ACS DOBFAR s.p.a.	**MODELLO ORGANIZZATIVO PRIVACY** **PRINCIPI GENERALI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI** Revisione 29 giugno 2018

INDICE

1. SCOPO E AMBITO DI APPLICAZIONE

Con il presente documento si intendono descrivere la struttura e i principali documenti del Sistema di Gestione Privacy (SGP), sviluppato in conformità alla vigente normativa ed applicabile alla Società quando si è in presenza di trattamento di dati personali. Per dato personale si intende *qualsiasi informazione riguardante una persona fisica identificata o identificabile 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 e sociale.*

Il SGP, finalizzato a ottimizzare i processi connessi al tema della protezione dei dati personali, è stato sviluppato e sarà mantenuto nell'ottica di:

a. garantire che i trattamenti dei dati personali si svolgano nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato;
b. assicurare che i dati siano:
   - trattati in modo lecito, corretto e trasparente;
   - raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo compatibile con tali finalità;
   - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
   - esatti e, se necessario, aggiornati;
   - conservati in una forma che consenta l'identificazione dell'interessato per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
   - trattati in maniera tale da garantire un'adeguata sicurezza, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali, mediante misure tecniche e organizzative adeguate.
c. comprovare – in armonia al principio di c.d. responsabilizzazione – il rispetto dei principi indicati sub b.;
d. individuare e dare forma ai ruoli interni ed esterni deputati alla protezione dei dati personali;
e. perseguire il miglioramento continuo dell'organizzazione e delle prestazioni in materia di protezione dei dati personali;

f. istituire un efficace sistema di controllo per il monitoraggio dell'attuazione del SGP e delle prestazioni in materia di protezione dei dati personali;
g. sviluppare una cultura adeguata in materia di protezione dei dati personali nell'intera organizzazione;
h. sviluppare una capacità di adeguamento continuo all'evoluzione di leggi, regolamenti, norme tecniche e buone prassi.

2. RUOLI PREVISTI

Per l'attuazione della normativa vigente in materia di protezione dei dati personali la Società ha definito i ruoli di seguito descritti.

Titolare

Il Titolare è 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.

Al Titolare sono assegnate le seguenti responsabilità:

- decidere le finalità e le modalità del trattamento dei dati personali;
- garantire che il trattamento dei dati sia lecito, corretto, trasparente e limitato a quanto necessario alle finalità del trattamento;
- effettuare una valutazione preventiva dell'impatto dei trattamenti previsti sulla protezione dei dati personali (DPIA, Data Protection Impact Assessment), in particolare qualora il trattamento preveda l'uso di nuove tecnologie che possano comportare un rischio elevato per i diritti e le libertà delle persone fisiche;
- adottare, se necessario a seguito della DPIA, le misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio, nonché implementare le eventuali prescrizioni dell'Autorità di controllo;
- mettere in atto misure tecniche e organizzative idonee per garantire un livello di sicurezza adeguato al rischio derivante dal trattamento; tali misure possono comprendere, a mero titolo esemplificativo e non esaustivo:

- la pseudonimizzazione e la cifratura dei dati oggetto di trattamento;
- l'applicazione del principio di "privacy by design" che consiste nell'integrare le misure di sicurezza direttamente in applicazioni, servizi e prodotti sin dalla fase di sviluppo e progettazione;
- l'applicazione del principio di "privacy by default" che comprende in particolare la minimizzazione dei dati, la definizione di un periodo di conservazione e l'accessibilità degli stessi;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico e/o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

