

N° rev	Date	Descrizione	Rif. Paragr.
0	12/10/2021	Prima emissione	
1	15/12/2023	Revisione Generale	
2	03/03/2025	Adeguamento alla Direttiva NIS 2	13

MODELLO ORGANIZZATIVO PRIVACY GLENNAIR ITALIA S.P.A.

Regolamento UE 2016/679

D.Lgs n. 196/2003, aggiornato al D.Lgs n. 101/2018



*- PROCEDURE e BEST
PRACTICES –*

*per un corretto trattamento dei dati
personali*

1 Premessa

Il presente Modello Organizzativo raccoglie le misure tecniche e organizzative che Glenair Italia attua per garantire – e dimostrare - la conformità al Regolamento UE 2016/679 e alla normativa italiana in materia di trattamento dei dati personali delle persone fisiche che la Società pone in essere direttamente o mediante soggetti terzi che effettuino un trattamento per suo conto.

Il Regolamento UE 2016/679 del 27 aprile 2016, “GDPR”, diviene definitivamente operativo e applicabile a partire dal 25 maggio 2018 in tutti i Paesi membri dell’Unione Europea e persegue il fine di rafforzare la protezione dei dati personali delle persone fisiche, sia all'interno che all'esterno dei confini europei, dunque a prescindere dal principio di territorialità, armonizzando le regole privacy di tutti gli Stati membri.

L’adozione di misure tecniche ed organizzative adeguate è imposta al Titolare dagli artt. 24e seguenti del GDPR, ai sensi dei quali le politiche interne e le misure da attuare per soddisfare i principi della protezione dei dati fin dalla fase di progettazione e della protezione dei dati di default, devono tener conto, in concreto, della natura, dell’ambito di applicazione, del contesto e delle finalità di trattamento nonché del rischio di ledere i diritti e le libertà delle persone fisiche coinvolte.

Al fine di rispettare tale requisito, Glenair Italia ha voluto elaborare il presente Modello Organizzativo che ha richiesto la preventiva esecuzione di un’attenta e critica attività di auditing interno, la quale ha consentito la verifica di ogni singola Unit aziendale e che mira ad una gestione lecita e trasparente del dato personale trattato.

Il presente Modello Organizzato viene revisionato e aggiornato dal Referente Privacy e approvato dal Titolare.

2 Obiettivi

L’obiettivo del presente Modello Organizzativo Privacy è di garantire e dimostrare che il trattamento dei dati personali da parte di Glenair Italia avviene in modo lecito, corretto e trasparente secondo i parametri giuridici individuati dal GDPR, raggiungibile attraverso la realizzazione di una gestione interna organizzata e strutturata.

Glenair Italia promuove nei propri Collaboratori una cultura della privacy e della tutela e sicurezza dei dati personali, consolidando quei principi comportamentali idonei a garantire la trasparenza, la sicurezza e la correttezza dei trattamenti effettuati, aumentando la propria affidabilità verso i propri

clienti, partners strategici, dipendenti ed interessati.

Il presente Modello Organizzativo si compone di n. 14 Sezioni dirette a fornire una panoramica sul sistema complessivo delle misure tecniche e organizzative che, sulla base delle concrete esigenze sistematiche ed operative del Glenair Italia, si ritengono adeguate, contenendo i principi, le regole organizzative e gli strumenti di controllo per garantire il trattamento lecito, corretto e trasparente dei dati personali.

Il presente Modello Organizzativo mira a rafforzare l'etica sul lavoro che contraddistingue il Personale che collabora con Glenair Italia.

Per Glenair Italia è fattore di competitività poter ambire ad una corretta gestione del dato personale durante lo svolgimento del proprio operato.

Il M.O.P. di Glenair Italia vuole infine evitare la possibile erogazione di sanzioni amministrative pecuniarie di cui all'art. 83 GDPR nonché di quelle penali di cui alla normativa nazionale potendo, con la sua adozione, dimostrare l'attuazione concreta, efficiente ed efficace delle misure tecniche e organizzative adeguate alla protezione dei dati personali da essa trattati, direttamente o tramite soggetti terzi che li effettuano per suo conto.

