Data Protection Master Policy

Data di emissione e decorrenza	***10 settembre 2020***
Numero revisione	***Rev. 02***
Revisione	
Preparata da	***ConsulenzeDPO***
Controllata da	***Referente privacy – Sara Anguilla***
Approvata da	***Emmanuele Adami***

Questo documento è di proprietà di JakinFarma S.r.l. che tutelerà i propri diritti in sede civile e penale a termini di legge

Sommario

1. INTRODUZIONE 3

1.1 NORMATIVA APPLICABILE 3
1.2 SCOPO 3
1.3 DESTINATARI E CONSEGUENZE IN CASO DI MANCATO RISPETTO DELLA *POLICY* 4

2. DEFINIZIONI 4

3. LE REGOLE GENERALI DEL TRATTAMENTO 7

3.1 IL PRINCIPIO DI *ACCOUNTABILITY* 7
3.2 *I PRINCIPI GENERALI DA RISPETTARE NEL TRATTAMENTO DEI DATI 7*
3. 3 PRINCIPI DA ATTUARE NELL'ORGANIZZAZIONE DEL TITOLARE 8

4. LA *PRIVACY GOVERNANCE* AZIENDALE 9

4.1 IL TITOLARE ED IL REFERENTE *PRIVACY* 9

4.2 I SOGGETTI AUTORIZZATI AL TRATTAMENTO *(NDR: LA DENOMINAZIONE DI QUESTI SOGGETTI, CORRISPONDENTI ALLA FIGURA DEGLI INCARICATI DI CUI ALL'ABROGANDO CODICE PRIVACY, PUÒ ESSERE CONCORDATA CON LA SOCIETÀ A SECONDA DELLE SUE ESIGENZE)* 9

4.3 IL DATA PROTECTION OFFICER (DPO) – *(NDR: IL PRESENTE PARAGRAFO ANDRÀ RIVISTO IN BASE AI CONCRETI COMPITI AFFIDATI AL DPO, SOPRATTUTTO SE SI TRATTERÀ DI DPO DI GRUPPO).* 9
4.4 IL RUOLO E LA SCELTA DEI RESPONSABILI 10

5. GLI INTERESSATI 11

5.1 TRATTAMENTO NEI CONFRONTI DI PROSPECT E DEI CLIENTI 11
5.1.1 L'informativa 11
5.1.2 Il consenso 12
5.13 I diritti del Prospect/Cliente 13
5.2 TRATTAMENTO NEI CONFRONTI DI DIPENDENTI, COLLABORATORI E CANDIDATI 13
5.2.1 L'Informativa Candidati 14
5.2.2 L'Informativa Dipendenti e Collaboratori 14
5.2.3 Il consenso 16
5.2.4 Il Regolamento per l'utilizzo degli strumenti aziendali 17
5.2.5 I diritti dei Dipendenti e Collaboratori 17
5.3 I TERZI 17
5.3.1. L'Informativa 18
5.3.2 I diritti dei Terzi 19

6. GLI STRUMENTI DI TRATTAMENTO 19

6.1 IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DEL TITOLARE 19
6.2 *DATA BREACH* 19
6.3 *DATA PROTECTION IMPACT ASSESSMENT* (DPIA) 17

7. LA GOVERNANCE IT 20

7.1 I principi del GDPR 20

1. Introduzione

1.1 Normativa applicabile

La *Data Protection Master Policy* (di seguito "Policy") della società JakinFarma S.r.l. (di seguito, anche la "Società") è adottata in attuazione del *Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al Trattamento "General Data Protection Regulation*" - di seguito GDPR - nonché ai recenti provvedimenti (D.lgs. 101 del 10 agosto 2018) "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016"* che armonizza il codice per la protezione dei dati personali, comunemente noto anche come "*Codice della Privacy*" (D.lgs. 196 del 30 giugno 2003).

Il GDPR prevede una disciplina uniforme in tema di *privacy*, valida in tutta l'Unione Europea, e ha lo scopo di assicurare all'interno della stessa un livello coerente ed elevato di protezione e la rimozione degli ostacoli alla circolazione dei Dati Personali.

Il GDPR è entrato in vigore il 24 maggio 2016 senza necessità di recepimento per mezzo di atti nazionali ed è applicabile in tutti i Paesi UE a partire dal 25 maggio 2018[1]. L'Autorità Garante per la Protezione dei Dati Personali (di seguito il "**Garante**") ha adottato il 28 aprile 2017 una prima "*Guida all'applicazione del Regolamento europeo in materia di protezione dei Dati personali*", successivamente aggiornata (di seguito "**Guida all'applicazione del GDPR**").

La *Policy* è quindi redatta tenuto conto delle disposizioni del GDPR nonché delle Linee Guida e dei Provvedimenti del Garante che resteranno in vigore (di seguito la **"Normativa Vigente"**) anche in considerazione del Decreto legislativo del 10 agosto 2018 n. 101, *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679".*

1.2 Scopo

Lo scopo della *Policy* è quello di fornire il quadro relativo all'attuazione del GDPR all'interno della Società. A tal riguardo, ai fini della predisposizione della *Policy* stessa, la Società ha condotto una attività di *Risk Assessment* che si è conclusa con la formalizzazione di un *report* che ha dato evidenza dello stato di adeguamento al Codice *Privacy*, del livello di maturità rispetto al *GDPR*, dei relativi *gap* riscontrati e del conseguente *action plan* (di seguito il **"*Risk Assessment*"**).

