controllo: l'autorità pubblica indipendente istituita da ogni Stato membro dell'Unione Europea. In Italia: il *Garante per la protezione dei dati personali*.

4. Responsabilizzazione

L'articolo 5, comma 2 del Regolamento prevede che il Titolare del trattamento – Asec S.p.a. è responsabile del rispetto della normativa sul trattamento dei dati personali e deve essere in grado di comprovarlo.

4.1 Legalità, correttezza e trasparenza

I dati personali devono essere trattati in modo lecito, equo e trasparente nei confronti dell'Interessato – di colui cioè i cui dati personali sono trattati.

4.2 Limitazione della finalità

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

4.3 Minimizzazione dei dati

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per i quali sono trattati. Se possibile per ridurre i rischi per gli interessati la Società deve applicare l'anonimizzazione o la pseudonimizzazione dei dati personali raccolti.

4.4 Esattezza

I dati personali devono essere esatti e, se necessario, aggiornati. Devono essere adottate misure ragionevoli per garantire che i dati personali inaccurati, in relazione alle finalità per cui sono trattati, siano cancellati o tempestivamente rettificati.

Limitazione del periodo di conservazione

I dati personali devono essere conservati per un periodo non superiore a quello necessario alle finalità per i quali i dati personali sono trattati.

4.5 *Integrità e riservatezza*

Tenendo conto dello stato della tecnologia e di altre misure di sicurezza disponibili, dei costi di implementazione e della probabilità e della gravità dei rischi dei dati personali, Asec deve utilizzare misure tecniche o organizzative adeguate per trattare i dati personali in modo tale da garantire la necessaria sicurezza dei dati personali, compresa la protezione contro la distruzione, la perdita, l'alternanza o la divulgazione accidentale o illecita o l'accesso non autorizzato.

5. Implementare la protezione dei dati nell'attività sociale

Al fine di dimostrare la conformità alla normativa in tema di privacy, la Società deve implementare la protezione dei dati personali *day by day*.

5.1 *Raccolta*

La Società deve cercare di raccogliere il minor numero possibile di dati personali. Se i dati sono raccolti da un terzo, Asec deve assicurarsi che i dati siano raccolti secondo le previsioni di legge.

5.2 *Trattamento*

Gli scopi, i metodi, i limiti di archiviazione e il periodo di conservazione dei dati personali devono essere coerenti con le informazioni contenute nell'informativa sulla protezione dei dati resa ai dipendenti, fornitori, clienti, terzi che hanno accesso alla sede legale ed ai navigatori sul sito web di Asec.

La Società deve sempre curare l'accuratezza, l'integrità, la riservatezza e la rilevanza dei dati personali in base alla finalità del trattamento.

È necessario utilizzare adeguati meccanismi di sicurezza volti a proteggere i dati personali per impedire che vengano rubati o utilizzati in modo improprio e prevenire le violazioni dei dati personali.

5.3 *Divulgazione a terzi*

Ogni volta la Società utilizza un terzo soggetto (ad esempio: un consulente del lavoro) per trattare i dati personali per suo conto, il *referente* privacy deve garantire che questo processore garantisca misure di sicurezza di salvaguardia dei dati personali appropriate ai rischi associati. A tal fine, è necessario utilizzare l'apposito questionario di conformità.

Detto terzo deve essere nominato Responsabile del trattamento (in seguito indicato come: "**Responsabile**") ex art. 28 del Regolamento.

Il Responsabile deve trattare i dati personali esclusivamente per adempiere ai propri obblighi contrattuali nei confronti della Società.

Quando Asec tratta i dati personali congiuntamente con un terzo soggetto (ad esempio: un *partner* commerciale), deve specificare esplicitamente le rispettive responsabilità e le modalità di trattamento.

5.4 Trasferimento transfrontaliero dei dati personali

Ad oggi ciò non avviene, prima però di un eventuale futuro trasferimento di dati personali dallo Spazio Economico Europeo dovranno essere utilizzate misure di salvaguardia adeguate, compresa la firma di un accordo sul trasferimento dei dati, come richiesto dall'Unione europea e, se necessario, dovrà essere ottenuta l'autorizzazione da parte del *Garante per la protezione dei dati personali* - Autorità italiana di controllo. L'entità che riceve i dati personali deve rispettare i principi del trattamento dei dati stabiliti nella *procedura* di trasferimento dei dati transfrontalieri.

5.5 Diritti di accesso degli Interessati

Asec è tenuta a fornire agli Interessati un ragionevole sistema di accesso che consenta loro di accedere ai propri dati personali e deve consentire loro di aggiornare, correggere, cancellare o trasmettere i propri dati personali, se del caso o richiesto dalla legge. Il sistema di accesso è dettagliato nella *Procedura di gestione delle richieste di esercizio dei diritti degli Interessati.*

5.6 Portabilità dei dati

Gli Interessati hanno il diritto di ricevere, su richiesta, una copia dei dati che hanno fornito in un formato strutturato e di trasmettere gratuitamente tali dati a un altro titolare.
Asec deve garantire che tali richieste vengano evase entro un mese.

