# Modello Organizzativo in materia di Protezione dei Dati Personali di Lepida ScpA

v3 del 08.11.2019

## 1. Contesto normativo ed indirizzi generali

Il 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, di seguito anche solo "Regolamento" o "GDPR" con la normativa nazionale di adeguamento, D. lgs. 196/03 come successivamente modificato dal D. lgs. 101/2018, afferma importanti principi quali il diritto alla protezione dei dati personali e quello della necessità del trattamento (need to know) e, al contempo, garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale, al diritto alla protezione dei dati personali, alla portabilità dei dati, sino al diritto all'oblio. I principi fondamentali introdotti dal Regolamento e non presenti nel precedente "Codice Privacy" (dec. legisl. 196/03), possono essere riassunti come segue:

1. Privacy by design e by default;
2. Rafforzamento del principio del "need to know";
3. Introduzione di adempimenti formali come l'adozione del Registro dei Trattamenti e redazione del PIA – Privacy Impact Assessment;
4. Nuovi diritti degli interessati;
5. Obbligo di gestione dei Data Breaches;
6. Determinazione delle misure di sicurezza secondo un approccio "risk based";
7. Introduzione della figura del DPO – Data Protection Officer (Responsabile della Protezione dei Dati Personali);
8. Ridefinizione della figura del Responsabile del Trattamento dei Dati Personali e del Contitolare del trattamento;
9. Forte inasprimento delle sanzioni che, in caso di inadempimento, possono arrivare sino a € 20 milioni o al 4% del fatturato annuo worldwide.

In tale contesto, anche in relazione all'introduzione di nuove figure ed adempimenti, vengono ridefiniti i ruoli dei diversi attori che intervengono nei

trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti:

1. il titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
2. il responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
3. Responsabile della protezione dei dati (di seguito anche Data Protection Officer o DPO): figura prevista dagli artt. 37 e ss. del regolamento, che ne disciplinano compiti, funzioni e responsabilità;
4. persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile: figura che si desume implicitamente dalla definizione di "terzo" di cui al n. 10 del comma 1 art. 4 del Regolamento.

Il presente documento dettaglia la Politica definita da Lepida ScpA (nel seguito la "Lepida") per adempiere alle prescrizioni del Regolamento delineando nel contempo il complessivo ambito di responsabilità, sulla base delle deleghe conferite dal Consiglio di Amministrazione ed in relazione all'ampliamento dell'oggetto sociale conseguente all'operazione di fusione per incorporazione di CUP 2000 scpa.

## 2. Ambito oggettivo di applicazione

Il Modello Organizzativo si applica alle attività che comportano il trattamento dei dati personali di titolarità di Lepida ScpA (quali, ad es. attività connesse alla gestione del personale, agli organi societari e agli adempimenti relativi ai propri clienti, fornitori ed eventuali consulenti, per cui Lepida ScpA ha titolarità autonoma), ovvero di contitolarità di Lepida ScpA (quali i dati personali raccolti presso l'interessato e finalizzati al rilascio delle credenziali SPID) ovvero alle attività che comportano il trattamento dei dati personali e particolari per le quali la società sia stata individuata, ai sensi dell'art. 28 del Regolamento Privacy, in qualità di responsabile del trattamento (quali, ad es. attività oggetto di convenzioni di servizio sottoscritte con Aziende Sanitarie ed Ospedaliere ovvero con la Regione Emilia-Romagna per le quali ha ricevuto apposita nomina, eventualmente con funzioni di amministrazione di sistema) nel rispetto delle finalità determinate dai committenti e secondo le modalità previste dalla convenzione di servizio e dalla nomina ricevuta.

Le nomine di Lepida ScpA in qualità di responsabile del trattamento definiscono l'ambito del trattamento autorizzato da parte dei Soci titolari. Nessun trattamento ulteriore è consentito, se non previa autorizzazione dei titolari a cui compete in via esclusiva la verifica della compatibilità dei trattamenti effettuati rispetto alle informative rilasciate ex art. 13 del Regolamento UE ed ai consensi acquisiti dagli

interessati, o ex art. 14 del medesimo Regolamento se i dati non siano stati ottenuto presso l'interessato.

## 3. Qualità e conservazione dei dati personali, principio di necessità del trattamento

I dati personali devono essere: esatti ed aggiornati; trattati unicamente per gli scopi determinati, espliciti e legittimi definiti da Lepida; pertinenti, completi e non eccedenti rispetto alle finalità della raccolta.

I sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. All'uopo sono utilizzate opportune clausole contrattuali, seguendo le procedure interne, le indicazioni del titolare e le indicazioni in termini di legge, quando lo sviluppo del software è commissionato all'esterno di Lepida. I dati personali da questa trattati sono conservati per il tempo necessario al raggiungimento delle finalità specificate nelle informative per le diverse categorie di soggetti, dopodiché vengono cancellati seguendo le procedure interne e le prescrizioni di legge.

