CIRCOLARE N. 1-2021

"Servizi aziendali di chat e messaggistica elettronica con il Gdpr"

PREMESSA

1. ATTO DI DOCUMENTAZIONE DELLE SCELTE E COINVOLGIMENTO DEL DPO
2. VALUTAZIONE DI IMPATTO PRIVACY
3. GARANZIE CONTRATTUALI DA EVENTUALE FORNITORE DI SERVIZI
4. TRATTATIVA SINDACALE/PROCEDURA AMMINISTRATIVA
5. SESSIONI DI ISTRUZIONE E FORMAZIONE DEL DIPENDENTE
6. REVISIONE DELL'ATTO DI AUTORIZZAZIONE DEL DIPENDENTE
7. REVISIONE DEL MANUALE DELLA SICUREZZA AD USO DEGLI AUTORIZZATI
8. REVISIONE/INTEGRAZIONE DEL REGISTRO DEI TRATTAMENTI
9. AGGIORNAMENTO DEL CODICE DISCIPLINARE
10. VERBALE DI CONSEGNA/UTILIZZO DEL DISPOSITIVO E IMPEGNO AL RISPETTO DELLE CONDIZIONI D'USO PRESCRITTE

FEDERPRIVACY – Associazione Professionale ai sensi della Legge 4/2013, iscritta nel Registro del Ministero dello Sviluppo Economico - Sede: Via Degli Innocenti, 2 50063 Figline Valdarno (FIRENZE) ITALY - Codice Fiscale 94156260484 - Partita Iva IT06413480481 – Tel. +39 055 5276058 – **Numero Verde 800910424** – Fax +39 055 5609184 - Web: **www.federprivacy.org** - Email: **urp@federprivacy.org** - Pec: **federprivacy@pec.it**- Skype: **Federprivacy** - Twitter: **@Federprivacy**

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 le organizzazioni pubbliche e private 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 datore di lavoro 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.

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 decalogo.

1. ATTO DI DOCUMENTAZIONE DELLE SCELTE E COINVOLGIMENTO DEL DPO

Il datore di lavoro deve mettere nero su bianco l'utilizzo di determinati strumenti, apparecchi o servizi. Non bisogna dare per scontato la possibilità di usare un apparato, soprattutto quando ciò espone a rischi di accessi da parte di soggetti non autorizzati o che comunque non dovrebbero venire a conoscenza delle informazioni trattate, nonché a pericoli di attacchi di terzi.

Va sempre ricordato, infatti, che in base al principio di "accountability" previsto dall'art.24 del Gdpr, le norme sulla protezione dei dati personali rimproverano e puniscono chi non ha predisposto idonee difese contro qualsiasi aggressore. L'aggredito è sempre sanzionato se non si dà cura di erigere barriere.

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.

FEDERPRIVACY – Associazione Professionale ai sensi della Legge 4/2013, iscritta nel Registro del Ministero dello Sviluppo Economico - Sede: Via Degli Innocenti, 2 50063 Figline Valdarno (FIRENZE) ITALY - Codice Fiscale 94156260484 - Partita Iva IT06413480481 – Tel. +39 055 5276058 – **Numero Verde 800910424** – Fax +39 055 5609184 - Web: **www.federprivacy.org** - Email: **urp@federprivacy.org** - Pec: **federprivacy@pec.it**- Skype: **Federprivacy** - Twitter: **@Federprivacy**

Nei casi in cui è stato designato il Data Protection Officer, (*Vedasi la* ***Circolare 1-2017*** *"Casi di nomina obbligatoria del responsabile della protezione dei dati nel Regolamento UE 2016/679"*), il datore di lavoro deve coinvolgerlo 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.

Anche l'utilizzo della messaggistica a mezzo di dispositivi del datore di lavoro o dei dipendenti per il trattamento dei dati personali in ambito aziendale è un evento rispetto al quale deve essere coinvolto il Dpo.

2. VALUTAZIONE DI IMPATTO PRIVACY

Un documento specifico da adottare prima dell'utilizzo di un sistema di chat e/o messaggistica aziendale, comunque realizzato, è 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. (*Vedasi la* ***Circolare n. 5-2017*** *"Applicare le disposizioni sulla valutazione d'impatto sulla protezione dei dati"*)

Si suggerisce di considerare questo adempimento come imprescindibile e di coinvolgere le rappresentanze sindacali dei lavoratori.

Si rammenta che la valutazione di impatto privacy ha una forte componente giuridica e include la predisposizione di meccanismi organizzativi per attenuare o indennizzare eventuali danni.

3. GARANZIE CONTRATTUALI DA EVENTUALE FORNITORE DI SERVIZI

Il datore di lavoro è sempre responsabile dei mezzi usati per lo svolgimento di prestazioni lavorative.

Questo vale a prescindere dal fatto che il datore di lavoro abbia o meno la proprietà o la disponibilità dello strumento usato. Questo impone al datore di lavoro di:

a) descrivere i mezzi usati;
b) verificare le vulnerabilità;
c) individuare e adottare le precauzioni per arginare le vulnerabilità;
d) controllare l'effettivo utilizzo delle precauzioni.

Nel caso in cui i dispositivi e/o i relativi servizi utilizzati siano forniti da un venditore occorre verificare se 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.