3 Principi per un corretto trattamento di dati personali

Il GDPR è costituito da tre principi ispiratori che permeano e sostengono l'intero comparto normativo ed il cui rispetto è protetto da un sistema sanzionatorio nei confronti di Titolari e Responsabili del trattamento.

Tali principi essenziali sono quelli di:

1. ***accountability***, ossia il principio di responsabilizzazione: il Regolamento non effettua una tipizzazione puntuale delle misure tecniche e organizzative, esprimendosi unicamente in termini di loro adeguatezza al rischio, "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche" (art. 32 GDPR). Si tratta di una innovazione profonda in quanto viene attribuito ai Titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento. Ciò impone un approccio integrato, che interessi tutte le BU aziendali, concreto e risk-based che dia luogo a comportamenti proattivi;

2. **privacy by design**, che impone l'adozione di misure di protezione fin dalla fase di progettazione del trattamento;

3. **privacy by default**, che prescrive un utilizzo che si limiti, per impostazione predefinita, ai soli dati necessari a rispondere alle finalità specifiche della gestione dei dati.

Glenair Italia ha voluto rendere propri i principi poco sopra delineati attraverso novità operative tra le quali:

a) l'istituzione del **Registro delle attività di trattamento** (art.30 GDPR e cons. 171) che costituisce il punto di partenza per la predisposizione dell'intero impianto documentale, deputato a raccogliere le evidenze, i controlli ed i processi che consentono di soddisfare l'accountability del sistema privacy;

b) Il **processo di gestione di un data breach**, (art. 33 e 34 GDPR) ossia l'analisi precipua e prodromica ad una eventuale notifica di una violazione dei dati personali, che richiede un'attenta analisi e conoscenza delle informazioni gestite, ma soprattutto investimenti organizzativi e tecnologici nelle modalità di monitoraggio, securizzazione e compartimentazione dei danni che ne possono derivare.

Diretto corollario dei sopra riferiti principi generali di accountability, privacy by design e privacy by default, è che la piena compliance al GDPR impone che il trattamento dei dati personali avvenga secondo i principi di liceità, correttezza e trasparenza.

Come nella precedente normativa, il trattamento è **lecito** allorché trovi fondamento in una base giuridica che, fermo restando in ogni caso l'obbligo di informativa a carico del Titolare del trattamento, può consistere in quanto segue:

1. consenso dell'interessato che deve essere libero, specifico, informato ed inequivocabile, non essendo ammesso il consenso tacito o presunto: deve, in altri termini, essere manifestato attraverso una "dichiarazione o azione positiva inequivocabile". Inoltre, per i dati "sensibili" di cui all'art. 9 GDPR, esso deve essere anche "esplicito", non necessariamente "documentato per iscritto" né da prestare in "forma scritta", sebbene tale modalità sia quella maggiormente idonea a dimostrare la sua prestazione, la sua inequivocabilità ed il suo essere "esplicito";
2. adempimento di obblighi contrattuali, ossia il trattamento è lecito se è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure

- precontrattuali adottate su richiesta dello stesso;
3. obblighi di legge cui è soggetto il titolare del trattamento, nel qual caso la finalità è specificata per legge;
 4. interessi vitali della persona interessata o di terzi: ossia se è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; utilizzabile però come base giuridica solo se nessuna delle altre condizioni di liceità può trovare concreta applicazione;
 5. legittimo interesse prevalente del titolare o di terzi cui i dati vengono comunicati, ossia quando il trattamento è necessario per il perseguimento dei legittimi interessi del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore;
 6. interesse pubblico o esercizio di pubblici poteri, ovvero necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento (tramite legge statale o dell'Unione) ed anche in tal caso la finalità deve essere specificata per legge.