Alla luce degli esiti di tale attività, la Società ha pertanto ritenuto, nell'ottica dell'*accountability*, di dotarsi di processi e procedure *privacy* di seguito descritta.

Inoltre, la Società, che svolge l'attività correlate al business di servizi di outsourcing per le medie e grandi aziende farmaceutiche, sulla base delle risultanze dell'attività di *Risk Assessment* condotte nel suddetto periodo, ha adottato un *set* di documenti conformi al GDPR (informative, nomine a responsabili, *policies*

[1] Benché formalmente il GDPR non abbia necessità di norme di attuazione per poter essere applicabile in Italia, il legislatore dovrà comunque emanare delle norme di coordinamento, con particolare riferimento a quanto previsto dalla Legge di Delegazione Europea n. 163/2017. La presente *Policy*, pertanto, potrebbe subire modifiche alla luce di quando sarà previsto nella suddetta norma di coordinamento, nonché a seguito di eventuali ed ulteriori linee guida attuative del GDPR.

varie, *etc*.) messi a disposizione dei Destinatari, come di seguito definiti, con le modalità specificate nel prosieguo.

In tal senso la *Policy* fornisce, altresì, indicazioni in merito a come viene disciplinato il Trattamento (come di seguito definito) di Dipendenti, Clienti e Fornitori, nonché di altri soggetti eventualmente Interessati, da parte della Società, "disegnato" sulla base del proprio *business*, come identificato nelle tabelle del paragrafo 5, tramite l'indicazione di regole interne conformi alle disposizioni del GDPR. La Società provvede al trattamento nell'ambito del perseguimento dei propri scopi, come risultanti dall'oggetto sociale, nei limiti e secondo le regole previste nella *Policy* e nei relativi allegati.

1.3 Destinatari e conseguenze in caso di mancato rispetto della *Policy*

Le regole ed istruzioni contenute nella Policy sono rivolte a tutti i Dipendenti, stagisti, lavoratori somministrati e collaboratori a qualsiasi titolo della Società.

A tal fine si considerano:

- ✓ Dipendente/i: un dipendente, un candidato o un precedente dipendente della Società, inclusi i lavoratori temporanei che hanno prestato attività lavorativa sotto la diretta supervisione della stessa (quali, a titolo esemplificativo, tirocinanti, somministrati, distaccati). La presente definizione non include i consulenti che prestano la propria attività presso la Società, né i dipendenti di soggetti terzi che forniscono servizi in suo favore.
- ✓ Collaboratore/i: soggetti che collaborano con la Società, a prescindere dal rapporto contrattuale (es. agenti non dipendenti, consulenti, professionisti).

La non ottemperanza delle disposizioni contenute nella Policy stessa potrà determinare l'applicazione da parte della Società di restrizioni considerate appropriate, nonché l'applicazione da parte della stessa:

- ✓ dei provvedimenti disciplinari a carico dei Dipendenti previsti dal contratto collettivo nazionale di lavoro;
- ✓ della risoluzione del contratto e delle azioni civili e penali stabilite dalla legge, nei confronti dei Collaboratori.

2. Definizioni

Ai fini della *Policy* vengono definiti i seguenti termini, la cui definizione non corrisponde necessariamente per ragioni di maggior chiarezza a quella indicata dal GDPR.

Dati

- **Dati Personali:** qualsiasi informazione riguardante una persona fisica identificata o identificabile. L'identificazione della persona fisica può avvenire, direttamente o indirettamente, tramite Dati quali: nome, un numero di identificazione, Dati relativi all'ubicazione, elementi caratteristici dell'identità

fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Esempio di Dati che identificano direttamente: nome per esteso, indirizzo email, codice fiscale. Esempio di Dati che identificano indirettamente: indirizzi IP, targa di moto/autoveicoli.

- **Categorie Particolari di dati:** dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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.
- **Dati biometrici:** dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
- **Dati relativi alla salute:** dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
- **Dati personali relativi a condanne penali e reati:** informazioni relative a reati attribuiti o a condanne penali subite da una persona fisica, nonché qualsiasi altra informazione ritenuta sensibile ai sensi di legge.
- **Dati:** Dati Personali, Categorie Particolari di dati e dati relativi a condanne penali e reati considerati congiuntamente.

Soggetti

- **Titolare:** la persona (fisica o giuridica), l'autorità pubblica, o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento.
- **Responsabile:** la persona (fisica o giuridica), l'autorità pubblica, il servizio o qualsiasi altro organismo, esterno alla Società, che tratta Dati Personali per conto del Titolare del Trattamento, ai sensi dell'art. 28 del GDPR.
- **Subresponsabile:** la persona (fisica o giuridica) nominata dal Responsabile per specifiche attività di Trattamento, nel rispetto degli stessi obblighi contrattuali che legano Titolare e Responsabile.
- **Interessato/Interessati:** la persona fisica cui si riferiscono i Dati Personali.
- **Referente Privacy:** la persona fisica nominata dalla Società in qualità di soggetto di riferimento interno dedicato al governo delle politiche relative al trattamento Dati Personali.
- **Persona Autorizzata al trattamento dei dati personali**: Persona Autorizzata al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Referente Privacy del trattamento.
- **Persona Incaricata del trattamento dei dati:** Persona Incaricata all'acquisizione dei dati c/o i clienti ed Autorizzata al trattamento dei dati personali nello svolgimento di una specifica attività sotto l'autorità diretta del Titolare o del Referente Privacy.

