# Regolamento recante disposizioni in materia di servizi aziendali di chat e messaggistica elettronica

Rif. Artt. 5, 6, 24, 25 e 32 Regolamento UE 2016/679 (GDPR)

| | |
|---|---|
| **Titolare del Trattamento** | Diocesi di Sabina – Poggio Mirteto |
| **Indirizzo sede legale** | Piazza Mario Dottori, 14 – 02047 Poggio Mirteto (RI) |
| **Codice Fiscale** | 91000810571 |
| **PEO** | diocesi@diocesisabina.it |
| **Responsabile** | S.E. Mons. Ernesto MANDARA |
| **DPO** | Giuliano PALOTTO |

| Edizione | Revisione | Data | Descrizione | il Titolare | il DPO |
|---|---|---|---|---|---|
| 1 | 0 | 04/03/2024 | Prima emissione | *approvato* | *verificato* |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**Documento di nr 6 pagine compresa la presente realizzato su format della**

# 1 PREMESSA

Le comunicazioni elettroniche scontano un livello ineliminabile di rischio e di insicurezza. Tale cornice di precarietà, stante l'inagibilità dell'opzione di bloccare lo scambio di comunicazioni elettroniche, induce il Titolare del trattamento, il responsabile del trattamento e tutti gli incaricati che ne facciano uso a ricorrere al maggior livello esigibile delle condotte di diligente precauzione.
Non vi è garanzia che tali condotte preventive possano scongiurare gli eventi dannosi e neppure che siano tali da evitare sanzioni amministrative da parte delle autorità di controllo. Peraltro, tale constatazione non può esimere dall'adottare le condotte preventive.
Le considerazioni finora condotte valgono anche per i sistemi di chat e messaggistica aziendali, siano essi gestiti direttamente dal Titolare del trattamento oppure provveduti da un fornitore di servizi esterno in outsourcing. Rispetto ad essi il pericolo maggiore da evitare è quello di cedere alle lusinghe della apparente facilità e velocità di utilizzo.
Solo una miopia organizzativa può tollerare una superficialità disposta a sottostimare e correre rischi così elevati di perdita della riservatezza, integrità e disponibilità del patrimonio informativo aziendale.
Va inoltre considerato che un utilizzo per scopi di prestazione lavorativa presuppone strumenti professionali e non strumenti destinati ad un uso domestico o per scopi strettamente personali con l'esclusione pertanto delle relative esimenti previste dall'art.2 par.1 lettera c) sull'ambito di applicazione del GDPR, fatto salvo la procedura BYOD che qui si richiama.
Queste le premesse sulle quali innestare gli adempimenti, di natura amministrativa e legale, connessi all'uso di sistemi di messaggistica aziendale, che vengono sintetizzate nel seguente regolamento.

# 2 ATTO DI DOCUMENTAZIONE DELLE SCELTE E COINVOLGIMENTO DEL DPO

Il Titolare del trattamento, per il tramite di questo, ha codificato l'utilizzo di determinati strumenti, apparecchi o servizi in quanto la possibilità di usare un apparato, quando ciò presenta rischi di accessi da parte di soggetti non autorizzati o che comunque non dovrebbero venire a conoscenza delle informazioni trattate, espone a pericoli di attacchi di terzi. In base al principio di "accountability", previsto dall'art.24 del GDPR, impone di predisporre idonee difese contro qualsiasi aggressore.
La prima barriera è rappresentata da un documento che deve dimostrare di essersi posti il problema che dia conto delle scelte tecniche utilizzate nonché delle misure di sicurezza applicate nel rispetto delle prescrizioni dell'art. 32 del GDPR.
Il Titolare del trattamento ha coinvolto il DPO informandolo sull'intenzione di avvalersi di un sistema di chat e/o messaggistica aziendale, atteso che il DPO deve essere coinvolto in relazione a qualsiasi aspetto relativo al trattamento dei dati personali ai sensi dell'articolo 38 del GDPR.

## 2.1 VALUTAZIONE DI IMPATTO PRIVACY

Questo documento ricomprende la valutazione di impatto privacy ai sensi dell'articolo 35 del GDPR, la quale è sempre richiesta prima di iniziare un trattamento di dati personali che possa comportare un rischio elevato per i diritti e le libertà delle persone interessate, consultando l´autorità di controllo nel caso in cui le misure tecniche e organizzative individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti, ovvero quando il rischio residuale per i diritti e le libertà degli interessati resti elevato. Sulla scorta di questo, si sono coinvolte le rappresentanze sindacali dei lavoratori in quanto trattasi di regolamento aziendale.

