Data Breach Policy

Data di emissione e decorrenza	***20 dicembre 2019***
Numero revisione	***Rev. 01***
Revisione	
Preparata da	***ConsulenzeDPO***
Controllata da	***Referente Privacy – Sara Anguilla***
Approvata da	***Emmanuele Adami***

Sommario

1. Introduzione

1.1 Normativa applicabile

La Data Breach *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 - General Data Protection Regulation* (di seguito **"GDPR"**) - ed in particolare i considerando n. 85, 86, 87, 88 artt. 33, 34 - e del D.lgs. 101/2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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 (regolamento generale sulla protezione dei dati)", oltre alle *"Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679"* adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017, versione emendata e adottata il 6 febbraio 2018, e dalle indicazioni relative a *"Violazioni di dati personali (data breach)",* ultimo aggiornamento 14 dicembre 2018 presenti sul sito del Garante della Privacy.

La Società, ai sensi del GDPR è tenuta a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).
È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, ciò al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici alla Società e per poter riscontrare nei tempi e nei modi previsti dalla normativa europea l'Autorità Garante e/o gli interessati.
Le sanzioni previste dal GDPR per omessa notifica di Data Breach all'Autorità di Controllo o omessa comunicazione agli interessati o entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, può comportare l'applicazione in capo alla Società di una sanzione amministrativa pecuniaria fino a 10 milioni di euro o fino al 2% del fatturato annuo totale dell'esercizio precedente, anche accompagnata da una misura correttiva ai sensi dell'art. 58 c. 2. 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"**).

1.2 Scopo ed ambito di applicazione

Lo scopo di questa procedura è di disegnare un flusso per la gestione delle violazioni dei dati personali trattati dalla Società in qualità di Titolare del trattamento (di seguito "**Titolare del trattamento**"). Queste procedure sono ad integrazione delle procedure adottate dal Titolare del trattamento in materia di protezione dei dati personali ai sensi della legislazione vigente.

In tal senso la *Policy* sintetizza le regole per garantire il rispetto dei principi esposti e la realizzabilità tecnica e la sostenibilità organizzativa, nella gestione del data breach, sotto i diversi aspetti relativi a:

- sensibilizzare i dipendenti sulle responsabilità in materia di protezione dei dati personali e sull'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli incidenti sulla sicurezza (inclusi i Personal data breach);
- definire processi per identificare, tracciare e reagire ad un incidente sulla sicurezza e a un Personal data breach, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se, in caso di Personal data breach, si renda necessario procedere alla (i) notifica al Garante e (ii) comunicazione agli Interessati;
- definire ruoli e responsabilità per la risposta agli incidenti sulla sicurezza e ai Personal data breach;
- assicurare un adeguato flusso comunicativo all'interno della Società tra le parti interessate.

La presente procedura si applica a tutte le informazioni personali e alle altre informazioni che, pur non costituendo informazioni personali, sono raccolte o gestite o comunque trattate dalla Società siano esse dati contenuti su dispositivi elettronici, accessibili via rete o web, contenuti su dispositivi mobili o portatili ovvero su supporti cartacei.

1.3 Destinatari

Questa *Policy* è rivolta a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento (meglio descritti al punto 5 della presente procedura) quali:

- i lavoratori dipendenti, nonché coloro che a qualsiasi titolo, e quindi a prescindere dal tipo di rapporto intercorrente, abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (di seguito genericamente denominati Destinatari interni);
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dal Destinatario interno che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 GDPR o di autonomo Titolare (di seguito genericamente denominati Destinatari esterni);

di seguito, genericamente denominati "Destinatari".