- **DPO:** il Data Protection Officer[2] soggetto nominato dalla Società in qualità di Responsabile della protezione dei Dati, qualora sussistano i requisiti previsti dall'articolo 37 del GDPR.
- **Amministratori di Sistema:** figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei Dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, secondo la definizione del Provvedimento del Garante del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (di seguito "Provvedimento ADS").
- **Garante Europeo:** l'autorità di sorveglianza indipendente che ha il compito di garantire che le istituzioni e gli organi dell'Unione Europea rispettino il diritto alla protezione dei dati in sede di Trattamento e di elaborazione di nuove politiche.
- **Autorità di Controllo:** indica l'autorità pubblica indipendente istituita da uno Stato membro dell'Unione Europea.
- **Garante:** Garante per la protezione dei dati personali. Indica l'Autorità di Controllo italiana.
- **Personale**: si riferisce, indistintamente, a Dipendenti e Collaboratori.

Modalità e strumenti a presidio del Trattamento

- **Trattamento:** trattamento dei Dati, ossia qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati o insiemi di Dati i. Il Trattamento può svolgersi mediante 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.
- **Limitazione del Trattamento:** l'operazione con cui si contrassegnano alcuni Dati Personali trattati, con l'obiettivo di limitarne il Trattamento in futuro.
- **Profilazione:** qualsiasi forma di Trattamento automatizzato, con cui i Dati vengano utilizzati per valutare determinati aspetti di una persona fisica, in particolare per analizzare o prevedere il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti.
- **Anonimizzazione:** modalità di Trattamento effettuata in modo tale che i Dati non possano più essere attribuiti a un soggetto specifico in quanto viene rimosso qualsiasi elemento riconoscibile che possa permettere a tali informazioni combinate di risalire al suddetto soggetto identificandolo.
- **Pseudonimizzazione:** modalità di Trattamento effettuata in modo tale che i Dati non possano più essere attribuiti a un soggetto specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e

[2] (individuato nella traduzione italiana del Garante anche"Responsabile Protezione dei Dati"),

organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile.

- **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.
- **Violazione dei Dati Personali ("Data Breach"):** una violazione in termini di sicurezza che comporti 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.
- **DPIA (acronimo di Data Protection Impact Assessment):** valutazione d'impatto sulla protezione dei dati.

3. Le regole generali del Trattamento

3.1 Il principio di *accountability*

Il GDPR impone un cambio di prospettiva ed un ruolo maggiormente attivo da parte dei Titolari nel Trattamento. In questo senso viene introdotto il concetto di "*accountability*" che si riferisce alla responsabilizzazione del Titolare stesso che deve farsi carico in prima persona di garantire il rispetto delle disposizioni a tutela dei Dati. Il Garante, nella Guida all'applicazione del GDPR, precisa che il Titolare deve attuare dei "*comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento*". La novità di questo principio consiste nell'attribuzione al Titolare del compito di decidere autonomamente le modalità, le garanzie e i limiti del Trattamento nel rispetto della Normativa Vigente.

Queste valutazioni devono essere svolte prima di procedere al Trattamento vero e proprio: è necessaria quindi un'analisi preventiva da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

A tal proposito la Società, come anticipato sopra, si è attivata mediante esecuzione di un *Risk Assessment* per conformare le procedure aziendali al GDPR.

Tutti i Destinatari devono essere pienamente consapevoli delle implicazioni connesse al Trattamento e delle regole di cui la Società stessa si è dotata al fine garantire una adeguata tutela dei Dati stessi.

Nella gestione e manutenzione del modello privacy di cui la Società si è dotata, quest'ultima ha individuato nel Referente Privacy il compito di rivedere periodicamente – e comunque almeno una volta all'anno – lo stato di attuazione della Normativa Vigente utilizzando a tal fine il file di *Risk Assessment.*

Al *Referente Privacy* è attribuito il compito di redigere/rivedere la documentazione in materia di data protection (informative, clausole contrattuali, Data Processing Agreement etc.) – anche tramite consulenti incaricati dalla Società – nonché di tenere l'archiviazione della suddetta documentazione e dei relativi aggiornamenti, anche in un database dedicato.