## 2.2 GARANZIE CONTRATTUALI DA EVENTUALE FORNITORE DI SERVIZI

Il Titolare del trattamento, in qualità di ente apicale al trattamento dei dati personali, è sempre responsabile dei mezzi usati per lo svolgimento di prestazioni lavorative, a prescindere dal fatto che abbia o meno la proprietà o la disponibilità dello strumento usato.
Per tale motivo, il Titolare del trattamento ha:

- descritto i mezzi usati;
- verificato le vulnerabilità;
- individuato e adottato le precauzioni per arginare le vulnerabilità;
- messo in atto un sistema di controlli circa l'effettivo utilizzo delle precauzioni.

Nel caso in cui i dispositivi e/o i relativi servizi utilizzati siano forniti da un venditore è stato verificato che il fornitore abbia curato la progettazione e il funzionamento dei dispositivi / servizi in conformità ai principi della privacy by design e della privacy by default prescritti dall'art. 25 del GDPR, curando la redazione e la sottoscrizione di apposite clausole di garanzia di conformità nei contratti di acquisto.
Nell'ipotesi in cui il fornitore non abbia curato la progettazione e il funzionamento dei dispositivi in conformità al GDPR e/o non rilasci garanzia su tale profilo, il Titolare del trattamento informerà il Responsabile e gli addetti tutti sul divieto di utilizzo dei dispositivi / servizi di quel fornitore.
Inoltre, quando si ricorre ad una piattaforma di chat e/o messaggistica elettronica in outsourcing, è il Titolare del trattamento provvede ad una attenta disamina legale delle condizioni contrattuali per verificare che i termini di servizio previsti dal venditore e la sua informativa sulla privacy non comportino criticità che siano incompatibili con le proprie policy aziendali in materia di protezione dei dati personali. Anche nel caso, assai ricorrente, in cui il sistema di chat e/o messaggistica aziendale si avvalga di servizi di hosting provider esterni o di sistemi di cloud computing, si può concretizzare un trasferimento di dati extra-UE, in tutto e per tutto soggetto alla specifica disciplina in materia.

## 2.3 TRATTATIVA SINDACALE/PROCEDURA AMMINISTRATIVA

L'utilizzo di qualsiasi strumento nel contesto lavorativo impone di verificare l'applicazione dell'articolo 4 della legge 300/1970 (Statuto dei lavoratori). Si ritiene che un punto di riferimento per l'interpretazione dell'articolo 4 sia rappresentato dal provvedimento n. 303 del 13 luglio 2016 del Garante per la protezione dei dati personali. In tale provvedimento il Garante ha chiarito quali strumenti possono essere considerati "strumenti di lavoro" non assoggettati alla preventiva procedura di accordo sindacale / autorizzazione amministrativa.
A tale fine sono strumenti di lavoro solo i servizi, software o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza.
Rientrano nella definizione di strumento di lavoro il servizio di posta elettronica e, per identità di funzione, il servizio di messaggistica offerto ai dipendenti con attribuzione di un account personale e gli altri servizi della rete aziendale, fra cui anche il collegamento a siti internet.
Costituiscono parte integrante di questi strumenti i sistemi di *logging* per il corretto servizio di posta elettronica, ma con conservazione dei soli dati esteriori, contenuti nella cosiddetta «*envelope*» del messaggio, per una breve durata (nel provvedimento citato il Garante ha indicato un termine non superiore ai sette giorni); lo stesso vale per i sistemi di filtraggio anti- virus che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui server per l'erogazione dei servizi di rete; idem per sistemi di inibizione automatica di contenuti in rete inconferenti con il lavoro, senza registrazione dei tentativi di accesso.
Al contrario non possono essere considerati strumenti di lavoro gli apparati e i sistemi software che consentono, con modalità non percepibili dall'utente (in background) e in modo del tutto indipendente rispetto alla normale attività, operazioni di monitoraggio, filtraggio, controllo e tracciatura costanti ed indiscriminati degli accessi ad internet o al servizio di posta elettronica e di chat e messaggistica aziendale. Gli apparati e sistemi, che non possono essere considerati strumenti di lavoro, non necessitano della procedura di accordo sindacale/autorizzazione amministrativa.
Ci sono poi altri strumenti come firewall o sistemi antintrusione, agenti su base statistica o con il ricorso a sorgenti informative esterne, che, non comportando un trattamento di dati dei dipendenti, sono fuori dal campo di applicazione dell'articolo 4 dello Statuto.
I dati raccolti mediante i controlli sugli strumenti di lavoro (oltre che sugli altri apparati se avallati dalla trattativa sindacale/autorizzazione amministrativa) possono essere utilizzati a tutti i fini connessi al rapporto di lavoro (quindi anche per fini disciplinari), purché sia data al lavoratore adeguata informazione:

