Regolamento per la gestione delle comunicazioni interne/esterne e per il trattamento dei dati personali delle persone fisiche e delle informazioni riservate/proprietarie della committenza

Indice delle Revisioni		
Rev	Data	Motivazione
0	14/02/2018	Emissione del documento
1	23/05/2019	Inserimento attività CAB_NB 305
2	10/01/2024	Integrazione risposta rilievi Accredia – MIMIT del 15/12/2023
3	30/05/2024	Aggiornato Par. 4.2
4	29/08/2024	Eliminate le indicazioni per la comunicazione efficacie (da gestire come istruzioni interne)

Sommario

0 - Introduzione al regolamento

Il presente regolamento, unitamente agli All.1 Organigramma nominativo e All.2 Funzionigramma, nella loro ultima revisione, fornisce le indicazioni a tutto il personale aziendale per la gestione delle comunicazioni e delle informazioni/dati con particolare riferimento:

all'utilizzo degli strumenti di comunicazione elettronica interna/esterna,

all'applicazione di regole comuni di gestione (acquisizione/archiviazione/trattamento) delle informazioni, dei dati e delle comunicazioni in/out.

1 – Responsabilità

Tutto il SGQ aziendale si basa sulla responsabilità di tutto il personale che è stato formato e informato:

- sulla struttura gerarchica aziendale (Organigramma),
- sul proprio ruolo e sui compiti assegnati (Funzioni gramma),
- sulle proprie interfacce di riferimento,
- sulle aspettative dell'azienda relativamente al proprio ruolo,
- sugli obiettivi di miglioramento stabiliti per la propria area di competenza,
- sulle azioni di contenimento dei rischi significativi derivanti dalla propria attività,
- sull'applicazione del metodo RBT (Risk Based Thinking) nell'ambito del processo decisionale riferito al proprio ruolo

Ogni persona in azienda in è pienamente responsabile:

- dell'esecuzione dei propri compiti;
- della corretta esecuzione dei compiti assegnati ai propri sottoposti:
    - fornendo le giuste indicazioni e istruzioni (scritte o verbali);
    - segnalando, al proprio diretto superiore, eventuali anomalie di comportamento del personale sotto la propria diretta responsabilità;
- dell'individuazione delle aree di miglioramento riferite sia alle attività specifiche del proprio ruolo/funzione che all'interazione con le altre funzioni/processi aziendali e della segnalazione delle proposte conseguenti al proprio diretto superiore;
- delle decisioni prese in autonomia in funzione del ruolo e dei compiti assegnati;
- della costante comunicazione e interazione con il personale dei reparti aziendali per i quali può essere sia fornitore che cliente interno, acquisendo i dati di input necessari alla corretta esecuzione del proprio lavoro e fornendo gli output necessari agli altri reparti per eseguire a loro volta correttamente i propri compiti.

NB

La responsabilità della corretta applicazione delle disposizioni generali per la gestione delle comunicazioni interne/esterne e per il trattamento dei dati personali delle persone fisiche e delle informazioni riservate/proprietarie della committenza da parte del personale interno è del Legale Rappresentate (facente funzione di titolare-responsabile del trattamento – RPD/DOP) che ne effettua un monitoraggio costante per tramite dei Direttori di Settore che sono stati a loro volta delegati come Sub-Responsabili anche ai sensi del DECRETO LEGISLATIVO 10 agosto 2018, n. 101.

I Responsabili dei diversi processi aziendali, ed in particolare il personale Dirigente, hanno l'obbligo di gestire le comunicazioni con gli operatori e quelle con la committenza nel rispetto dei requisiti deontologici di riservatezza, e delle disposizioni previste dal presente regolamento, anche tramite appositi interventi formativi/informativi dei quali deve essere tenuta evidenza documentata.