3.2 I principi generali da rispettare nel trattamento dei Dati

In estrema sintesi, i principi generali posti alla base di qualsiasi Trattamento, secondo il GDPR, sono:

a) liceità, correttezza e trasparenza: i Dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato. Il principio di liceità e correttezza prevede che i Dati di un Interessato possano essere trattati solo se questi: (i) ha espresso il proprio consenso al Trattamento per una o più specifiche finalità, (ii) quando il Trattamento è necessario all'esecuzione di un contratto di cui l'Interessato è parte, (iii) quando il Trattamento è necessario per adempiere un obbligo legale a cui è soggetto il Titolare; (iv) quando il Trattamento è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica (v) quando è necessario per l'esecuzione di un compito di interesse pubblico o per il perseguimento del legittimo interesse del Titolare. Inoltre, in omaggio al principio di trasparenza, le modalità con cui sono raccolti e utilizzati i Dati devono essere trasparenti e le informazioni e comunicazioni relative al Trattamento devono esser altresì facilmente accessibili e comprensibili;

b) limitazione della finalità: i Dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo che il relativo Trattamento non sia incompatibile con tali finalità. È considerato compatibile con le finalità inziali un ulteriore Trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;

c) minimizzazione dei Dati: i Dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati: il Trattamento deve avere ad oggetto solo la quantità di Dati necessari per eseguire correttamente una determinata attività. Inoltre, i Dati raccolti per uno scopo non possono essere trattati per un altro scopo senza prima acquisire lo specifico consenso da parte dell'Interessato. La Società deve quindi limitare la raccolta, l'archiviazione e l'utilizzo dei Dati a quelli rilevanti, adeguati e assolutamente necessari per l'esecuzione dello scopo per il quale i dati vengono trattati;

d) esattezza: i Dati 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;

e) limitazione della conservazione: i Dati devono essere conservati in una forma che consenta l'identificazione degli Interessati per un arco di tempo non superiore al tempo strettamente necessario al conseguimento delle finalità per le quali sono trattati. I Dati possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR a tutela dei diritti e delle libertà dell'Interessato;

f) integrità e riservatezza: i Dati devono essere trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate per proteggerli da Trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale.

3. 3 Principi da attuare nell'organizzazione del Titolare

In base all'art. 25, è necessario rispettare i principi che seguono:

a) Privacy by design (o 'fin dalla progettazione'): tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal Trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il Titolare mette in atto misure tecniche e organizzative adeguate, quali ad esempio la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli Interessati (art. 25, par. 1 GDPR).

b) Privacy by default (o 'per impostazione predefinita'): il Titolare mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del Trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza un intervento individuale (art. 25, par. 2 GDPR).

4. La *Privacy Governance* Aziendale

4.1 Il Titolare ed il Referente *Privacy*

Ai fini dell'applicazione del GDPR la Società è Titolare dei Dati trattati nello svolgimento delle proprie attività e contenuti nelle relative banche dati, sia su supporto elettronico che cartaceo.

Il Titolare ha conferito alla Dott.ssa Sara Anguilla, con verbale del Consiglio di Amministrazione del 01 settembre 2020, la delega in materia di privacy, conferendole i conseguenti poteri necessari all'adempimento degli obblighi previsti dalla Normativa Applicabile, compreso il potere di designare e preporre al trattamento dei Dati uno o più soggetti autorizzati, nonché i Responsabili.

4.2 I soggetti Autorizzati al Trattamento

Il GDPR, all'art. 29, precisa che chiunque agisca sotto l'autorità del Titolare e che abbia accesso ai Dati non può procedere al relativo Trattamento se non è debitamente istruito in tal senso dal Titolare medesimo.

Il Referente Privacy ha il compito di consegnare formalmente all'Autorizzato o all'Incaricato al Trattamento le istruzioni specifiche per il tipo di attività che quest'ultimo dovrà svolgere sui dati.

A tal fine, il Referente Privacy dovrà utilizzare il *template* di istruzioni allegato alla presente procedura e denominato "*JAKINFARMA_Istruzioni Persona Autorizzata o Incaricata*".

4.3 Il Data Protection Officer (DPO)

Il GDPR individua una nuova figura nell'ambito del governo della privacy (artt. 37-39 del GDPR) che dovrà:

- Informare e fornire consulenza al Titolare e al Responsabile in merito agli obblighi derivanti dalla Normativa Vigente;

- Sorvegliare l'osservanza del GDPR da parte del Titolare e dei Responsabili, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa al Trattamento;
- Fornire su richiesta pareri in merito alla valutazione d'impatto e sorvegliarne lo svolgimento;
- Cooperare con il Garante fungendo, tra l'altro, da punto di contatto per questioni connesse al Trattamento, effettuando consultazioni di ogni tipo, con particolare riguardo e attenzione ad un'eventuale attività di consultazione preventiva.

La funzione del DPO può essere ricoperta da un soggetto con conoscenze specialistiche della normativa e delle prassi in materia di protezione dei Dati. Il DPO deve essere scelto in base alle sue qualità professionali ed alla sua preparazione in relazione alle operazioni di Trattamento, sia sul piano teorico che su quello pratico. Questa figura può essere scelta tra i Dipendenti che non siano coinvolti in attività di Trattamento della Società oppure può essere un libero professionista, esterno e autonomo, incaricato in base a un contratto di servizi. Il GDPR prevede che il DPO debba essere obbligatoriamente nominato dal Titolare in tre occasioni:

1. Quando il Trattamento è effettuato da un'autorità pubblica o da un organismo pubblico (ad eccezione delle autorità giurisdizionali nell'esercizio delle loro funzioni);
2. Quando le attività principali del Titolare o del Responsabile consistono in Trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli Interessati su larga scala;
3. Quando le attività principali del Titolare o del Responsabile consistono nel Trattamento su larga scala, di Categorie particolari di dati personali (art. 9) o di Dati relativi a condanne penali e reati di cui all'articolo 10 GDPR.

