UPM MODENA S.p.A.

MODELLO ORGANIZZATIVO PRIVACY

Regolamento UE 679/2016

REVISIONI DEL DOCUMENTO

DATA	COMMENTO
2022	ADOZIONE DEL MODELLO ORGANIZZATIVO PRIVACY
2024	AGGIORNAMENTO DEL MODELLO ORGANIZZATIVO PRIVACY

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

1.PREMESSE

1.1. Scopo

Il presente Modello Organizzativo è lo strumento che permette a UPM Modena S.p.A. (di seguito, "UPM" o "Società") di individuare e, quindi, di adottare le misure di sicurezza necessarie alla protezione del proprio patrimonio informativo, in ottemperanza al dettato della normativa europea in tema di protezione dei dati personali.

In adesione al Principio di *Accountability* previsto e disciplinato dall'art. 24 GDPR 679/2016, il presente Modello individua: **(i)** la mappatura dei trattamenti effettuati, con espressa indicazione delle categorie di dati utilizzati, dei soggetti interessati e delle aree di rischio connesse all'attività svolta, **(ii)** i diversi soggetti e i ruoli dagli stessi rivestiti nel ciclo di trattamenti effettuati dalla Società, **(iii)** i registri delle attività di trattamento per ogni area aziendale considerata, **(iv)** le misure legali, organizzative e tecniche adottate per prevenire il verificarsi di trattamenti illeciti, **(v)** le procedure necessarie a garantire un continuo adeguamento alla normativa in materia di Privacy, comprese quelle finalizzate a porre rimedio a eventuali violazioni al sistema.

Il presente strumento permette a UPM di assicurare la protezione dei dati trattati fin dalla progettazione del proprio *business-plan*: **l'attenzione è rivolta a ridurre al minimo il trattamento dei dati personali mediante l'applicazione di tutte le misure tecniche e organizzative necessarie e adeguate**. I meccanismi di tutela valutati troveranno diretta applicazione nell'ambito della riorganizzazione aziendale in materia di Privacy, divenendo un'impostazione di lavoro predefinita.

1.2. Fonti

A partire dal 26 maggio 2016 la principale fonte in materia di protezione dei dati personali è rappresentata dal **Regolamento Europeo n. 679/2016 (GDPR)** che detta una disciplina unitaria e omogenea in materia di privacy all'interno dei vari stati membri, ponendo fine ad una regolamentazione frammentata della normativa sulla protezione dei dati personali.

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

La citata disciplina trova definitiva applicazione a partire dal 25 maggio 2018 ed è obbligatoria in tutti i suoi elementi, nonché direttamente applicabile in ciascuno degli Stati membri, senza la necessità di un atto di recepimento da parte del nostro Legislatore.

L'entrata in vigore della nuova disciplina privacy, tuttavia, non ha comportato *ipso facto* l'automatica abrogazione della normativa interna; lo stesso GDPR ha previsto che il legislatore italiano procedesse ad un adeguamento della stessa al nuovo assetto normativo imposto dal Regolamento Europeo, asservendo il "vecchio" D. Lgs 196/2003 (Codice Privacy) alle nuove disposizioni in materia di trattamento dei dati.

A tal fine, il Legislatore italiano, con il D. Lgs. 101/2018 del 10.08.2018, pubblicato in G.U. il 4.09.2018, entrato in vigore il 19.09.2018 ha profondamente modificato il Codice della Privacy.

Fondamentale, tuttavia, ricordare come il GDPR sia e resti prima di tutto, parametro di legittimità della normativa nazionale.

A seguito del nuovo decreto di adeguamento, infatti, il vecchio Codice privacy risulta non solo significativamente novellato nelle sue disposizioni, ma anche fortemente modificato nella sua ispirazione di fondo e nella sua stessa finalità.

Il novellato articolo 2 D. Lgs. 196/2003, a conferma, recita: "Il presente Codice reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del Regolamento".

1.3. Le parole della Privacy

Allo scopo di rendere più agevole la consultazione del presente Modello e dei documenti allegati allo stesso, si riporta la definizione dei termini più significativi in materia di Privacy.

Trattamento: qualunque operazione o complesso di operazioni, compiuta con o senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati personali.

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

Dato Personale: qualunque informazione che sia tale da consentire di identificare la persona fisica, sia in modo diretto che indiretto.