## 4. Ruoli e responsabilità: il Titolare

Il Titolare del trattamento ai sensi dell'art. 4, c.1, n. 8 del Regolamento europeo 2016/679 è la Società nel suo complesso, in persona del Presidente del Consiglio di Amministrazione e legale rappresentante. Spetta pertanto in particolare a LepidaScpA in veste di titolare:

1. porre in essere ovvero adottare tutti gli atti necessari all'attuazione della normativa sulla protezione dei dati personali, ivi compresi le valutazioni di impatto e l'istituzione del Registro dei Trattamenti;
2. designare il Responsabile della protezione dei dati;
3. designare i soggetti delegati all'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;
4. effettuare, a mezzo della struttura competente, apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso i profili relativi alla sicurezza informatica, in collaborazione con il DPO designato;
5. organizzare periodicamente iniziative formative destinate ai soggetti autorizzati al trattamento dei dati personali.

## 5. Ruoli e responsabilità: Direttore Generale - Delegato agli adempimenti ed alla gestione della privacy

Con delibera n. D0319_44 del 25/03/2019 il Consiglio di Amministrazione, in relazione agli effetti della fusione ed alla necessità di omogeneizzare i processi già precedentemente adottati in CUP 2000 scpa e Lepida spa, ha conferito mandato al Direttore Generale di procedere alla definizione dei ruoli e delle competenze in ordine alla formalizzazione e alla sottoscrizione di ogni atto e/o adempimento richiesto dalla vigente normativa Privacy e/o dai provvedimenti emessi dal Garante per la protezione dei dati personali sia sul versante societario interno (ad es. definizione dei ruoli e delle responsabilità aziendali in ambito Privacy, formalizzazione di procedure, nomina del personale quale autorizzato al trattamento ex art. 29 e 4.10 del GDPR, etc.) sia nei confronti dei Terzi (ad es. Contratto di nomina a Responsabile del trattamento e/o sub-Responsabile ex art. 28 del GDPR nei confronti di fornitori/soggetti terzi le cui attività contrattualmente affidate implichino operazioni di trattamento dei dati).

Spettano in ogni caso al Direttore Generale:

1. l'adozione di policy in materia di privacy e sicurezza informatica, con particolare riferimento all'utilizzo, alla sicurezza delle risorse informatiche e allo sviluppo delle applicazioni informatiche, da aggiornare periodicamente, ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario;
2. la sottoscrizione degli atti di consultazione preventiva al Garante; la notifica e la comunicazione delle violazioni dei dati personali all'autorità di controllo ai sensi degli artt. 33 e 34 del Regolamento;
3. la designazione degli amministratori di sistema in aderenza alle norme vigenti in materia;
4. la sottoscrizione, su proposta dei Direttori di Divisione o dei Coordinatori, delle lettere di autorizzazione, con relative istruzioni operative, per le persone individuate ai fini dello svolgimento delle attività che comportano trattamento di dati personali e particolari.

Con formale provvedimento a firma del Direttore Generale e previa organizzazione di apposite sessioni formative volte alla diffusione ed alla conoscenza del presente modello organizzativo, potranno essere sub-delegati ai Direttori di Divisione ed ai Coordinatori in via meramente esemplificativa e non esaustiva i compiti di seguito indicati:

1. verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;
2. disporre, in conseguenza alla verifica di cui alla lett. a) le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
3. adottare soluzioni di privacy by design e by default;

4. fornire i propri contributi ai fini del costante aggiornamento del registro delle attività di trattamento per la struttura di competenza;
5. individuare e proporre alla Direzione, ai fini della formale preposizione, i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "incaricati" o "autorizzati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente documento ed, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali;
6. predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa;
7. fornire supporto, anche tramite gli autorizzati nel riscontro alle istanze degli interessati inerenti l'esercizio dei diritti previsti dalla normativa;
8. disporre l'adozione dei provvedimenti imposti dal Garante;
9. collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
10. adottare, se necessario, specifici Disciplinari tecnici di settore, anche congiuntamente con altri soggetti delegati all'attuazione, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla propria area di competenza.

Nell'attuazione dei compiti sopra indicati i soggetti delegati, ove nominati, possono acquisire il parere del DPO nei casi e con le modalità specificate nel seguito.

## 6. Ruoli e responsabilità: i Responsabili del trattamento

Sono designati responsabili del trattamento di dati personali i soggetti esterni a Lepida ScpA in possesso delle caratteristiche di cui all'art. 28 del Regolamento che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati persona di titolarità di Lepida ScpA.