In tutti gli altri casi la nomina del DPO è comunque facoltativa da parte del Titolare.

4.4 Il ruolo e la scelta dei Responsabili

Qualora il Trattamento debba essere effettuato per conto della Società da un soggetto ad essa terzo si procede a formalizzare con un contratto la nomina di quest'ultimo ai sensi dell'art. 28 del GDPR.

Questi soggetti devono offrire garanzie di esperienza, capacità ed affidabilità circa l'osservanza della Normativa Vigente nonché circa l'affidabilità sull'ottemperanza alle istruzioni ricevute.

Il Referente Privacy dovrà valutare la necessità di nominare un fornitore Responsabile e conseguentemente gestire la formalizzazione del contratto con il fornitore esterno nonché la sottoscrizione dell'accordo sul Trattamento.

Per formalizzare la nomina dovrà essere utilizzato il template di nomina denominato "*JAKINFARMA_ Nomina Responsabile del trattamento dei dati*" disponibile presso l'ufficio del Referente Privacy.

Nella scelta di un Fornitore sarà necessario di volta in volta verificare la nomina a Responsabile al trattamento utilizzando la *check list* denominata "*JAKINFARMA_Checklist Data Processing Agreement*".

5. Gli Interessati

Il GDPR, all'art. 6, prevede che il Trattamento è lecito ove sussista una delle seguenti condizioni:

a) L'Interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) Il Trattamento è necessario all'esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) Il Trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare;

d) Il Trattamento è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;

e) Il Trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare;

f) Il Trattamento è necessario per il perseguimento del legittimo interesse del Titolare 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.

Sulla base del proprio business, la Società ha individuato, quali basi giuridiche del Trattamento, quattro categorie illustrate alle tabelle del successivo paragrafo (contratto, consenso, normativa, legittimo interesse), che rispettivamente si riportano alle lettere a), b), c), f).

Le categorie di Interessati sono:

- Clienti (clienti (Classe Medica, degli Operatori Sanitari e dei Farmacisti Ospedalieri e Territoriali)
- Dipendenti/Collaboratori/Candidati
- Terzi (Fornitori persone fisiche, stakeholders, consulenti, membri del CdA)

5.1 Trattamento nei confronti dei Clienti

La Società raccoglie e conserva i dati relativi ai propri Clienti, al fine di avviare attività di servizi per la salute e l'informazione medica attraverso la quale promuove formazione tecnico-scientifica e aggiornamento professionale.

La Società, inoltre, ha individuato, per ciascuna categoria di Dati, in relazione a ciascuna finalità, i relativi tempi di conservazione, che ha riportato in un apposito documento denominato "*JAKINFARMA_Regole relative al periodo di conservazione dei dati*" disponibile presso l'ufficio del Referente Privacy.

5.1.1 L'informativa

L'informativa deve essere fornita al Cliente prima di effettuare la raccolta dei Dati.

I modelli di informativa da utilizzare a seconda delle circostanze sono disponibili presso l'ufficio del Referente Privacy

Il Referente Privacy si occuperà sia della redazione delle informative che del conseguente adattamento del documento.

La Società ha individuato le seguenti tipologie di informative, che corrispondono ad altrettante occasioni nel corso delle quali vengono raccolti i dati dei Clienti.

A. <u>Informativa Clienti</u>

Il modello dell'informativa, riportato nel documento denominato "*JAKINFARMA_Informativa Privacy (personale medico)*", si trova presso l'ufficio del Referente Privacy e deve essere rilasciata al momento del primo contatto con l'Interessato (es. in caso di contatto telefonico ad inizio telefonata o visita presso l'Interessato per la formazione tecnico-scientifica e aggiornamento professionale.

B. <u>Informativa Dati non raccolti presso l'Interessato</u>

Talvolta la raccolta dei dati può essere effettuata tramite soggetti terzi; in tali circostanze, è necessario:

- ✓ che sia verificata la possibilità per il terzo di comunicare i Dati alla Società (ad es. in quanto l'Interessato ha fornito un espresso consenso alla comunicazione dei dati;
- ✓ acquisire idonea dichiarazione da parte del terzo che certifichi che i Dati sono stati raccolti/trattati in conformità alla Normativa Vigente e che possono essere oggetto di comunicazione/cessione a terzi (acquisiti dietro specifico consenso);
- ✓ fornire agli Interessati (i cui dati sono stati oggetto di comunicazione e registrazione da parte della Società) una specifica informativa in merito al Trattamento che sarà svolto dalla Società, entro un termine ragionevole che non può superare un mese dalla raccolta, oppure al momento della comunicazione dei dati.

5.1.2 Il consenso

Il consenso del Cliente al Trattamento deve essere richiesto ogni qualvolta non trovi applicazione una delle altre basi giuridiche previste dal GDPR.

Per quanto riguarda il Trattamento per Clienti, il consenso è richiesto per le seguenti finalità:

- Marketing;
- Profilazione;
- Indagini e ricerche di mercato;
- Comunicazione a terzi.

I consensi ottenuti saranno custoditi ed archiviati in una apposita banca dati gestita dal Referente Privacy di JakinFarma.

I consensi ottenuti saranno conservati in accordo a quanto previsto nelle "Linee Guida concernenti le regole ai periodi di conservazione dei dati".