- in caso di violazione dei dati personali ("data breach"), notificare detta violazione all'Autorità di controllo competente e/o agli Interessati, nei termini e attraverso le modalità stabilite nella *procedura data breach*;
- nominare i Responsabili con atto giuridico, attribuendo a quest'ultimi una serie di obblighi e fornendo loro le istruzioni adeguate;
- assicurare la info-formazione di ogni soggetto autorizzato a trattare i dati personali;
- decidere ed effettuare tutte le spese necessarie, nel rispetto delle procedure aziendali, per adottare le misure organizzative e di sicurezza relative ai dati trattati;
- vigilare sui Responsabili del trattamento nominati e sugli altri soggetti autorizzati al trattamento affinché rispettino le norme e le istruzioni loro impartite;
- garantire all'Interessato l'esercizio dei diritti previsti dalla normativa, quali, ad esempio, il diritto di accesso ai dati trattati, il diritto di rettifica, il diritto all'oblio, il diritto di limitazione di trattamento, il diritto alla portabilità dei dati e il diritto di opposizione al trattamento;
- predisporre e tenere aggiornato il registro delle attività di trattamento;
- predisporre e tenere aggiornato il registro delle violazioni;

- predisporre e tenere aggiornata la documentazione relativa alle scelte tecniche e organizzative effettuate.

Nel caso siano presenti più Titolari del medesimo trattamento, il rapporto di Contitolarità deve essere determinato in modo trasparente attraverso un accordo formale che indichi le diverse responsabilità in merito agli obblighi derivanti dalla normativa.

Responsabile del trattamento

Il Responsabile del trattamento (interno o esterno) è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, individuato e nominato dal Titolare per il trattamento di dati personali per suo conto. Il Titolare può nominare uno o più Responsabili che presentino garanzie tecniche e organizzative adeguate per soddisfare i requisiti normativi. I Responsabili della Società sono nominati tramite contratto o altro atto giuridico, ove è prevista la possibilità per il Responsabile, per quanto concerne i processi di acquisto di beni, servizi e prestazioni, di nominare altri Responsabili del trattamento.

Al Responsabile sono assegnate le seguenti responsabilità:

- trattare i dati personali a fronte di un contratto o altro atto giuridico;
- garantire che le persone autorizzate al trattamento dei dati personali abbiano ricevuto adeguate istruzioni riguardo l'obbligo di riservatezza o abbiano un obbligo legale di riservatezza;
- in analogia a quanto definito per il Titolare, adottare tutte le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato rispetto ad eventuali rischi emersi;
- garantire il supporto al Titolare tramite opportune misure tecniche ed organizzative, per soddisfare le richieste formulate dagli interessati relativamente al trattamento dei propri dati;
- assicurare adeguato supporto al Titolare per garantire il rispetto della normativa vigente riguardo gli obblighi relativi alla sicurezza dei dati personali;

- se fornitore di servizi, su indicazione del Titolare o del Responsabile, cancellare o restituire tutti i dati personali, ivi incluse le copie, a conclusione dei trattamenti attinenti la prestazione del servizio;
- assicurare la disponibilità di tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di legge o definiti dal Titolare / Responsabile e partecipare alle eventuali attività ispettive promosse dal Titolare o da altro soggetto responsabile di tali ispezioni;
- predisporre e mantenere aggiornato il Registro delle attività di trattamento dei dati personali svolti per conto del Titolare / Responsabile;
- assicurare adeguato supporto al Titolare per tutte gli adempimenti necessari in caso di violazione dei dati personali ("Data Breach").

Persona autorizzata al trattamento di dati personali

È la persona fisica autorizzata dal Titolare a compiere operazioni di trattamento dati.

Amministratore di sistema (AdS)

È la figura professionale, in ambito informatico, dedicata alla gestione e alla manutenzione di sistemi con cui vengono effettuati trattamenti di dati personali, compresi – a mero titolo esemplificativo - i sistemi di gestione delle basi di dati, i sistemi di software complessi quali i sistemi ERP utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

3. UFFICI COINVOLTI

I principali Uffici coinvolti nelle attività di trattamento e nella corretta applicazione del SGP sono:

- **ICT Department:**
  - individua, progetta e realizza le soluzioni tecniche e identifica le prassi operative cui devono ottemperare gli utilizzatori dei sistemi informativi;

- collabora con il Titolare ai fini dell'identificazione delle più idonee misure di sicurezza informatiche;
- partecipa al processo di gestione del Data Breach, per quanto compete i dati presenti sui sistemi informatici;
- si impegna a diffondere a livello dipartimentale la cultura relativa alla corretta gestione e protezione dei dati personali.