Il trattamento dei dati personali è **corretto** se trasparente nei confronti degli interessati, ossia i dati personali devono essere trattati per scopi determinati, espliciti e legittimi, e senza scorrettezze o raggiri nei confronti degli interessati (essendo dunque vietata un'informazione confusa o parziale).

Quello della **trasparenza** non è solo un principio fondamentale del trattamento, ma anche un vero e proprio diritto dell'interessato: devono cioè essere trasparenti e corrette le modalità di raccolta dei dati e di utilizzo degli stessi.

Gli interessati devono essere informati in merito alle finalità del trattamento, alle modalità del trattamento e all'indirizzo del titolare del trattamento, prima che inizi il trattamento stesso. Le modalità del trattamento devono essere esplicitate in maniera comprensibile in modo che gli interessati siano in grado di capire cosa accadrà ai loro dati.

L'interessato deve avere a disposizione una procedura efficace e accessibile per consentirgli di ottenere l'accesso ai suoi dati in un tempo ragionevole, e quindi di conoscere se e quali dati sono detenuti dal titolare.

In questo senso, il Titolare ha un limite temporale (prorogabile in talune circostanze) per gestire e riscontrare l'esercizio di un diritto proposto da un Interessato.

4 Definizioni

Vengono illustrate le principali terminologie necessarie ad una corretta comprensione della normativa in materia di protezione dei dati personali delle persone fisiche.

1) **Dato Personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile (**Interessato**); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come:

- il nome o cognome,
- indirizzo e-mail,
- immagine e voce,
- un numero di identificazione (Carta d'Identità, Codice Fiscale, Passaporto ecc.),
- dati relativi all'ubicazione,
- un identificativo online,
- uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

2) **Dato Particolare:** qualsiasi informazione che riveli:

- l'origine razziale o etnica,
- le opinioni politiche,
- le convinzioni religiose o filosofiche,
- l'appartenenza sindacale,
- 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.

3) **Dato Giudiziario:** dati personali relativi alle condanne penali e ai reati o connesse a misure di sicurezza (giurisdizione penale).

4) **Trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come:

- 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
- 5) **Titolare del Trattamento:** la persona fisica o giuridica, che determina le finalità e i mezzi del trattamento di dati personali.
- 6) **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.
- 7) **Responsabile della Protezione Dati / Data Protection Officer:** soggetto designato in funzione delle proprie qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i seguenti compiti:
- informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla normativa
 - sorvegliare l'osservanza della normativa in materia di tutela dei dati personali
 - cooperare con l'Autorità di controllo
 - fungere da punto di contatto per l'Autorità di controllo
- 8) **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.
- 9) **Informativa:** documento con il quale vengono fornite all'interessato le seguenti informazioni:
- l'identità e i dati di contatto del titolare del trattamento
 - i dati di contatto del responsabile della protezione dei dati
 - le finalità del trattamento
 - gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali
 - l'intenzione del Titolare del trattamento di trasferire dati personali a un Paese terzo o a un'Organizzazione internazionale
 - il periodo di conservazione dei dati personali
 - i diritti dell'interessato (15-22 GDPR)
 - il diritto di proporre reclamo a un'Autorità di controllo (Garante per la protezione dei dati)

personali)

- la base giuridica del trattamento
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione

10) **Violazione dei dati personali c.d. Data Breach:** la violazione di sicurezza che comporta accidentalmente o in modo illecito:

- la distruzione,
- la perdita,
- la modifica,
- la divulgazione non autorizzata,
- l'accesso ai dati personali trasmessi, conservati o comunque trattati.

11) **Destinatario:** la persona fisica o giuridica che riceve comunicazione di dati personali.

12) **Archivio:** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati.

8 Richieste dell'interessato – esercizio di un diritto

8.1.1 Premessa

Il Titolare del trattamento ha incaricato un Referente Privacy Interno all'Azienda che ha la funzione di dare riscontro alle comunicazioni con cui gli interessati esercitano i propri diritti.