Si considerano quali dati personali, a mero titolo esemplificativo: il nome, un numero di identificazione, i dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Categorie Particolari di Dati Personali: dati personali che rivelano l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati o associazioni, lo stato di salute, la vita sessuale, l'orientamento sessuale della persona, nonché i dati genetici (caratteristiche genetiche ereditarie che forniscono informazioni sulla fisiologia o sulla salute fisica della persona) e i dati biometrici (relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali ad esempio l'immagine facciale).

Dati Giudiziari: dati relativi alle condanne penali o a misure di sicurezza applicate nei confronti del soggetto interessato.

Finalità del Trattamento: lo scopo determinato, esplicito e legittimo che viene perseguito dal Titolare con il Trattamento.

Titolare del Trattamento: persona fisica o giuridica, P.A. e qualsiasi altro ente o associazione cui competono, anche insieme ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del Trattamento e agli strumenti utilizzati.

Responsabile del Trattamento: persona fisica o giuridica, autorità pubblica o altro organismo che tratta dati personali per conto del Titolare del trattamento.

Il rapporto tra Titolare e Responsabile viene regolato da un contratto o da altro atto giuridico, nel quale devono essere indicati la materia, la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, nonché gli obblighi e i diritti del Titolare del trattamento.

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

Responsabile della Protezione Dati (DPO): soggetto, nominato dal Titolare o dal Responsabile, dotato di conoscenze specialistiche della normativa e delle pratiche in materia di privacy.

I compiti del DPO si sostanziano essenzialmente in importanti funzioni di carattere consultivo a favore del Titolare e del Responsabile del trattamento su tutte le tematiche privacy. Svolge, inoltre, funzione di raccordo con l'Autorità Garante e di controllo sull'osservanza del Regolamento nell'ambito dell'azienda o ente di riferimento.

Nell'esercizio dei suoi compiti il DPO agisce in piena indipendenza ed in assenza di conflitti di interesse.

Il conferimento di tale incarico è obbligatorio solo nelle ipotesi previste dal GDPR; in tutti gli altri casi Titolare e Responsabile dovranno valutare l'opportunità di tale nomina, motivando la scelta maturata.

Interessato: persona fisica alla quale si riferiscono i dati personali.

Soggetto Autorizzato: chiunque (personale dipendente o collaboratore) venga autorizzato a compiere operazioni di trattamento, sulla base di adeguate istruzioni ricevute dal Titolare o dal Responsabile.

Accountability: principio di responsabilizzazione, secondo il quale il Titolare procede con la mappatura dei trattamenti effettuati, con la valutazione del grado del rischio e con la predisposizione delle misure giuridiche, organizzative e tecniche adeguate ed efficaci per la protezione dei dati personali, nel rispetto del principio di adeguatezza.

Base Giuridica: condizione di liceità del trattamento, che può consistere alternativamente nel: (i) consenso dell'interessato, (ii) contratto tra le parti, (iii) obbligo legale cui è soggetto il Titolare, (iv) salvaguardia di interessi vitali dell'interessato o di altra persona fisica, (v) esecuzione di un compito di pubblico interesse o connesso all'esercizio di pubblici poteri, (vi) interesse legittimo del Titolare.

Informativa: documento che deve essere consegnato prima di effettuare il trattamento, contenente tutte le informazioni che il Titolare deve fornire all'Interessato in merito a: categorie di dati personali oggetto del trattamento, modalità attraverso cui tali dati verranno trattati, finalità perseguite, tempi di conservazione,

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

soggetti che entreranno in contatto con i suoi dati personali, obbligatorietà del conferimento dei dati personali e conseguenze del rifiuto, nonché diritti che l'interessato potrà esercitare.

Consenso: manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato con cui questi accetta espressamente, mediante dichiarazione o azione positiva inequivocabile, che i suoi dati personali siano oggetto di trattamento.

Registro Attività Trattamenti: strumento di compliance aziendale che deve indicare:

- il nome e i dati di contatto del Titolare del trattamento, del Rappresentante del Titolare del trattamento e del Responsabile della protezione dei dati (DPO) ove nominato;
- le finalità del trattamento;
- la descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi;
- se presenti, i trasferimenti di dati personali verso paesi terzi e la loro identificazione;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative.

Sebbene la tenuta di tale registro sia obbligatoria solamente nel caso di imprese o organizzazioni con più di 250 dipendenti, il Garante della Privacy ha consigliato a tutti i Titolari e Responsabili del trattamento di predisporre tale registro, al fine di garantire una corretta gestione dei dati personali.