Gli inserimenti in banca dati dovranno evidenziare eventuali modifiche/revoche del medesimo consenso.

5.1.3 I diritti del Cliente

Per la gestione dei diritti che Clienti, in qualità di Interessati, possono esercitare nei confronti del Titolare quest'ultimo si è dotato di una specifica procedura denominata "*JAKINFARMA_Procedura di Richiesta accesso ai Dati da parte dell'Interessato*" disponibile presso l'ufficio del Referente Privacy.

5.2 Trattamento nei confronti di Dipendenti, Collaboratori e Candidati

La Società tratta i Dati Personali dei propri Dipendenti e Collaboratori per l'esecuzione di obblighi derivanti dal contratto che disciplina il rapporto di lavoro (ad esempio, ai fini del rispetto della normativa in materia di previdenza e assistenza, in materia fiscale, in materia di tutela della salute, ai fini della rilevazione della presenza sul posto di lavoro, ai fini della tenuta della contabilità, ai fini della gestione del contenzioso, ai fini della corresponsione di stipendi, assegni, premi, per finalità di dichiarazione dei redditi, ecc.) e/o adempimento di obblighi previsti da leggi, da regolamenti e dalla normativa comunitaria.

Per taluni servizi, la Società si avvale di soggetti terzi di propria fiducia che, in qualità di Responsabili del trattamento svolgono compiti di natura tecnica od organizzativa, quali, ad esempio:

- servizi amministrativo-contabili;
- attività di revisione contabile;
- servizi di elaborazione cedolini paga dipendenti e gestione del personale;
- servizi di acquisizione, registrazione e trattamento di dati rivenienti da documenti o supporti forniti o originati dagli stessi Dipendenti e Collaboratori;
- servizi di archiviazione della documentazione;
- gestione parco veicoli aziendali;
- gestione welfare aziendale.

La Società e i soggetti di cui al capoverso precedente procedono al trattamento dei dati personali mediante elaborazioni manuali o strumenti elettronici o comunque automatizzati, secondo logiche strettamente correlate alle finalità stesse e comunque in modo da garantire la sicurezza e la riservatezza dei dati stessi.

Il conferimento dei dati personali di Dipendenti e Collaboratori è, in alcuni casi, obbligatorio per legge (adempimenti di obblighi fiscali e previdenziali), in altri casi è facoltativo ma comunque funzionale alla gestione del rapporto di lavoro (dati necessari al pagamento delle retribuzioni e degli altri emolumenti).

La Società raccoglie e tratta, anche attraverso l'ausilio di soggetti esterni adeguatamente nominati a Responsabili del trattamento, i Dati Personali dei Candidati presenti all'interno del CV ovvero attraverso la compilazione dell'apposito form, al solo fine di individuare possibili candidati con cui avviare un processo di selezione, a seguito del quale, in caso di esito positivo, poter procedere all'assunzione.

La Società, inoltre, ha individuato, per ciascuna categoria di Dati, in relazione a ciascuna finalità, i relativi tempi di conservazione, che ha riportato in un apposito documento "*JAKINFARMA_Regole relative al periodo di conservazione dei dati*" disponibile presso l'ufficio del Referente Privacy.

5.2.1 L'Informativa Candidati

Il Trattamento dei candidati è effettuato dalla Società per finalità connesse o strumentali allo svolgimento dell'attività di ricerca e selezione del personale. I Dati dei candidati vengono inseriti nel database aziendale utilizzato per le attività di selezione e conservati per 6 mesi. Decorso tale termine di conservazione senza aver proceduto all'assunzione del candidato, i Dati sono distrutti *o resi anonimi*.

L'informativa destinata ai candidati è aggiornata a cura della funzione competente della Società ed è tenuta dal Referente Privacy il quale si occuperà sia della redazione dell'informativa che del conseguente adattamento del documento. L'informativa sarà pubblicata sul sito del Gruppo alla voce "Lavora con noi" per le candidature inviate spontaneamente via email, in ogni caso sarà fornita al momento del primo contatto successivo all'invio del *Curriculum*. L'eventuale trasferimento extra UE sarà effettuato in conformità ai requisiti di legittimità e JakinFarma si assicurerà che sia garantito un livello di protezione adeguato per i Suoi dati ed osservando le normative applicabili a protezione dei dati personali.

In caso di selezioni effettuate direttamente tramite la Società, l'informativa sarà consegnata direttamente ai candidati al momento della presentazione al colloquio.

Le informative cartacee verranno firmate dall'Interessato, per presa visione, ed archiviate.

Il documento "*JAKINFARMA_Informativa Candidati*" è disponibile presso l'ufficio del Referente Privacy.

Nel caso di candidatura al job posting attraverso canale telematico in risposta ad annuncio pubblicato, il candidato farà pervenire i propri dati alla Società attraverso il portale inrecruiting.it, che gestirà, ai sensi del contratto di servizio il dato come Responsabile Esterno al Trattamento, mentre la titolarità del dato resterà in capo alla Società.