Tutti i Destinatari devono essere debitamente informati dell'esistenza della presente procedura, mediante metodi e mezzi che ne assicurino la comprensione.
Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

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 del trattamento:** 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 del trattamento:** 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.
- **DPO:** il Data Protection Officer[1] soggetto nominato dalla Società in qualità di Responsabile della protezione dei Dati, qualora sussistano i requisiti previsti dall'articolo 37 del GDPR.
- **Delegato del trattamento:** la persona fisica che, secondo l'organizzazione aziendale, ricopre un ruolo gestionale e di responsabilità all'interno della società che determina specifiche modalità organizzative rispetto ad uno o più trattamenti.
- **Autorizzato al trattamento:** la persona fisica, espressamente incaricata, che opera sotto l'autorità del Titolare del trattamento, incaricato di specifici compiti e con funzioni connesse al trattamento dei dati personali.
- **Referente privacy:** la persona fisica, direttamente o indirettamente, afferente alla Società che operativamente si occupa della Policy privacy, propone la stesura dei regolamenti sulla privacy e sul trattamento dati ed effettua e valuta controlli sugli stessi.
- **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.

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

- **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 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. Gestione del data breach interno alla struttura

3.1 Premesse

La tempestività è un fattore determinante nella risposta agli incidenti sulla sicurezza e ai Personal data breach ed è dovere di ciascun soggetto, nell'ambito del proprio ruolo nella struttura e nella catena di comunicazione, non ritardare iniziative di reazione all'incidente e rispettare le procedure e le tempistiche di comunicazione individuate dal presente documento.

La risposta a un incidente sulla sicurezza o a un Personal data breach deve avvenire secondo le fasi descritte di seguito; considerando, tuttavia, che gli incidenti possono avere molteplici cause o coinvolgere diversi soggetti ed avere conseguenze caratterizzate da vari livelli di gravità, tali fasi potrebbero sovrapporsi o richiedere tempistiche differenti o aggiornamenti.
Considerati i rischi e, in caso di Personal data breach, le ridotte tempistiche per effettuare la Notifica e per la comunicazione agli interessati, occuparsi degli incidenti di sicurezza deve essere obiettivo prioritario per tutti i soggetti coinvolti nella loro gestione.

Tutti gli incidenti di sicurezza e i Personal data breach devono essere trattati con il massimo livello di riservatezza: le informazioni devono essere condivise esclusivamente con il personale identificato nella presente procedura e solo quando strettamente necessario. Eventuali comunicazioni a soggetti non coinvolti nella gestione dell'Incidente dovranno limitarsi all'indicazione che si è verificato un problema e che lo stesso è in fase di gestione.

In ogni azienda è individuato il Referente privacy ed è opportuno che sia affiancato da un gruppo privacy (gruppo multidisciplinare di professionisti che supportano il Referente privacy per specificità tecniche quali ICT, SIC, area giuridica, area del personale…). Il Referente privacy assume, ai fini della presente Policy, il ruolo di responsabile del processo.

È necessario che la Società dia notizia a tutti gli autorizzati al trattamento in merito alla presente Policy mediante idonea delibera e circolare.

3.2 Modalità e profili di notifica all'Autorità Garante Privacy

Il personale e i collaboratori che prestano attività in JakinFarma S.r.l., ove dovessero venire a conoscenza di un incidente sulla sicurezza o di elementi che fanno sospettare (anche a seguito di segnalazione di terzi) che si sia verificato o possa verificarsi un tale incidente, sono tenuti a comunicare immediatamente tale circostanza al Referente privacy utilizzando il modulo allegato (All. 1).

Il Referente privacy effettua immediatamente una valutazione preliminare - avvalendosi, nel caso, del gruppo privacy e di eventuali altre professionalità con funzioni consulenziali necessarie per la corretta analisi della situazione - al fine di determinare se si sia effettivamente verificato un incidente sulla sicurezza, e stabilisce inoltre, se quest'ultimo possa qualificarsi anche come Personal data breach.

Ai fini di una corretta classificazione dell'episodio il Referente privacy utilizzerà lo schema di scenario di data breach allegato al presente schema di procedura. Al termine di tale valutazione preliminare, la Società si

considera "venuta a conoscenza" della violazione e, conseguentemente, da tale momento inizieranno a decorrere i termini per la notifica e la comunicazione.