Data Breach: violazione dei dati personali che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Gruppo imprenditoriale: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate.

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

2. FINALITA' E AMBITO

2.1. Finalità

Il presente documento rappresenta il Modello Organizzativo Privacy ("MOP") di UPM, predisposto in modo da rispondere alle disposizioni del Regolamento Europeo 2016/679 ("GDPR").

Con l'osservanza di questo documento si intende richiamare tutte le risorse operanti all'interno della Società al rispetto della normativa sulla sicurezza dei dati personali, con espressa attenzione all'impiego delle risorse informative.

Il MOP andrà costantemente aggiornato in relazione all'evoluzione del settore e dell'organizzazione.

2.2 Ambito di applicazione

Il presente documento è vincolante per tutto il personale, sia dipendete che collaboratore, della Società, coinvolto in attività che prevedono il trattamento di dati personali.

3. ANALISI DELL'ORGANIZZAZIONE

3.1. Organigramma e ruoli

UPM definisce e mantiene aggiornata la mappa dell'organizzazione aziendale volta a individuare e descrivere i ruoli, le responsabilità e i compiti assegnati a ciascuna delle figure coinvolte nelle attività di trattamento dei dati personali, al fine di garantire il corretto funzionamento del sistema di gestione dei dati personali e la gestione dei rischi a esso associati.

La mappatura dei ruoli e delle responsabilità viene documentata attraverso:

- ✓ il sistema di autorizzazioni al trattamento ex art. 29 GDPR, secondo il c.d. principio "*Need to Know*";

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

- ✓ la formalizzazione delle nomine di Responsabili del Trattamento ex art. 28 GDPR nei confronti dei soggetti esterni a cui vengono delegate determinate attività.

3.2. Titolare del Trattamento e Responsabile del Trattamento – criteri utilizzati per la loro individuazione

Nel rinviare al glossario di cui al precedente paragrafo 1.3, si riportano di seguito, in estrema sintesi, i criteri utilizzati per l'individuazione delle posizioni di garanzia in oggetto, da utilizzarsi nei casi in cui la distinzione tra le due figure possa richiedere passaggi interpretativi, soprattutto in virtù del non sempre agevole coordinamento tra la disciplina europea in materia di Privacy e la normativa interna.

L'interpretazione univoca del testo normativo europeo individua, come **elemento caratterizzante il ruolo del Responsabile, l'esternalizzazione del trattamento.**

Tale concetto, tuttavia, pecca, una volta calato nella realtà imprenditoriale, di estrema genericità: di fatto, l'esternalizzazione non riguarda mai un singolo trattamento, ma un'attività nel suo complesso, che implica un ciclo definito di trattamenti. In ragione di quanto sopra, pertanto, si è ritenuto che un soggetto rivesta il ruolo di Responsabile ogni qualvolta esso stesso svolga un'attività che avrebbe potuto espletare in prima battuta il Titolare, ma che, di fatto, in ragione di una mera scelta imprenditoriale, questi ha preferito delegare a un soggetto esterno.

Per capire quando si è in presenza di un Responsabile del Trattamento si dovrà valutare **se quella svolta dal soggetto di volta in volta considerato, sia un'attività che l'azienda può eseguire in autonomia** (come a esempio l'attività di elaborazione delle buste paga, quella di assistenza informatica e, in genere, tutte quelle strumentali al core business aziendale), oppure se si tratta di un tipo di incarico che deve necessariamente essere effettuato da un soggetto terzo (come l'attività posta in essere dalle società di revisione e di certificazione): mentre nel primo caso non vi è dubbio alcuno che, trattandosi di attività delegate in outsourcing, i relativi soggetti rivestano il ruolo di Responsabile esterno del Trattamento, nel secondo caso si

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

è certamente in presenza di un autonomo Titolare del Trattamento, in quanto soggetto che pone in essere un'attività diversa, ben distinta da quelle rientranti nelle competenze aziendali e, quindi, da quest'ultima non realizzabili.

Ciò premesso, i criteri utilizzati da UPM per riconoscere un Responsabile del trattamento si riferiscono:

- ✓ al **livello di istruzioni preliminari fornite** (tanto più specifiche saranno le istruzioni, tanto minore sarà il livello di autonomia del soggetto esterno che quindi dovrà essere identificato quale Responsabile),
- ✓ al **grado di controllo effettuato dal Titolare** in relazione all'esecuzione del servizio,
- ✓ all'**immagine data all'esterno** e al conseguente **legittimo affidamento dei soggetti interessati**,
- ✓ al **grado di competenza professionale** e di **specifiche conoscenze** delle parti.