5.2.2 L'Informativa Dipendenti e Collaboratori

La Società tratta Dati Personali dei Dipendenti e Collaboratori, quali, ad esempio, dati anagrafici, codice fiscale, dati retributivi, eventuali coordinate bancarie. Può accadere inoltre che, nell'adempimento di specifici obblighi relativi alla gestione del rapporto di lavoro/collaborazione (nei limiti in cui sia applicabile), la Società venga in possesso di Categorie particolari di dati e cioè quelli da cui possono eventualmente desumersi, fra l'altro, l'origine razziale ed etnica, l'adesione a partiti, sindacati, nonché un generale stato di salute (ad esempio, certificati di malattia e infortunio; certificati di gravidanza; appartenenza alle c.d. categorie protette; esiti di visite mediche effettuate ai sensi di legge e di contratto, *etc*.). Questi ultimi possono formare oggetto di Trattamento senza consenso.

Il documento "*JAKINFARMA_Informativa Collaboratori e Dipendenti*" è disponibile presso l'ufficio del Referente Privacy.

Il Referente Privacy è tenuto alla costituzione dell'archivio delle informative dei Dipendenti, ai fini di permettere in qualsiasi momento le opportune verifiche e al riguardo provvede il giorno stesso dell'assunzione a consegnare al neoassunto l'informativa per i Dipendenti che l'Interessato deve riconsegnare firmata per presa visione; l'informativa sottoscritta deve essere inserita nella cartella del Dipendente. La sottoscrizione della informativa aggiornata sostituirà in toto la precedente e la società sarà libera di non tenere in Archivio le precedenti.

5.2.3 Il consenso

La Società richiede il consenso dei Dipendenti qualora sia necessario trattare le immagini degli stessi, per inserimento nell'organigramma o per attività legate alla comunicazione aziendale. Il Referente Privacy raccoglierà, su supporto cartaceo, i consensi aggiornati dei Dipendenti archiviandoli nelle relative cartelle, ai fini di permettere in qualsiasi momento le opportune verifiche.

5.2.4 Il Regolamento per l'utilizzo degli strumenti aziendali

La Società ha adottato un Regolamento per l'utilizzo degli strumenti aziendali con cui il Personale svolge le attività per conto del Titolare (*pc, tablet, smartphone aziendali, rete internet ed intranet, posta elettronica aziendale,* …). In relazione ai Dipendenti, in particolare, il suddetto Regolamento è conformato al principio dall'art. 4 comma 3 della L. 300/1970 (Statuto dei Lavoratori), secondo cui le informazioni raccolte tramite gli strumenti adoperati dal lavoratore per rendere la prestazione lavorativa e quelli necessari alla registrazione degli accessi e delle presenze, possono essere utilizzate ai fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione sulle modalità d'uso degli strumenti utilizzati e di effettuazione dei controlli, nel rispetto di quanto disposto dalla Normativa Vigente.

Il Regolamento viene consegnato al Personale al momento dell'instaurazione del rapporto contrattuale con la Società, a cura del Referente Privacy ai diversi Destinatari (Personale o Collaboratori).

Il Referente Privacy si occuperà della revisione/aggiornamento del documento.

L'insieme delle norme comportamentali ivi incluse è riportato nel documento "*JAKINFARMA _Regolamento per l'uso degli strumenti informatici*", disponibile presso l'ufficio del Referente Privacy.

5.2.5 I diritti dei Dipendenti e Collaboratori

Il Dipendente/Collaboratore può esercitare nei confronti del Titolare i diritti riconosciuti dal GDPR. Le relative richieste del Dipendente/Collaboratore devono essere indirizzate via mail al Referente Privacy che deve provvedere al tempestivo riscontro ed all'evasione entro 30 giorni dalla corretta ricezione della richiesta stessa, anche con l'ausilio degli Autorizzati al Trattamento.

La policy per l'esercizio dei diritti dei Dipendenti e Collaboratori è disponibile presso l'ufficio del Referente Privacy e denominata "*JAKINFARMA_Procedura Richiesta di accesso ai Dati da parte dell'Interessato*"

5.3 I Terzi

Per Terzi la Società intende:

- Fornitori, persone fisiche e titolari di ditte individuali;
- Esponenti, persone fisiche, di società/enti/associazioni/fondazioni ed altre persone giuridiche;

- Stakeholders;
- Membri del CdA, non Dipendenti;
- Membri del Comitato Controllo e Rischi, non Dipendenti
- Consulenti persone fisiche liberi professionisti
- Agenti persone fisiche liberi professionisti

La Società tratta i seguenti Dati Personali di Terzi per finalità amministrative e contabili in relazione all'instaurazione, gestione ed esecuzione dei Contratti, anche in considerazione delle proprie esigenze produttive, organizzative e di conduzione del suo business aziendale e per l'adempimento di tutti gli obblighi derivanti dalla relativa normativa applicabile.

La Società, inoltre, ha individuato, per ciascuna categoria di Dati, in relazione a ciascuna finalità, i relativi tempi di conservazione, che ha riportato in un apposito documento "*JAKINFARMA_Regole relative al periodo di conservazione dei dati*" disponibile presso l'ufficio del Referente Privacy.

5.3.1. L'Informativa a Terzi

Il Referente Privacy di volta in volta invierà l'informativa al Terzo contestualmente alla trasmissione del contratto di fornitura di beni/servizi/consulenza da stipulare.

L'invio e la raccolta delle informative per gli amministratori, i revisori ed i sindaci della Società è di competenza diretta del Referente Privacy, il quale si occuperà sia della redazione dell'informativa sia del conseguente adattamento del documento.