- **Health Safety & Security Department:**
  - si impegna a tutelare i dati trattati durante le proprie attività di controllo e tutela e per ogni attività svolta;
  - si impegna a diffondere a livello dipartimentale la cultura relativa alla corretta gestione e protezione dei dati personali.

- **Pharmacovigilance Department:**
  - si impegna a tutelare i dati presenti nelle segnalazioni di reazioni avverse e nelle restanti attività svolte;
  - si impegna a diffondere a livello dipartimentale la cultura relativa alla corretta gestione e protezione dei dati personali.

- **HR& Payroll Department:**
  - si impegna a tutelare i dati trattati durante le attività di propria competenza;
  - si impegna a diffondere a livello aziendale e dipartimentale la cultura relativa alla corretta gestione e protezione dei dati personali.

- **Altri Uffici:**
  - ogni Ufficio, sulla base della propria competenza e responsabilità, collabora al processo di protezione dei dati personali delle persone fisiche e applica i principi inclusi nel presente Modello organizzativo segnalando eventuali ambiti di miglioramento;
  - ogni responsabile di ufficio/dipartimento si impegna a diffondere all'interno del proprio ambito di responsabilità la cultura relativa alla corretta gestione e protezione dei dati personali.

4. INDIRIZZI GENERALI E PROCESSO DI GESTIONE DELLA PROTEZIONE DEI DATI

Le attività di gestione della protezione delle persone fisiche con riguardo al trattamento dei dati personali si sviluppano secondo alcuni processi che, attraverso l'interazione tra gli Uffici, contribuiscono a sostenere l'architettura complessiva del Sistema di Gestione Privacy, come di seguito illustrato:

- l'Ufficio HR redige ed aggiorna il Modello organizzativo Privacy;
- il Titolare è responsabile del processo di aggiornamento delle nomine dei Responsabili e della definizione dei relativi compiti e responsabilità;
- ogni Responsabile nominato, in collaborazione con l'Ufficio HR, è responsabile del processo di definizione dei ruoli (es. Amministratori di Sistema, persone autorizzate al trattamento) e della definizione dei relativi compiti e responsabilità;
- ogni Ufficio, per quanto di propria competenza, detiene il registro dei trattamenti ed è responsabile del suo aggiornamento;
- ogni Ufficio, per quando di propria competenza, predispone le procedure operative necessarie alla gestione dei dati personali, ad eccezione delle procedure d'ambito tecnico-informatico, predisposte dall'Ufficio ICT. Tutte le procedure vengono sottoposte all'approvazione del Titolare che ha il compito di emetterle e di comunicarne il contenuto a tutti i soggetti tenuti alla loro applicazione ed al loro rispetto.
- in caso di attivazione di un nuovo progetto che abbia un impatto sul tema privacy, il Titolare deve individuare un referente di progetto che possa supportarlo relativamente alla valutazione preliminare di impatto dei trattamenti dei dati personali e nell'individuazione delle eventuali azioni da intraprendere.

5. SISTEMA DOCUMENTALE

Le disposizioni previste dal presente Modello Organizzativo Privacy si integrano con quelle previste dai seguenti, ulteriori documenti:

a) Procedure
   - Information Security Policy
   - Procedure operative:

   1) Registro dei trattamenti
   2) Esercizio dei diritti degli interessati
   3) DPIA - Data Protection Impact Assessment
   4) Data Breach

È compito di ogni Ufficio, per quanto di propria competenza, mantenere aggiornate le Procedure Organizzative.

b) Documenti di nomina
   - Nomina dei Responsabili del trattamento

È compito dell'Ufficio HR archiviare le nomine dei Responsabili del trattamento.

c) Documenti di informazione e formazione
   - Istruzioni per le persone autorizzate al trattamento
   - Certificazioni di avvenuta fruizione di un corso

È compito di ogni Ufficio, per quanto di propria competenza, definire e mantenere aggiornate le Istruzioni per le persone autorizzate al trattamento.