- delle modalità d'uso degli strumenti e di effettuazione dei controlli e
- nel rispetto di quanto disposto dal Codice della privacy.

Come ha rilevato il Garante la possibilità del controllo dell'adempimento della prestazione, mediante gli strumenti di lavoro, diventa un effetto naturale del contratto: una possibilità, però, non illimitata, in quanto valgono le prescrizioni sulla trasparenza delle informazioni, sulla proporzionalità e liceità del controllo e sulla tutela della dignità del lavoratore.

### 2.4 SESSIONI DI ISTRUZIONE E FORMAZIONE DEL DIPENDENTE

Ai sensi degli articoli 29 e 32 del GDPR la persona autorizzata al trattamento (c.d. incaricato) deve essere istruita, e quando necessario aggiornata, a riguardo delle modalità del trattamento effettuato tramite i sistemi di chat e messaggistica aziendali, ed essa deve essere opportunamente resa edotta dei rischi connessi al trattamento, nonché delle precauzioni a suo carico.
Le medesime istruzioni assumono rilievo ai fini dell'articolo 4, comma 3, della legge 300/1970.
Tali istruzioni sono parte integrante di sessioni formative da realizzare ai sensi e per gli effetti dell'articolo 39, paragrafo 1, lettera b) del GDPR.
Anche a riguardo di tali incombenze di formazione e istruzione è necessario il coinvolgimento del DPO.

## 3 VALUTAZIONE DI IMPATTO

### 3.1 DESCRIZIONE DEI MEZZI USATI

Ai fini del presente si intendono quali mezzi hardware utilizzati computer, tablet, portatili, iphone, smartphone, cellulari ed altri mezzi elettronici:

- di proprietà del Titolare del trattamento ovvero noleggiati o in leasing operativo;
- non di proprietà del Titolare del trattamento ma utilizzati secondo la procedura BYOD.

Ai fini del presente si intendono quali mezzi software utilizzati:

- servizi di posta elettronica ordinaria e certificata;
- servizi di messaggistica (SMS);
- servizi di messaggistica "chat" (es. WhatsApp, Telegram, Signal, ecc.).

Ai fini del presente si intendono quali mezzi software da NON utilizzare:

- servizi social (es. Facebook, Instagram, Twitter, ecc.)

### 3.2 VERIFICA DELLE VULNERABILITÀ

I mezzi (hardware e software) indicati al paragrafo precedente quali "utilizzabili" sono da considerarsi sicuri sulla scorta delle vulnerabilità individuate nelle valutazioni precedenti, ovvero dalla disamina delle condizioni di utilizzo e dell'informativa sul trattamento dei dati personali redatta dal fornitore e delle precauzioni da adottarsi indicate al paragrafo successivo.

### 3.3 INDIVIDUAZIONE E ADOZIONE DELLE PRECAUZIONI PER ARGINARE LE VULNERABILITÀ

Le precauzioni da adottare al fine di arginare le vulnerabilità sono individuate in:

- ✓ utilizzo di sistemi di accesso a riconoscimento per i dispositivi hardware;
- ✓ utilizzo di login e password per i servizi di posta elettronica ordinaria e certificata;
- ✓ utilizzo costante di backup;
- ✓ utilizzo delle procedure di disaster recovery secondo le indicazioni degli Amministratori di Sistema;
- ✓ utilizzo sistematico di antivirus, antispam e firewall di ultima generazione aggiornati all'ultima versione disponibile.