Pertanto, qualora occorra affidare un incarico comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Attesa la natura negoziale delle designazioni dei responsabili del trattamento, questa deve essere effettuata all'interno di contratti o convenzioni e, in ogni caso, in costanza di formazione del rapporto contrattuale, in aderenza ai modelli messi a disposizione dalla struttura competente in materia di privacy.

Lepida ScpA assume la qualità di responsabile del trattamento nell'ambito delle convenzioni di servizio sottoscritte con i propri soci in attuazione delle quali è chiamata a svolgere servizi che comportano il trattamento di dati personali di titolarità del singolo socio. A seguito della fusione Lepida ScpA è deputata a svolgere servizi di supporto tecnico/organizzativo, prima in capo alla società incorporata CUP 2000 scpa, a favore delle Aziende Sanitarie ed Ospedaliere, sicchè ai trattamenti di dati personali già gestiti da Lepida ScpA si aggiungono le attività di trattamento di dati cd. particolari di cui all'art. 9 del GDPR propri della nuova mission.

In tal caso la nomina avviene mediante apposito atto definito direttamente dalla struttura privacy dell'Ente socio nel quale vengono declinati i compiti e le responsabilità di Lepida ScpA, ivi compresa la possibilità di designare sub-responsabili (nuova figura introdotta dall'art. 28, par. 4 del GDPR) per specifiche attività di trattamento, nel rispetto degli obblighi contrattuali che legano titolare e responsabile primario.

## 7. Ruoli e responsabilità: gli Autorizzati

Gli autorizzati al trattamento sono i soggetti – nominati dal Titolare e/o dal Responsabile del trattamento (Art. 29 del Regolamento) – che trattano i dati personali cui hanno accesso, attenendosi alle istruzioni loro impartite dal Titolare e/o dal Responsabile.

Le risorse impiegate in mansioni che comportino trattamento di dati personali e particolari devono essere appositamente preposte con nomina sottoscritta dal Direttore Generale. I nominativi degli Autorizzati al trattamento sono forniti dalle Divisioni aziendali, in accordo con l'Area Gestione Risorse umane, unitamente all'indicazione dell'ambito del trattamento.

La designazione scritta deve inoltre contenere le istruzioni operative impartite agli incaricati del trattamento.

Tali istruzioni, oltre a riguardare eventuali aspetti di dettaglio da diversificare in relazione alle specificità dei singoli trattamenti, devono quanto meno contenere un espresso richiamo alle policy di LepidaScpA in materia di sicurezza informatica e protezione dei dati personali.

## 8. Ruoli e responsabilità: il Responsabile della Protezione dei dati (DPO)

Il "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 prevede l'obbligo per gli Enti pubblici di designare il Responsabile della protezione dei dati (Data Protection Officer, di seguito DPO).

Specificatamente, sono di seguito indicati i compiti del DPO in aderenza agli 37 e ss del suddetto regolamento, conformati alla precipua organizzazione di Lepida ScpA:

1. informa e fornisce consulenza la Società in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali;
2. sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche di Lepida ScpA in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
3. coopera con il Garante per la protezione dei dati personali;
4. funge da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;
5. partecipa allo svolgimento delle verifiche di sicurezza svolte dall'Aggregato Processi e Sicurezza;
6. partecipa alla gestione degli incidenti di sicurezza nelle modalità previste da specifica policy di Lepida ScpA;
7. formula gli indirizzi per realizzazione del Registro delle attività di trattamento di cui all'art. 30 del Regolamento;
8. fornisce i pareri obbligatori e facoltativi richiesti dalle strutture secondo quanto specificato di seguito.

Il DPO fornisce il proprio parere in ordine alla legittimità e alla correttezza dei trattamenti di dati personali sulle istanze che le strutture di Lepida ScpA presentano nei casi di seguito indicati.

Devono essere obbligatoriamente richiesti pareri in ordine a:

1. individuazione delle misure che abbiano un significativo impatto sulla protezione dei dati personali che Lepida ScpA intende adottare ai fini della tutela della riservatezza, integrità e disponibilità del patrimonio informativo di Lepida ScpA, anche a seguito di incidenti di sicurezza o analisi dei rischi;
2. adozione di policy e disciplinari in materia di protezione dei dati personali e sicurezza delle informazioni, redazione e aggiornamento dei disciplinari tecnici con impatto sulla sicurezza delle informazioni;

3. individuazione di misure poste a mitigazione del rischio delle criticità emerse dall'analisi dei rischi, che abbiano un significativo impatto sulla protezione dei dati personali;
4. incidenti sicurezza.

Possono essere inoltre richiesti, se ritenuti utili, pareri in ordine a:

1. progettazione di nuove applicazioni o modifica sostanziale di quelle esistenti, in aderenza al principio della privacy by design e by default;
2. valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del Regolamento 2016/679;
3. valutazione dell'eventuale pregiudizio che l'accesso civico potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento UE n. 679/2016;
4. opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.