2 – Informazioni documentate e documenti di registrazione

Premesso che:

- Premesso che:
- Il Legale Rappresentante e i Direttori di settore sono in possesso delle competenze previste dalla normativa vigente per le attività di Coordinamento e Controllo delle attività di gestione delle comunicazioni interne/esterne e per il trattamento dei dati personali delle persone fisiche e delle informazioni riservate/proprietarie della committenza;
- l'azienda è supportata nei processi gestionali ed amministrativi da:
    - un Software Gestionale (Contabilità aziendale e registrazione processo di emissione certificati rif Circ. 7617)
    - registrazioni informatiche del SGQ strutturate su misura per le esigenze aziendali che coprono i principali processi gestionali e produttivi considerati significativi in base al Risk Assessment;
    - una rete LAN gestita tramite SQL - Server
- tutto il personale dotato di terminale collegato alla rete aziendale dispone di pacchetto Sw Office completo di applicazione Outlook per la gestione delle comunicazioni interne e esterne e altre applicazioni Sw funzionali all'esecuzione dei servizi offerti (in varie release come indicato nell'allegato All.E "Valutazione d'impatto sulla protezione dei dati);
- i Responsabili dei diversi processi aziendali hanno, oltre al SWG, la possibilità di utilizzare apposito spazio dedicato sui server di stabilimento per l'archiviazione dei documenti prodotti e delle comunicazioni in/out;
- l'azienda ha valutato i rischi derivanti da una eccessiva burocratizzazione dei propri processi gestionali e le opportunità derivanti da una gestione controllata degli stessi tramite gli strumenti di comunicazione e interna disponibili.

Le Informazioni documentate che l'organizzazione ha stabilito di predisporre e conservare a supporto delle attività oggetto del presente regolamento, soddisfano i requisiti di garanzia della piena corrispondenza delle attività svolte ai requisiti cogenti in materia di Privacy e Riservatezza;

I documenti predisposti ai sensi del presente regolamento comprendono:

All. E PIA (Privacy Impact Assessment)

All. E.1 (Privacy policy - Informativa privacy)

All. E.2 (Cookie Policy - Informativa estesa sull'uso dei cookie-web information)

I documenti direttamente correlati al presente regolamento con richiami alla Privacy e Riservatezza con valore d'informazione per le parti interessate sono:

Reg-1 u.r. Gestione Informazioni documentate

Reg3b All1 u.r. Condizioni generali di contratto

Oltre al presente regolamento, le comunicazioni interne svolgono funzione di Informazioni documentate[1] quando assumono valore:

- di disposizioni interne
- di documenti di registrazione dei processi/attività svolte anche in relazione alle azioni correttive e di miglioramento

I principali strumenti di comunicazione con valore di informazione documentata sono riconducibili a:

- E-mail interne/esterne;
- Archivi elettronici (con funzione di repository e interscambio)
- Avvisi e registrazioni incontri formativi/informativi

[1] *Questo tipo di informazioni documentate sono definiti documenti specifici di livello inferiore ed hanno lo scopo di comunicare le informazioni necessarie all'organizzazione stessa per operare (Vedere p.to 4.4. ISO 9001:2015).*

2.1 Dati personali e Informazioni riservate

Tutte le informazioni documentate/registrazioni tramite le quali sia possibile identificare, direttamente o indirettamente, un individuo sono soggette a specifico trattamento/protezione in base a specifica "gap analysis" effettuata in sede Risk Assessment (Privacy Impact Assessment – PIA) nel corso della quale sono stati considerati i seguenti dati "personali" in riferimento al personale interno (inclusi i collaboratori), alla committenza e ai fornitori (elenco non esaustivo ...):

- Nome e Cognome
- Numeri e codici identificativi (Codice fiscale, numero della tessera sanitaria, ...)
- Indirizzo e-mail
- Informazioni mediche e/o relative alla sfera fisica, fisiologica o genetica
- Informazioni relative alla localizzazione geografica
- Informazioni bancarie
- Reddito
- Profilo culturale/professionale (incluso ruolo e azienda di appartenenza)
- Indirizzi IP
- Cookies

Oltre alle informazioni documentate contenenti dati personali, sono soggette a specifico trattamento/protezione in base a specifica "gap analysis" effettuata in sede Risk Assessment **le informazioni riservate** dei committenti acquisite e registrate nell'esercizio delle attività di certificazione e prova; fanno eccezione quelle informazioni per le quali la Tecnocontrolli sia tenuta per legge o sia autorizzata da accordi contrattuali a divulgare dette informazioni riservate; nel caso specifico la Tecnocontrolli provvederà sempre ad avvertire il committente o la persona interessata salvo eventuale diversa prescrizione delle autorità richiedenti.