In particolare, la Società si attiene alle indicazioni fornite dal Garante per la Protezione dei dati personali in merito alla tipizzazione dei rapporti Titolare-Responsabile del Trattamento:

- ✓ nei **gruppi di imprese** generalmente le singole società hanno distinta e piena titolarità in merito al trattamento dei dati personali dei propri dipendenti e collaboratori. Nel caso in cui la società capogruppo svolga su mandato delle società controllate adempimenti in materia di lavoro, previdenza e assistenza sociale per i lavoratori andrà designata quale Responsabile del Trattamento;
- ✓ i fornitori di servizi di **localizzazione geografica** (nell'ambito del rapporto di lavoro), di posta elettronica e di televigilanza devono essere individuati quali Responsabili del Trattamento;
- ✓ il **medico competente** viene considerato quale Titolare del Trattamento, in considerazione del fatto che è la stessa legge a fornirgli autonoma titolarità riguardo al trattamento dei dati relativi alla sorveglianza sanitaria; tale soluzione appare avvalorata dal fatto che si tratta di un professionista tenuto al rispetto del segreto professionale e delle regole deontologiche di settore e che il datore di lavoro non può accedere ai dati relativi alle patologie accertate (ma solo al giudizio di idoneità al lavoro);

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

- ✓ il **consulente del lavoro** è autonomo Titolare riguardo al trattamento dei dati dei propri dipendenti, collaboratori e clienti, ma riveste la qualifica di Responsabile relativamente al trattamento dei dati del personale dipendente dei propri clienti;
- ✓ le **Società Assicuratrici** sono state individuate quali autonomi Titolari del Trattamento, sulla base della considerazione che <<…l'esercizio dell'attività assicurativa non può in alcun modo, neanche astrattamente, formare oggetto di "delega" da parte del soggetto che affida tramite gara tale servizio, in quanto la stessa può essere svolta esclusivamente da soggetti specializzati e sottoposti ad una disciplina di settore…>>.

3. MODELLO ORGANIZZATIVO PRIVACY

3.1. Metodologia di predisposizione del Modello

In ossequio al Principio di *Accountability* e delle regole applicative da esso derivanti (trasparenza, adeguatezza, neutralità tecnologica, necessità, proporzione, correttezza, tracciabilità e ricostruibilità), UPM, al fine di addivenire all'individuazione del proprio Modello Operativo Privacy, ha posto in essere le seguenti attività.

Analisi degli assetti aziendali *as is* e valutazione del grado di compliance attuale. Le attività hanno avuto a oggetto: (i) Individuazione dei *Key Officer* (personale operante in/per l'azienda che gestisce aree o processi che impattano sulla normativa privacy); (ii) Incontro preliminare con i *Key Officer* finalizzato alla sensibilizzazione sul progetto da realizzare e sulle modalità operative per la realizzazione stessa; (iii) Interviste individuali con i *Key Officer* finalizzate a mappare l'attuale struttura operativa e funzionale dell'azienda.
In particolare, si è proceduto: (i) al censimento e classificazione dei dati trattati dalla società, (ii) alla mappatura delle attuali modalità (raccolta, inventariazione, misure di sicurezza ecc...) attraverso le quali avvengono detti trattamenti, (iii) alla ricostruzione dell'attuale organigramma aziendale Privacy con individuazione dei vari ruoli a oggi vigenti (incaricati, responsabili...), con emersione delle posizioni ricoperte "di fatto" (anche ipotesi di contitolarità) e dei trattamenti affidati a terzi senza o carenti di regolamentazione specifica; (iv) alla mappatura e analisi delle procedure di controllo esistenti e della regolamentazione aziendale disciplinante

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

l'attività in materia di trattamento dei dati, (v) alla verifica dell'utilizzo corretto della strumentazione informatica, (iii) alla mappatura delle regole di prevenzione di condotte scorrette o anche solo inconsapevoli che possano mettere a rischio la sicurezza informatica e la tutela dei dati (Utilizzo e norme di comportamento per attrezzature e dei posti di lavoro, Procedura di salvataggio dati, Gestione password, Utilizzo Software aziendali - antivirus, gestionale… - Gestione e utilizzo della rete e della posta elettronica, Procedure di connettività ADSL e Wi.Fi.).