Pertanto, sulla scorta delle determinazioni raggiunte, il Referente privacy predispone l'eventuale comunicazione all'Autorità Garante, a firma del Titolare del trattamento, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.

Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.

È comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi)

La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del Referente privacy.

4. Gestione del data breach esterno alla struttura

4.1 Premesse

Ogniqualvolta la Società, in qualità di Titolare del trattamento, si trovi ad affidare il trattamento di dati ad un soggetto terzo, in qualità di Responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di data breach sia inclusa nel suddetto contratto. Ciò al fine di obbligare il responsabile ad informare il titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di data breach.

Ad ogni Responsabile del trattamento deve essere comunicato il contatto del Referente privacy al quale effettuare la predetta segnalazione.

4.2 Modalità e profili di notifica all'Autorità Garante Privacy

Ogni Responsabile del trattamento, qualora dovesse venire a conoscenza di un incidente sulla sicurezza o di elementi che fanno sospettare (anche a seguito di segnalazione di terzi) che si sia verificato o possa verificarsi un tale incidente, è tenuto a comunicare immediatamente tale circostanza al Referente privacy utilizzando il modulo allegato (All. 2)

Il Referente privacy effettua immediatamente una valutazione preliminare - avvalendosi, nel caso, del gruppo privacy e di eventuali altre professionalità con funzioni consulenziali necessarie per la corretta analisi della situazione - al fine di determinare se si sia effettivamente verificato un incidente sulla sicurezza, e stabilisce inoltre, se quest'ultimo possa qualificarsi anche come Personal data breach.

Ai fini di una corretta classificazione dell'episodio il Referente privacy utilizzerà lo schema di scenario di data breach allegato al presente schema di procedura. Al termine di tale valutazione preliminare, la Società si considera "venuta a conoscenza" della violazione e, conseguentemente, da tale momento inizieranno a decorrere i termini per la notifica e la comunicazione.

Pertanto, sulla scorta delle determinazioni raggiunte, il Referente privacy predispone l'eventuale comunicazione all'Autorità Garante, a firma del Titolare del trattamento, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.

Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.

È comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi).

La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del Referente privacy.

5. Modalità di comunicazione agli Interessati

Il Titolare del trattamento, con il supporto del Referente privacy, provvede alla comunicazione ai soggetti interessati dal Personal data breach quando la violazione è suscettibile di presentare un rischio elevato per i loro diritti e libertà fondamentali. Anche tale valutazione dovrà essere effettuata utilizzando le tabelle riportate al paragrafo E.

La comunicazione ai soggetti interessati deve avvenire nel più breve tempo possibile e senza ingiustificato ritardo, al fine di permettere a questi ultimi di adottare le necessarie contromisure per limitare i danni. In caso di urgenza, si può rendere necessario procedere alla comunicazione agli Interessati anche prima di aver effettuato la notifica al Garante.

Il Titolare del trattamento, con il supporto del Referente privacy, valuta se contattare il Garante per chiedere suggerimenti sulla necessità di comunicare l'incidente agli interessati e sull'individuazione del messaggio più appropriato da fornire.

Lo strumento per effettuare tale comunicazione varia in base al numero dei soggetti interessati da contattare, al costo e ai mezzi normalmente utilizzati per le comunicazioni con i soggetti interessati.

La comunicazione è individuale e compiuta per iscritto (via e-mail, sms, etc.); tuttavia, ove ciò richiedesse degli sforzi sproporzionati, è possibile procedere anche con una comunicazione pubblica (banner o post su sito internet, pubblicazione di annuncio sul giornale, etc.). In ogni caso, la comunicazione deve essere trasparente ed effettuata con mezzi tali da garantire che gli interessati siano effettivamente informati del fatto che si è verificato un Personal data breach.