FEDERPRIVACY – Associazione Professionale ai sensi della Legge 4/2013, iscritta nel Registro del Ministero dello Sviluppo Economico - Sede: Via Degli Innocenti, 2 50063 Figline Valdarno (FIRENZE) ITALY - Codice Fiscale 94156260484 - Partita Iva IT06413480481 – Tel. +39 055 5276058 – **Numero Verde 800910424** – Fax +39 055 5609184 - Web: **www.federprivacy.org** - Email: **urp@federprivacy.org** - Pec: **federprivacy@pec.it**- Skype: **Federprivacy** - Twitter: **@Federprivacy**

In ogni caso la responsabilità di utilizzo di tali dispositivi/servizi è a carico del titolare del trattamento.

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, sarà comunque onere del datore di lavoro conformare l'utilizzo degli stessi agli standard normativi del Gdpr.

Inoltre, quando si ricorre ad una piattaforma di chat e/o messaggistica elettronica in outsourcing, è sempre raccomandata 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.

Il soggetto che decide di avvalersi di tali servizi per un proprio sistema di chat e/o messaggistica aziendale ha la responsabilità della scelta di un fornitore affidabile che deve operare in conformità alla normativa sulla protezione dei dati personali, ivi includendo la preoccupazione circa l'eventuale trasferimento dei dati extra-UE e la sussistenza dei presupposti legali per procedervi in modo lecito. *(Vedasi la **Circolare N.3-2020** "La disciplina sul trasferimento dei dati personali extra-UE")*

4. 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.

FEDERPRIVACY – Associazione Professionale ai sensi della Legge 4/2013, iscritta nel Registro del Ministero dello Sviluppo Economico - Sede: Via Degli Innocenti, 2 50063 Figline Valdarno (FIRENZE) ITALY - Codice Fiscale 94156260484 - Partita Iva IT06413480481 – Tel. +39 055 5276058 – **Numero Verde 800910424** – Fax +39 055 5609184 - Web: **www.federprivacy.org** - Email: **urp@federprivacy.org** - Pec: **federprivacy@pec.it**- Skype: **Federprivacy** - Twitter: **@Federprivacy**

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 a 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, 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.

Si rammenta che 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.

5. SESSIONI DI ISTRUZIONE E FORMAZIONE DEL DIPENDENTE

Ai sensi degli articoli 29 e 32 del Gdpr la persona autorizzata al trattamento 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.

È opportuno che le specifiche istruzioni siano inserite in un documento messo a disposizione dell'autorizzato, di cui si sia in grado di dimostrarne la consegna o la conoscibilità.

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, se nominato.

6. 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.

FEDERPRIVACY – Associazione Professionale ai sensi della Legge 4/2013, iscritta nel Registro del Ministero dello Sviluppo Economico - Sede: Via Degli Innocenti, 2 50063 Figline Valdarno (FIRENZE) ITALY - Codice Fiscale 94156260484 - Partita Iva IT06413480481 – Tel. +39 055 5276058 – **Numero Verde 800910424** – Fax +39 055 5609184 - Web: **www.federprivacy.org** - Email: **urp@federprivacy.org** - Pec: **federprivacy@pec.it**- Skype: **Federprivacy** - Twitter: **@Federprivacy**

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.

7. REVISIONE DEL MANUALE DELLA SICUREZZA AD USO DEGLI AUTORIZZATI

Qualora, come opportuno, l'apparato documentale "privacy" adottato presso il 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 devono essere inserite in un apposito paragrafo e della nuova edizione del manuale deve essere data informazione a tutto il personale.

8. 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.

È del tutto opportuno che nel registro dei trattamenti si riferisca dell'utilizzo della chat e/o messaggistica aziendale, dei sistemi utilizzati e della sintesi delle condizioni di sicurezza.

9. AGGIORNAMENTO DEL CODICE DISCIPLINARE

Le prescrizioni (obblighi e divieti) a carico dei lavoratori a proposito del sistema di chat e/o messaggistica aziendale comportano la necessità di integrare o specificare il codice disciplinare aziendale, precisando che le violazioni delle stesse espongono il lavoratore all'applicazione di provvedimenti disciplinari a suo carico, le cui descrizioni e relative entità delle sanzioni previste è opportuno che siano esattamente indicate nello stesso disciplinare, il quale deve essere portato a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti a norma dell'art. 7 della Legge 300/1970 (Statuto dei Lavoratori).

10. 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 è necessario verbalizzare anche l'utilizzo per scopi di chat e/o messaggistica aziendale di dispositivi di proprietà del dipendente, con le relative precauzioni di utilizzo, alle quali impegnare il dipendente stesso.

FEDERPRIVACY – Associazione Professionale ai sensi della Legge 4/2013, iscritta nel Registro del Ministero dello Sviluppo Economico - Sede: Via Degli Innocenti, 2 50063 Figline Valdarno (FIRENZE) ITALY - Codice Fiscale 94156260484 - Partita Iva IT06413480481 – Tel. +39 055 5276058 – **Numero Verde 800910424** – Fax +39 055 5609184 - Web: **www.federprivacy.org** - Email: **urp@federprivacy.org** - Pec: **federprivacy@pec.it**- Skype: **Federprivacy** - Twitter: **@Federprivacy**