Predisposizione di apposita Relazione di Mappatura – Valutazione del Rischio e *Gap Analisys*. Al termine delle predette attività è stato possibile predisporre una specifica **Relazione di Mappatura** (situazione *as is*) che è stata messa "in controluce" con la disciplina introdotta dal Regolamento UE n. 679/2016 (c.d. GDPR) al fine di **evidenziare il grado di rischio** attualmente presente in azienda e le azioni che la società deve porre in essere (**Gap Analysis)** per l'allontanamento/prevenzione di detto rischio e l'adeguamento alla normativa in questione (la Relazione di Mappatura, Valutazione del rischio e *Gap Analisys* è allegata al presente Modello).

Sulla base delle predette attività è stato poi possibile delineare il Modello di gestione del Sistema Privacy (Modello Operativo Privacy), ritagliato sulle specifiche caratteristiche operative di UPM che si basa sulla implementazione, rispetto e aggiornamento (anche in ottica di continuo miglioramento) delle regole e principi esposti al successivo paragrafo.

3.2. Modello Operativo Privacy di UPM: regole e principi

UPM mantiene un approccio "*by design*", **tenendo in considerazione il tema della protezione dei dati personali per ciascun progetto fin dalle fasi preliminari e, quindi, prima dell'inizio delle attività di trattamento**.

La Società, in veste di Titolare, verifica l'intero processo di trattamento dei dati, dalla raccolta fino alla cancellazione/distruzione e identifica in modo chiaro e preciso gli eventuali Responsabili incaricati di alcuni trattamenti (o parte di essi), nonché i soggetti Destinatari di particolari comunicazioni. Allo stesso tempo la

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

Società individua se vi siano situazioni di Contitolarità e, in caso positivo, attiva specifici protocolli di gestione delle stesse.

Una volta **individuati i trattamenti necessari alle finalità perseguite** – sia in veste di Titolare che di Responsabile - la Società, nel rispetto del principio di "*privacy by default*":

- verifica le categorie di dati personali utilizzati (identificativi, particolari ex art. 9 GDPR 679/2016, giudiziari ex art. 10 GDPR 679/2016), controllando di trattare unicamente le informazioni strettamente necessarie alle finalità perseguite;
- limita i periodi di conservazione dei dati raccolti al tempo necessario al perseguimento delle finalità individuate, compatibilmente con il rispetto della normativa civilistica, contributiva, previdenziale e fiscale vigente;
- identifica espressamente i soggetti/dipendenti autorizzati ai vari trattamenti, fornendo agli stessi appositi mansionari che prevedano l'indicazione delle modalità da seguire, nonché degli strumenti e dei supporti da utilizzare per tutto il ciclo del trattamento, a seconda della posizione rivestita (Titolare / Responsabile del Trattamento).

La Società controlla la **conformità delle misure adottate ai requisiti richiesti dalla normativa vigente**, verificando in particolare:

- la corretta individuazione della base giuridica che legittima il trattamento (consenso, contratto, obblighi e diritti conseguenti al rapporto di lavoro, ecc..) e il rispetto del principio di necessità e proporzione;
- il rispetto del diritto degli interessati a ricevere un'informazione chiara e precisa dei trattamenti eseguiti, contenente l'espressa previsione di tutti i diritti dagli stessi esercitabili, con la chiara indicazione delle modalità da utilizzare;
- l'osservanza delle garanzie necessarie in caso di eventuale trasferimento dei dati al di fuori dell'Unione Europea.

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

Successivamente, UPM **identifica le possibili fonti di rischio** rilevanti, individuando tre aree:

- rischi relativi agli strumenti tecnici – informatici utilizzati (misure tecniche);
- rischi riconducibili alla non conformità alla normativa vigente (misure legali);
- rischi relativi all'organizzazione aziendale (misure organizzative).

Per ogni area la Società **valuta il grado del rischio di ciascun trattamento**.