6. Registro delle violazioni

È istituito un registro in cui il Referente privacy, per quanto di sua competenza, dovrà documentare gli incidenti di sicurezza/Personal data breach a prescindere dal fatto che da questi sia seguita la notifica al Garante e/o la comunicazione agli Interessati.

Il registro deve contenere (i) la descrizione della tipologia di dati oggetto della violazione, (ii) le cause, (iii) gli effetti, (iv) le azioni poste in essere per rimediarvi, (v) le motivazioni per le quali si è deciso di non procedere alla notifica al Garante e/o alla comunicazione agli Interessati ovvero l'indicazione della notifica effettuata e delle eventuali successive integrazioni.

Dovranno essere altresì documentate le ragioni che hanno condotto alla Notifica per fasi o al ritardo nella notifica.

Il registro dovrà inoltre indicare se, a seguito di un Personal data breach, è stata effettuata la comunicazione al soggetto interessato, i relativi tempi e mezzi di comunicazione utilizzati.

Il Referente privacy cura l'aggiornamento del registro delle violazioni, ai sensi dell'art. 33, comma 5 del GDPR.

7. Schema di valutazione scenari data breach

Di seguito sono illustrati alcuni esempi, non esaustivi, di possibili violazioni di dati personali, allo scopo di supportare i soggetti coinvolti nella procedura, nella valutazione in merito alla necessità di effettuare o meno la notifica di data breach all'Autorità Garante.

Tipo di Breach	Definizione	Estensione minima / Soglia di segnalazione	Esempi	Controesempi
Distruzione	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, né di altri. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo	Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	• Guasto non riparabile dell'hard disk contenente uno o più banche dati che, in violazione al regolamento, erano salvate localmente • Incendio di archivio cartaceo delle schede cliente. • Distruzione di copie back up	• Rottura di una chiavetta USB che non contiene dati personali originali (in unica copia) • Rottura di un PC che non contiene dati personali originali (in unica copia) • Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura nell'apposito applicativo
Perdita	Un insieme di dati personali a seguito di un incidente o azione fraudolenta, non è più nella disponibilità del Titolare ma potrebbe esserlo in quella di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non	Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili • Dati relativi a più soggetti relativi a interi episodi o relativi a tipologie di dato la cui indisponibilità lede i diritti fondamentali	• Smarrimento di chiavetta USB contenente dati originali • Smarrimento di fascicolo cartaceo personale dipendente	• Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa

	sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato	dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla perdita possa ledere i diritti fondamentali dell'interessato Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione		
Modifica	Un insieme di dati personali irreversibilmente modificato a seguito di incidente o azione fraudolenta, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con la certezza che non sia stato alterato.	Caratteristiche: • Modifiche sistematiche su più casi Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	Caratteristiche: • Guasto tecnico che altera parte dei contenuti del sistema, compromettendo anche i backup • Azione involontaria, o fraudolente, di un utente che porta alla alterazione di dati di un cliente in modo non tracciato e irreversibile	• Guasto tecnico che altera parte dei contenuti del sistema, rilevato e sanato tramite operazioni di recovery • Azione involontaria di un utente che porta ad una alterazione di dati tracciata e reversibile • Modifica di un documento non ancora validato dal proprio autore
Divulgazione non Autorizzata	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a	Caratteristiche: • Modifiche sistematiche su più casi	Caratteristiche: • Consegna di un device portatile di archiviazione con dati dei clienti ad altra	• Infezione virale di un PC con un virus che dalla scheda

	seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento della Società	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	struttura senza autorizzazione	tecnica non trasmette dati su internet • Trasmissione non autorizzata di un documento non ancora validato dal proprio autore
Accesso non Autorizzato	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche incaricati dal titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti della Società	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Accesso alla rete aziendale da persone esterne alla Società che sfruttano vulnerabilità di sistemi • Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso al sistema	• Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi • Accesso non autorizzata di un documento non ancora validato dal proprio autore.
Indisponibilità temporanea del dato	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'interessato	Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale	• Infezione da ransomware con temporanea perdita di disponibilità dei dati e questi non possono essere ripristinati dal backup • cancellazione accidentale dei dati da parte di una persona non autorizzata	• Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso

			• perdita della chiave di decrittografia di dati crittografati in modo sicuro • irraggiungibilità di un sito di stoccaggio dei dati per isolamento dovuto a cause di forza maggiore	

Un incidente sulla sicurezza o un Personal data breach, quindi, non è solo un attacco informatico ma può consistere anche in un incidente a seguito di una calamità naturale ove venga pregiudicata la disponibilità o l'integrità dei dati ovvero nella perdita o il furto di un dispositivo aziendale in disponibilità di un dipendente (notebook, tablet, smartphone, chiavetta USB, disco esterno, etc.) o in un accesso abusivo o una sottrazione di documenti con dati personali invalidando la riservatezza degli stessi

I casi di incidente sulla sicurezza o un Personal data breach per le casistiche già descritte si estendono ai documenti cartacei o su supporti analogici.

La comunicazione involontaria di documenti, o in generale di dati, che non abbiano vero senso compiuto o riconducibilità verso l'interessato non è considerato incidente sulla sicurezza o un Personal data breach, ma come un normale errore procedurale; questo poiché (i) chi riceve non può sapere a quale cliente fisico sono riferiti i dati, (ii) il cliente fisico non è danneggiato poiché nessuno riferimento alla sua persona è stato diffuso.

La violazione di quanto previsto nella presente Policy espone il Titolare del trattamento al rischio di responsabilità civile, penale e a sanzioni amministrative. Il soggetto autore delle violazioni potrà incorrere in responsabilità disciplinare e conseguentemente nei provvedimenti sanzionatori, secondo quanto previsto dalla normativa vigente e dal CCNL di riferimento applicabile.

ALLEGATO 1 – MODULO DI COMUNICAZIONE DATA BREACH INTERNO ALLA STRUTTURA

Qualora scopra un incidente sulla sicurezza o un Personal data breach, è pregato di informare immediatamente il Suo superiore gerarchico, il quale, a sua volta, dovrà compilare la modulistica a seguire e inviarla a mezzo e-mail al seguente indirizzo privacy@jakinfarma.it:

Comunicazione di Data Breach	Note
Data scoperta violazione:	
Data dell'incidente:	
Luogo della violazione (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili):	
Nome della persona che ha riferito della violazione:	
Dati di contatto della persona che ha riferito della violazione (indirizzo e-mail, numero telefonico): *In caso di destinatario esterno indicare la ragione sociale*	
Denominazione della/e banca/che dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati:	
Categorie e numero approssimativo di interessati coinvolti nella violazione:	
Breve descrizione di eventuali azioni poste in essere al momento della scoperta della violazione:	
Responsabile del dipartimento:	
data:	

ALLEGATO 2 – MODULO DI COMUNICAZIONE DATA BREACH ESTERNO ALLA STRUTTURA

Qualora scopra un incidente sulla sicurezza o un Personal data breach, è pregato di informare immediatamente la Società e dovrà compilare la modulistica a seguire e inviarla a mezzo e-mail al seguente indirizzo email privacy@jakinfarma.it:

Comunicazione di Data Breach	Note
Responsabile del Trattamento:	
Data scoperta violazione:	
Data dell'incidente:	
Luogo della violazione (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili):	
Nome della persona che ha riferito della violazione:	
Dati di contatto della persona che ha riferito della violazione (indirizzo e-mail, numero telefonico): *In caso di destinatario esterno indicare la ragione sociale*	
Denominazione della/e banca/che dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati:	
Categorie e numero approssimativo di interessati coinvolti nella violazione:	
Breve descrizione di eventuali azioni poste in essere al momento della scoperta della violazione:	
Responsabile del trattamento (legale rappresentante):	
data:	