5.7 Diritto all'oblio

Su richiesta, l'Interessato ha il diritto di ottenere dalla Società la cancellazione dei suoi dati personali come da *Procedura di gestione delle richieste di esercizio dei diritti degli Interessati.*

5.8 Informativa agli Interessati

Al momento della raccolta o prima della raccolta di dati personali per qualsiasi tipo di attività di trattamento svolto, Asec deve informare adeguatamente gli Interessati di quanto segue: la tipologia di dati personali raccolti, le finalità del trattamento, i metodi di trattamento, i diritti degli interessati in relazione ai loro dati personali, il periodo di conservazione, i potenziali eventuali futuri trasferimenti internazionali di dati, se i dati saranno condivisi con terzi e le misure di sicurezza adottate dalla Società per proteggere i dati personali.
Il *referente* privacy ha tutti i modelli di *Informativa* necessari per la raccolta dei dati personali inerenti all'attività sociale.
Ogni *Informativa* dovrà specificatamente rendicontare agli Interessati le modalità di trattamento dei dati personali.
Laddove i dati personali siano condivisi con terzi, la Società deve informarne gli Interessati.
Parimenti, laddove in futuro eventualmente i dati personali siano trasferiti in un paese terzo, l'*Informativa* deve specificarlo, indicando chiaramente dove e a quale entità i dati stessi vengono trasferiti.

5.9 Raccolta dei consensi

Ogni qualvolta il trattamento dei dati personali è fondato sul consenso dell'Interessato, la Società deve conservare la copia del consenso raccolto garantendo che possa essere revocato in qualsiasi momento.

Quando viene richiesto di correggere, modificare o distruggere registrazioni di dati personali, il *Referente* Privacy deve garantire che tali richieste siano evase entro un ragionevole lasso di tempo, comunque non oltre un mese di calendario.
I dati personali devono essere trattati solo per le finalità per le quali sono stati originariamente raccolti. Nel caso in cui la Società desideri trattare i dati personali raccolti per un'altra finalità, la Società deve richiedere il consenso degli interessati in forma scritta chiara e concisa. Qualsiasi richiesta di questo tipo deve specificare la finalità originale per cui sono stati raccolti i dati e anche le nuove finalità.

6. Organizzazione e responsabilità

La responsabilità di garantire un adeguato trattamento dei dati personali spetta a chiunque lavori all'interno della Società o per suo conto e abbia accesso ai dati personali da essa trattati.
Le principali aree di responsabilità per il trattamento dei dati personali sono riferibili ai seguenti ruoli organizzativi.
Il **Consiglio di Amministrazione** adotta le decisioni e approva le strategie generali della Società in materia di protezione dei dati personali.
Il **Referente Privacy** monitora e studia la normativa vigente sui dati personali ed assiste i reparti aziendali nel trattamento dei dati personali.
L'**Amministratore di Sistema – Responsabile Ufficio Sistemi Informativi e Qualità** ha la responsabilità di:

- garantire che tutti i sistemi, i servizi e le attrezzature utilizzate per il trattamento e l'archiviazione dei dati personali abbiano standard di sicurezza adeguati;
- effettuare controlli periodici ed esami per verificare il livello di sicurezza dell'hardware e il funzionamento corretto del software.

Il **Responsabile Ufficio Vettoriamento e Misura,** il **Responsabile Ufficio Contabilità e Controllo di Gestione,** il **Responsabile Ufficio Affari Legali,** il **Responsabile Ufficio Segreteria di Presidenza, Sviluppo Business Aziendale ed** il **Responsabile Ufficio Progettazione,** sono responsabili di:

- rilasciare qualsiasi dichiarazione sulla protezione dei dati richiesta durante l'attività sociale.

Il **Responsabile Ufficio delle Risorse Umane** è responsabile di:

- migliorare la consapevolezza di tutti i dipendenti sulla protezione dei dati personali;
- organizzare la formazione per i dipendenti che lavorano con dati personali per aumentarne la competenza e la consapevolezza in materia di protezione dei dati personali.

  Il **Data Protection Officer** è responsabile di adempiere i compiti previsti dall'art. 39 del Regolamento (UE) 2016 / 679.

7. Data breach

Quando Asec viene a conoscenza di una sospetta o reale violazione dei dati personali, il *Referente* Privacy deve, informandone immediatamente il Data Protection Officer, condurre un'indagine interna ed adottare appropriati provvedimenti in maniera tempestiva, secondo quanto previsto dalla procedura per la violazione dei dati. Se ci sono delle minacce ai diritti e alle libertà degli interessati, la Società deve notificarle al *Garante per la protezione dei dati personali* - Autorità di controllo senza alcun ritardo, entro e non oltre 72 ore informandone parimenti anche l'interessato.

8. Responsabilità

Chiunque violerà la presente procedura sarà oggetto di un'azione disciplinare, e se la violazione commessa infrangerà leggi o regolamenti la persona sarà soggetta anche a responsabilità civili e penali.

9. Aggiornamento del presente documento

Il responsabile del presente documento è il *Referente* Privacy, che ha il compito di controllarlo e se necessario, aggiornarlo, almeno annualmente con l'ausilio del Data Protection Officer.

Catania, 19/02/2019

Il Titolare del Trattamento