Al fine di assicurare l'integrità dei dati, la sicurezza e la protezione dei luoghi e degli strumenti utilizzati, nonché il ripristino della disponibilità dei dati in caso di distruzione o danneggiamento, in base al precedente esame dei rischi, la Società **individua gli opportuni protocolli di controllo del rischio e rimedi**, calibrati tra:

Misure Tecniche – nell'ambito dell'utilizzo, della gestione e della funzionalità della strumentazione informatica, considerando software gestionali, programmi applicativi, rete informatica, cloud, siti web, posta elettronica, ecc.. In particolare, la Società dovrà implementare, diffondere, controllare il rispetto e mantenere aggiornate le regole e le procedure previste dalla **Politica Aziendale per la Sicurezza Informatica** (vedasi Allegato);

Misure Legali – quali (i) la formalizzazione di incarichi a ciascun dipendente/collaboratore, in qualità di soggetti autorizzati, (ii) la regolare organizzazione di sessioni di formazione e aggiornamento dei propri dipendenti e collaboratori in materia di privacy, (iii) la formalizzazione di accordi e impegni con i Titolari/Responsabili del Trattamento, che prevedano adeguate garanzie reciproche in tema di rispetto della normativa vigente in materia di privacy, (iv) l'individuazione quali Responsabili del Trattamento di soggetti professionalmente qualificati, che forniscano esplicite garanzie, tecniche e organizzative, di adeguamento alla normativa vigente, (v) l'individuazione delle situazioni di Contitolarità e predisposizione di un accordo interno volto alla distribuzione delle responsabilità tra Contitolari, (vi) la valutazione circa la necessità di nominare un DPO, (vii) la predisposizione e la verifica della modulistica necessaria a rendere una corretta informativa e a

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

raccogliere, ove necessario, il consenso dell'interessato; (viii) il rispetto delle regole autorizzative e di gestione dei sistemi di videosorveglianza.

Misure Organizzative – quali (i) la creazione e l'aggiornamento di un preciso organigramma in materia di privacy, (ii) la predisposizione di *job description*, (iii) l'individuazione di luoghi sicuri e non accessibili al pubblico in cui vengono conservati ed archiviati i documenti in formato cartaceo, (iv) il costante aggiornamento di misure e piani che garantiscano la sicurezza dei luoghi in cui vengono conservati i dati, anche in ipotesi di calamità naturali.

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

4. POLICY

Ai fini dell'effettiva attuazione del Modello Organizzativo Privacy sopra delineato, la Società si è dotata di apposite policy aziendali (allegate al Modello stesso) che, di seguito, si procede a illustrare.

4.1 Gestione dell'esercizio dei diritti da parte degli interessati

UPM, in qualità di Titolare del Trattamento, ha predisposto una policy volta a regolare in modo preciso e puntuale modalità e tempistiche dirette a favorire l'esercizio dei diritti dei soggetti interessati.

I soggetti interessati che vorranno ricevere le informazioni e le comunicazioni di cui agli artt. 15-21 GDPR dovranno inviare, all'attenzione di UPM, come specificato nell'informativa resa, una raccomandata A.R. o una e-mail all'indirizzo privacy@upmgroup.it, avendo cura di precisare il contenuto della richiesta (al fine di facilitare ulteriormente l'accesso all'esercizio di tali diritti, la Società mette a disposizione dei soggetti interessati, un modello di richiesta predefinito).

UPM individua nell'Ufficio Legale la Funzione aziendale incaricata di gestire le richieste e a fornire le risposte alle domande pervenute.

Sulla base dei principi di responsabilizzazione, adeguatezza e tracciabilità, il Titolare del Trattamento può essere chiamato a dimostrare il corretto adempimento della predetta policy, in caso di richiesta da parte degli interessati. A tal fine, UPM ha predisposto un apposito registro, contenente tutte le domande inviate dai soggetti interessati con l'indicazione della data della richiesta e della risposta; la compilazione di detto registro fa sempre capo alla predetta funzione aziendale.

4.2 Valutazione della sussistenza dei requisiti per la nomina del DPO

L'attività di allineamento alla normativa in materia di protezione dei dati personali ha compreso una prima valutazione rispetto alla necessità di nominare un Data Protection Officer (DPO), tenendo in considerazione quanto stabilito dall'art. 37 GDPR, in merito ai casi in cui tale nomina è obbligatoria. A conclusione della

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

citata verifica, la Società ha deciso di non dotarsi di tale figura, non rientrando in alcuna delle ipotesi descritte dalla citata norma.

Successivamente UPM ha ritenuto opportuno procedere con una nuova valutazione in merito all'opportunità di dotarsi di un DPO, alla luce delle raccomandazioni, in termini di buona prassi, emanate dal Gruppo di Lavoro dei Garanti europei (oggi noto come European Data Protection Board).