I Dati dei Terzi vengono trattati per finalità strettamente connesse e strumentali alla gestione del rapporto con la Società, nonché per le finalità previste agli obblighi previsti da leggi, da regolamenti e dalla normativa comunitaria.

Il documento "*JAKINFARMA_Informativa Terzi*" è disponibile presso l'ufficio del Referente Privacy.

5.3.2 I diritti dei Terzi

Il Terzo può esercitare nei confronti del Titolare i diritti riconosciuti dal GDPR. Come previsto nella relativa informativa, le richieste del fornitore devono essere indirizzate al Referente Privacy via email che deve provvedere al tempestivo riscontro ed all'evasione entro 30 giorni dalla corretta ricezione della richiesta, anche con l'ausilio degli Autorizzati al Trattamento.

6. Gli strumenti di trattamento

6.1 Il Registro delle attività di trattamento del Titolare

L'articolo 30 del GDPR prevede che ogni Titolare debba tenere un registro delle attività di Trattamento. Sono esentate dalla tenuta del Registro le imprese od organizzazioni con meno di 250 Dipendenti, a meno che il trattamento effettuato:

- Possa presentare un rischio per i diritti e le libertà degli Interessati,
- Il trattamento non sia occasionale
- Includa il trattamento di categorie particolari di dati

La Società in qualità di Titolare ha predisposto e mantiene il proprio Registro delle attività di trattamento, ed il documento Il documento "*JAKINFARMA_Registro delle attività di trattamento*" è disponibile presso l'ufficio del Referente Privacy.

6.2 Data Breach

Secondo quanto previsto dal GDPR, in caso di violazione dei Dati Personali, la Società deve notificare al Garante la relativa violazione senza ritardo, a meno che sia improbabile che la violazione dei Dati Personali presenti un rischio per i diritti e le libertà degli Interessati.

Ciò avviene quando il *Data Breach* comporti l'insorgenza o l'aggravamento di danni, quali perdita del controllo dei propri Dati Personali, discriminazione, furto o usurpazione di identità, perdite finanziarie, decifratura non autorizzata della pseudonomizzazione, pregiudizio alla reputazione, perdita di riservatezza dei Dati Personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo.

Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà degli Interessati, la Società deve altresì – salvo alcune specifiche e circoscritte eccezioni – darne comunicazione agli Interessati stessi.

Gli obblighi di comunicazione descritti sopra devono essere effettuati nel rispetto di precise tempistiche e contenuti formali e prevedono, altresì, alcune valutazioni preliminari che devono accompagnare sia la fase dell'individuazione dell'esistenza o meno di un reale *Data Breach*, sia la valutazione sulla necessità di procedere alla notificazione al Garante ovvero alla comunicazione agli Interessati.

I processi per la gestione del data breach sono normati nella 'Il documento "*JAKINFARMA_ Data Breach Policy*" disponibile presso l'ufficio del Referente Privacy.

6.3 *Data Protection Impact Assessment* (DPIA)

In conformità all'articolo 35 del GDPR, la Società procede ad una DPIA in fase di sviluppo di ogni nuova iniziativa o servizio previsto, o di nuovi applicativi e soluzioni informatiche, in particolare qualora il nuovo Trattamento sia caratterizzato da almeno due dei seguenti elementi:

- Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura (ad es. inclusione o esclusione automatica, senza valutazione ulteriore, di Fornitori in/da procedure di gara, sulla base dei dati forniti);
- Monitoraggio sistematico (ad es. sorveglianza sistematica di aree pubbliche);
- Categorie particolari di dati;
- Trattamenti su larga scala (da determinare sulla base del numero di Interessati, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata, o persistenza, dell'attività di Trattamento; ambito geografico dell'attività di Trattamento);
- Combinazione o raffronto di insiemi di dati (ad es. derivanti da due o più Trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'Interessato);
- Dati relativi a Interessati vulnerabili (ad es. minori);
- Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
- Trattamenti che, di per sé, "impediscono [agli Interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto". Ciò comprende i trattamenti finalizzati a consentire, modificare o negare l'accesso degli Interessati a un servizio o la stipulazione di un contratto.

Per la procedura da seguire si rinvia alla lettura del documento "*JAKINFARMA_Procedura Data Protection Impact Assessment - DPIA*" disponibile presso l'ufficio del Referente Privacy.

7. La Governance IT

7.1 I principi del GDPR

Il GDPR "rifonda" le misure minime di sicurezza alla base del sistema di protezione dei dati personali, modificando radicalmente approccio e lasciando al Titolare ampio margine di libertà di scelta in funzione della realtà produttiva nella quale opera.

Questo nuovo sistema poggia i cardini su tre principi fondamentali:

- la necessità di un'analisi del rischio;
- la stretta connessione con la migliore tecnica e i costi da supportare:
- la comprensione e l'applicazione costante della nozione di "*accountability*".

La Società, come già evidenziato, per garantire il rispetto dei suddetti principi ha condotto un'attività di Risk Assessment, all'esito della quale ha deciso di dotarsi di un Documento per la valutazione dei rischi che riassume, per poi rinviare alle policy IT di dettaglio, le misure di sicurezza adottate per contenere il rischio di data incident.