Salvo che il Titolare dimostri che non è in grado di identificare l'interessato, la persona incaricata dal Titolare dovrà fornire un riscontro senza ingiustificato ritardo, comunicando in maniera concisa, trasparente, intellegibile e con un linguaggio chiaro e semplice.

Il termine massimo per il riscontro a una richiesta dell'interessato è di un mese dal ricevimento. Tale termine può essere prorogato di due mesi, ove necessario, tenuto conto della complessità e dell'eventuale numero delle richieste pervenute. Il Titolare del trattamento, o la persona incaricata, informa l'interessato dell'eventuale proroga e dei motivi del ritardo entro un mese dal ricevimento della richiesta.

Nel caso in cui non si riesca ad ottemperare alla richiesta dell'interessato, quest'ultimo dovrà essere informato senza ritardo, al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo al Garante della Privacy o di proporre ricorso giurisdizionale alle Autorità competenti.

Ogniquale volta vi sia una richiesta di esercizio dei propri diritti da parte dell'interessato, occorre sempre assicurarsi che questo ne sia titolare.

Le comunicazioni di riscontro alle richieste dell'interessato sono gratuite. Ove le richieste

dell'interessato siano manifestamente infondate o eccessive, in particolare in caso di ripetitività, il Titolare può:

- Addebitare un ragionevole contributo spese tenendo conto degli eventuali costi amministrativi sostenuti per fornire un riscontro all'interessato;
- Rifiutare di soddisfare la richiesta. In questo caso il Titolare avrà l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta pervenuta.

Il Titolare del trattamento ha adottato misure idonee a fornire all'interessato tutte le informazioni che quest'ultimo possa richiedere, tramite la creazione di un indirizzo mail dedicato alle comunicazioni da parte degli interessati.

9 Violazione dei Dati Personali - Data Breach

9.1 Premessa

Glenair ha individuato nel Team IT e nel Referente Privacy (gdpr@glenair.it) le figure responsabili per l'Azienda deputate alla gestione delle Violazioni dei Dati Personali (Data Breach).

Per Data Breach o Violazione dei Dati Personali si intende una "violazione di sicurezza che comporta – in maniera accidentalmente o illecitamente - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Una violazione dei dati personali può compromettere la **riservatezza**, l'**integrità** o la **disponibilità** degli stessi.

10 Linee guida a protezione del Know How Aziendale

Glenair Italia, in ottica di tutela del proprio patrimonio digitale costituito da informazioni e dati personali, ha proceduto a far sottoscrivere ai propri Dipendenti e Collaboratori precisi accordi di riservatezza.

11 Criteri per la selezione dei responsabili esterni di Glenair Italia

Glenair Italia, al fine di assicurare che i propri dati personali vengano trattati applicando idonee misure di protezione da parte di fornitori e partner esterni ha regolato il flusso di tali dati mediante la predisposizione di Data Processing Agreement per ogni outsourcer aziendale e trasversale.

Il DPA disciplina e regola, in conformità ai requisiti imposti dall'art. 28 GDPR, le responsabilità del

partner in relazione al trattamento di dati effettuato per conto di Glencair Italia quale Titolare del Trattamento.

Per i nuovi Outsourcers, viene adottata la seguente procedura:

- 1) L'attività di trattamento che dovrà essere effettuata in outsourcing viene discussa preliminarmente con il Manager IT che valuterà i potenziali rischi del trattamento e avviserà il Titolare in caso di incongruenze con i requisiti imposti dalla normativa;
- 2) Una volta che il Partner è stato scelto tra quelli selezionati per l'espletamento dell'attività di trattamento in outsourcing, viene inoltrata una copia del contratto al Manager IT;
- 3) Il Manager IT predispose il DPA che andrà allegato alla bozza del contratto;
- 4) Nel momento in cui il DPA viene sottoscritto, una copia digitale viene archiviata nell'apposita cartella all'interno della cartella Modello Organizzativo Privacy.