Le richieste di parere devono essere inviate all'indirizzo di posta elettronica dpo@lepida.it. Possono presentare le richieste di parere il Direttore Generale e i soggetti delegati ove nominati. I pareri sono espressi nel rispetto delle seguenti codifiche:

1. NC: acronimo di "non conformità", nei casi in cui siano rilevati elementi di non conformità alla normativa e alle policy in materia di protezione dei dati personali;
2. OS: acronimo di "osservazione", nei casi in cui vi siano elementi di miglioramento che garantiscono una maggiore aderenza alla normativa e alle policy in materia di protezione dei dati personali, non costituendo vincolo di attuazione;
3. PO: acronimo di "positivo", nei casi in cui siano prospettati elementi valutati come conformi alla normativa e alle policy regionali in materia di protezione dei dati personali.

Nei casi in cui il DPO esprima pareri "NC" e "OS" il Direttore Generale o i soggetti delegati, ove nominati, devono formalizzare, nelle medesime forme utilizzate dal DPO per l'espressione del parere, le motivazioni che giustificano l'esecuzione dell'attività o l'implementazione della soluzione tecnologica, in contrasto alle indicazioni fornite dal DPO.
I pareri espressi dal DPO sono conservati agli atti del Direttore Generale o dei soggetti delegati.

## 9. Ruoli e responsabilità: Divisione Amministrativa

Il Direttore Generale è supportato dalla Divisione Amministrativa:

1. nel presidio dell'evoluzione normativa di riferimento sulla privacy;

2. nella definizione delle azioni di privacy necessarie per la relativa implementazione;
3. nella mappatura del trattamento dati personali e particolari relativi alla privacy;
4. nella gestione dei registri dei trattamenti sulla privacy;
5. nella predisposizione dei template aziendali sulla privacy da utilizzare in tutti i contratti, convenzioni e atti;
6. nella gestione delle istruttorie corrispondenti sulla privacy e sulla messa a disposizione di dati ad istanze pervenute da soggetti terzi ed in particolare dalle pubbliche autorità.

## 10. Ruoli e responsabilità: Aggregato Processi e Sicurezza

Il Direttore Generale è Supportato dall'Aggregato Processi e Sicurezza:

1. nella definizione di politiche, di piani, di procedure, di linee guida e di azioni di controllo della filiera della privacy relativa a Lepida ed ai servizi da essa erogati a favore dei Soci;
2. nel coordinamento ed implementazione di azioni tra Divisioni e Aggregati relative alla privacy, in particolare con i rapporti con il DPO;
3. nella verifica puntuale che le azioni previste sulla privacy siano state effettuate dalle Aree e Divisioni con produzione di report periodici al DG;
4. nel coordinamento degli acquisti e dell'utilizzo dei fornitori per le azioni di privacy nel rispetto delle risorse complessivamente allocate dalla Società;
5. nella analisi di ogni possibile causa di rischio nei processi aziendali relativi alla privacy, anche mediante l'interazione con Aree e Divisioni;
6. nel coordinamento della analisi normativa per i rischi sulla privacy e a relativi reati legati alle attività della Società;
7. nel monitoraggio dei processi aziendali, anche con attività proattive e relative interrelazioni, procedure, strumenti, indicatori in relazione al mantenimento delle certificazioni che includano elementi di privacy;
8. nella conduzione di audit interni relativi alla privacy e ai relativi rischi;
9. nel presidio delle attività di formazione e consapevolezza in materia di protezione dei dati personali e sicurezza delle informazioni.

## 11. Ruoli e responsabilità: Divisioni e Aggregati

In conformità al principio di cui all'art. 25.1 del Regolamento europeo (privacy by design), ciascuna Divisione e Aggregato è chiamata a conformare ab origine i propri progetti e processi alla protezione dei dati personali.

L'analisi preventiva sulla tutela dei dati personali e sulla conformità ai principi del Regolamento europeo delle azioni e dei processi della Divisione viene condivisa con l'Aggregato Processi e Sicurezza ai fini dell'analisi dei rischi e delle

conseguenti azioni proattive o implementative da intraprendere. Tale principio orienta, pertanto, anche ogni attività di analisi, progettazione e realizzazione software, sia rispetto alla produzione interna, sia rispetto a servizi di progettazione di sistemi che vengano affidati a fornitori terzi.

Inoltre, a fronte di una procedura per l'affidamento di servizi/forniture che comporti anche un trattamento di dati personali/particolari, la Divisione o l'Area referente della procedura di acquisizione segnala alla Divisione Amministrativa la necessità di predisporre il contratto di nomina a Responsabile del trattamento in costanza di formalizzazione dell'ordinativo di fornitura. Tale documento è parte integrante della procedura di acquisto e condizione per il perfezionamento della stessa.