### 3.4 SISTEMA DI CONTROLLI CIRCA L'EFFETTIVO UTILIZZO DELLE PRECAUZIONI

Al fine di controllare l'effettivo uso delle precauzioni è fatto obbligo al Responsabile del trattamento e agli incaricati di segnalare eventuali disfunzioni delle precauzioni sopra indicate, invero di segnalare eventuali precauzioni suppletive rispetto a quelle indicate.
Annualmente, in fase di Audit, saranno campionati alcuni incaricati onde valutare il grado di efficacia ed efficienza delle precauzioni predisposte.

# 4 REVISIONE DELL'ATTO DI AUTORIZZAZIONE DEL DIPENDENTE

L'atto di autorizzazione al trattamento è l'atto fondante la legittimità delle operazioni effettuate dal dipendente. Per la natura autorizzativa ad esso propria è opportuna la maggiore analiticità possibile nella specificazione dell'ambito del trattamento autorizzato. Nel concetto di ambito di trattamento rientrano le base di dati accessibili dal singolo autorizzato e le operazioni per il quale il singolo dipendente è autorizzato. Qualora tali operazioni incrementino o diversifichino il livello di rischio è opportuno che sia integrato l'atto di autorizzazione.
Tale evenienza ricorre a proposito del sistema di chat e/o messaggistica aziendale e la detta integrazione ha per oggetto le specifiche istruzioni conformate all'utilizzo della stessa.
L'atto di autorizzazione al trattamento è ricompreso nel contratto in subordine o professionale tra il Titolare del trattamento ed il Responsabile e/o gli incaricati, completato dalle disposizioni e istruzioni impartite nel corso dello svolgimento della prestazione lavorativa

# 5 REVISIONE DEL MANUALE DELLA SICUREZZA AD USO DEGLI AUTORIZZATI

Qualora, come opportuno, l'apparato documentale "*privacy*" adottato dal Titolare del trattamento preveda un manuale della sicurezza ad uso degli autorizzati, le precauzioni e le prescrizioni connesse al sistema di chat e/o messaggistica aziendale sono inserite in un apposito paragrafo e della nuova edizione del manuale deve essere data informazione a tutto il personale. Il presente, portato a conoscenza del Responsabile e degli incaricati, ha valenza di integrazione manuale della sicurezza ad uso degli autorizzati a proposito del sistema di chat e/o messaggistica aziendale.

# 6 REVISIONE/INTEGRAZIONE DEL REGISTRO DEI TRATTAMENTI

Il registro dei trattamenti è la fotografia dei trattamenti e nello stesso è necessario inserire i contenuti previsti dall'articolo 30 del GDPR. Ciò non esclude che nello stesso sia possibile inserire dati ulteriori. Il registro dei trattamenti riferisce anche in merito all'utilizzo della chat e/o messaggistica aziendale, dei sistemi utilizzati e della sintesi delle condizioni di sicurezza.

# 7 AGGIORNAMENTO DEL CODICE DISCIPLINARE

Le prescrizioni (obblighi e divieti) a carico dei lavoratori a proposito del sistema di chat e/o messaggistica aziendale non comportano la necessità di integrare o specificare il codice disciplinare aziendale, in quanto la precisazione circa le violazioni espongono il lavoratore all'applicazione di provvedimenti disciplinari a suo carico - le cui descrizioni e relative entità delle sanzioni previste sono indicate nello stesso disciplinare – già ricomprendono l'uso illecito di dati personali attraverso l'utilizzo di mezzi elettronici hardware e software sia di proprietà del Titolare del trattamento, sia secondo la procedura BYOD. Tale disposto è portato a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti (es. chat aziendale) a norma dell'art. 7 della Legge 300/1970 (Statuto dei Lavoratori).

# 8 VERBALE DI CONSEGNA/UTILIZZO DEL DISPOSITIVO E IMPEGNO AL RISPETTO DELLE CONDIZIONI D'USO PRESCRITTE

Rientra nell'ambito delle precauzioni di ordine generale a proposito dei beni aziendali verbalizzare la consegna degli stessi e far sottoscrivere al dipendente l'impegno ad osservare obblighi e divieti specifici. In linea con quanto sopra indicato, il presente ricomprende anche la verbalizzazione circa l'utilizzo per scopi di chat e/o messaggistica aziendale di dispositivi aziendali e/o BYOD di proprietà del dipendente, con le relative precauzioni di utilizzo e impegno al rispetto.

# Sommario