In particolare, le motivazioni per le quali i Garanti Europei consigliano di procedere con la nomina su base volontaria di un DPO anche al di fuori dei casi di obbligatorietà previsti dalla normativa sono le seguenti:

- migliore gestione del sistema di protezione dei dati personali in caso di elevato numero di trattamenti svolti e/o di soggetti interessati coinvolti,
- opportunità di aumentare il sistema di controllo interno,
- acquisizione di una maggiore competitività verso l'esterno, attraverso una maggiore qualificazione nei confronti di clienti, fornitori e partners commerciali,
- necessità di stimolare internamente un sempre maggiore grado di attenzione al principio di responsabilizzazione.

UPM ha valutato come l'attuale assetto organizzativo permetta alla Società di assicurarsi i citati vantaggi anche senza la nomina di un DPO, avendo strutturato un sistema caratterizzato da:

- ✓ una funzione interna (Ufficio Legale), composta da personale competente in materia di *Data Protection*, che si occupa, con continuità di azione, delle attività di monitoraggio e aggiornamento del Sistema di gestione della protezione dei dati;
- ✓ il supporto di un consulente esterno che ha maturato un'approfondita conoscenza della normativa e delle buone prassi in materia di privacy, che viene interpellato in merito alle questioni attinenti alla materia della protezione dei dati che comportano un grado di complessità superiore rispetto a quello gestibile con le sole risorse interne.

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

UPM non considera tale valutazione come definitiva; in considerazione della dinamicità del contesto normativo e imprenditoriale in cui opera, la Società procederà a rivalutare la necessità/opportunità di dotarsi di un Data Protection Officer in caso di: (i) modifiche legislative, (ii) interpretazioni fornite dall'Autorità Garante e/o dalla giurisprudenza, in materia di requisiti per la nomina del DPO, (iii) implementazione dei trattamenti svolti, (iv) utilizzo di nuove modalità per l'espletamento di trattamenti già oggetto di analisi.

Nel caso in cui UPM dovesse decidere di individuare un Data Protection Officer, si ricorda che lo stesso dovrà:

- ✓ informare e fornire consulenza alla Società in merito agli obblighi derivanti dalla legislazione Europea (GDPR e altre disposizioni dell'Unione) e dalla legislazione nazionale in materia di protezione dei dati personali;
- ✓ sorvegliare l'osservazione del GDPR 679/2016 e in genere della legislazione – Europea e interna – in tema di protezione dei dati, oltre che oltre che delle Policy adottate in materia dalla Società (compresi l'attribuzione delle responsabilità la sensibilizzazione e la formazione del personale);
- ✓ fornire un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- ✓ cooperare con l'Autorità di controllo;
- ✓ fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.

4.3. Gestione eventi di Data Breach

Conformemente al dettato del GDPR 679/2016, UPM si è dotata di una policy per gestire l'eventuale violazione di sicurezza subita, comportante la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato ai dati trattati dalla società, indipendentemente dalla natura della causa che ha generato tale violazione.

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

La citata policy, a seconda che la Società rivesta il ruolo di Titolare o di Responsabile del Trattamento, scansiona le varie fasi di intervento, prevedendo *in primis* la valutazione dei rischi derivanti dall'episodio di Data Breach, nonché tutti i conseguenti adempimenti.

UPM individua nell'Ufficio Legale la Funzione aziendale demandata alla corretta gestione degli episodi di Data Breach.

4.4. Aggiornamento della sicurezza dei dati (privacy by design and by default)

In ottemperanza ai principi di *Accountability*, UPM si è dotata di una policy contenente le indicazioni per procedere con un'analisi periodica circa l'entità delle minacce e la vulnerabilità del proprio sistema; tale policy garantisce - anche per il futuro, in un'ottica di continuo aggiornamento – un costante e attuale adeguamento della policy aziendale alla normativa Privacy, sia nel caso di nuovi trattamenti, che nel caso di modifiche normative e/o interpretazioni e provvedimenti da parte dell'Autorità Garante.

4.5. Verifica dei casi di Contitolarità

In ottemperanza ai principi di correttezza e trasparenza, UPM si è dotata di una policy per l'individuazione delle situazioni di Contitolarità, ai sensi dell'art. 26 GDPR 679/2016, al fine di gestire, sia a livello interno che verso l'esterno, problematiche ed effetti derivanti da tali situazioni.

4.6. Regolamento per il corretto utilizzo del Sistema Informativo Aziendale

UPM si è dotata di un apposito Regolamento volto **(i)** all'indicazione delle regole alle quali si deve attenere il personale che utilizza strumenti aziendali per l'esecuzione delle proprie mansioni, nonché **(ii)** alla precisazione dei trattamenti (controlli, verifiche, ecc.) che la Società si riserva di realizzare sull'utilizzo degli stessi e delle modalità con le quali tali trattamenti saranno svolti.

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

Il Regolamento viene diffuso tra tutto il personale che ha accesso al sistema informatico aziendale, con modalità che ne permettano la tracciabilità e viene archiviato in modo da rendere sempre possibile (e agevole) per tutto il personale il reperimento della versione più aggiornata.

Considerata l'importanza strategica del documento in esame, la Società organizza specifiche sessioni di formazione sul contenuto del Regolamento, volte ad aumentare il grado di consapevolezza riguardo sia alle corrette modalità di utilizzo degli strumenti informatici, sia alla natura e alla modalità di esecuzione dei controlli che la Società si riserva di effettuare rispetto al funzionamento del sistema informativo e al corretto utilizzo della strumentazione aziendale assegnata.

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

5. ATTUAZIONE E AGGIORNAMENTO DEL MODELLO - DOCUMENTAZIONE E MODULISTICA

5.1 Registro delle Attività di Trattamento (RAT)

UPM si è dotata del **Registro delle Attività di Trattamento**, andando a diversificare le varie aree operative.

Nonostante l'art. 30 GDPR preveda l'obbligo di istituire tale registro solo per imprese o realtà imprenditoriali con oltre 250 dipendenti, la Società proprio in ragione del principio di *Accountability* e di ottemperanza alle raccomandazioni del Garante per la Privacy – volte alla massima tracciabilità dell'attività svolta – ha ritenuto opportuno procedere alla redazione del citato RAT.

Tale Registro andrà sempre aggiornato, ogniqualvolta UPM implementi il ciclo dei trattamenti effettuati, sia in qualità di Titolare che di Responsabile del Trattamento, e/o persegua finalità ulteriori o diverse da quelle a oggi individuate.

5.2. Modulistica

Dopo aver verificato il contenuto della modulistica già in uso, UPM ha proceduto a un aggiornamento della stessa, valutando come imprescindibile un intervento di adeguamento ai nuovi requisiti richiesti dal GDPR.

La Società ha, pertanto, predisposto la seguente modulistica, che si allega al presente Modello:

- comunicazioni al proprio personale dipendente, in ragione dell'organigramma in materia Privacy, contenenti espresse autorizzazioni al trattamento dei dati.
- atti di informazione, per dipendenti, candidati, fornitori, clienti e soggetti potenziali clienti, completi di raccolta del consenso ove necessario;
- questionario da inviare ai soggetti di volta in volta qualificabili come Responsabili o Titolari del Trattamento, volti alla verifica dell'adeguamento delle misure di sicurezza adottate alla normativa europea;

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL

- contratti con i soggetti di volta in volta qualificabili come Responsabili o Titolari del Trattamento (nomine e manleve).

5.3. Aggiornamento

La Società, utilizzando il documento di cui al precedente paragrafo 4.4, provvede a mantenere costantemente aggiornato il proprio Sistema di Gestione della Privacy; in particolare, ogni volta che insorga una variazione nel ciclo di trattamenti effettuati o nelle categorie di dati utilizzati, valuta l'eventuale presenza di nuovi rischi e pianifica le conseguenti misure aggiuntive che si dovessero rendere necessarie.

Allegati:

1) Relazione di Mappatura dei Trattamenti, Valutazione del Rischio e Gap Analisys
2) Policy aziendali
3) Regolamento per il corretto utilizzo del Sistema Informativo Aziendale
4) RAT Titolare/RAT Responsabile
5) Moduli autorizzazione al trattamento dati
6) Moduli Informative e raccolta consenso ove necessario
7) Documentazione relativa alla selezione, nomina e monitoraggio dei Responsabili del trattamento

UPM MODENA spa
via Bottego, 50 • 41126 Modena
tel. +39 059 346699 • info@upm-italy.com • www.upm-italy.com
PI. - C.F. - R.I. 00941030363 | SDI: 2LCMINU | N. REA MO-439182 | R.A.E.E. IT08020000003219 | cap. soc. € 1.000.000 (i.v.)
Società soggetta ad attività di direzione e coordinamento di BROWNS & BROWNS SRL