3 – Identificazione, rintracciabilità e trattamento delle comunicazioni interne/esterne, dei dati personali e delle informazioni riservate

3.1 comunicazioni interne/esterne

Il Mezzo principale di comunicazione sia interno che verso l'esterno è l'e-mail.

Tutte le e-mail scambiate internamente tra le funzioni e quelle in/out con l'esterno devono essere identificate, anche ai fini della successiva rintracciabilità, come minimo con:

- mittente;
- destinatario principale;
- destinatario/i per conoscenza "Cc" (ove necessario);
- destinatario/i per conoscenza in copia nascosta "Ccn" (ove necessario);
- un oggetto univoco che individui sinteticamente il contenuto;
- data di invio;
- richiesta di ricevuta di ritorno per avvenuta lettura;
- la priorità in funzione dell'urgenza e del "peso" del contenuto;

Per alcune comunicazioni interne di programmazione e pianificazione urgente così come le variazioni alle disposizioni già esecutive può essere utilizzata anche l'Applicazione WhatsApp disponibile su tutti i dispositivi mobili (smartphone) aziendali in dotazione al personale

Le comunicazioni dispositive "urgenti" gestite tramite WhatsApp devono essere emesse dal Responsabile che le ha in gestione il servizio oggetto di comunicazione;

queste devono:

a. includere l'identificazione e la descrizione appropriata;
b. essere destinate esclusivamente ai diretti interessati dalle disposizioni contenute (corretta distribuzione)
c. prevedere sempre un feedback di ricevuta/accettazione (non esclusivamente la spunta di lettura automatica);
d. essere conservate per l'eventuale per futura reperibilità;

queste non devono:

contenere dati e/o informazioni di tipo personale sui soggetti interni/esterni interessati dalla disposizione impartita ma solamente i riferimenti alle attività da svolgere nell'ambito del servizio oggetto di comunicazione.

3.2 informazioni riservate

La Tecnocontrolli in qualità di CAB è tenuta alla riservatezza sulle informazioni acquisite nel corso dello svolgimento delle verifiche/visite ispettive sulle attività, sulla struttura organizzativa e sul personale delle aziende committenti;

L'impegno alla riservatezza e richiamato a livello contrattuale tramite i riferimenti al Reg3a_All1 ur_Condizioni generali di contratto (Cap. 5.2 Obblighi dell'Organismo).

Le sole informazioni pubbliche sono relative ai certificati emessi in funzione delle attività verifica e prova eseguite dalla Tecnocontrolli.

La documentazione di registrazione delle evidenze raccolte in sede di verifica e/o di prova è destinata solo alla dimostrazione dei risultati che hanno portato all'emissione dei certificati e, a seconda dei casi, posso/devono essere allegate ai certificati emessi, archiviate e rese disponibili alle Autorità preposte alla verifica del corretto e conforme comportamento dell'ODC e dei Laboratori alla normativa cogente.

La tempistica di archiviazione e definita dal Reg-1(Gestione Informazioni documentate)

3.3 dati personali

La Tecnocontrolli gestisce i dati "personali" in ottemperanza alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, così come aggiornato con le rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 201.

Per la definizione della conformità al suddetto regolamento è stata effettuato uno specifico "Privacy Impact Assessment – PIA" tramite il quale:

- è stata effettuata una mappatura completa dello stato dell'arte dei dispositivi tecnologici (HW e SW) in dotazione;
- sono stati individuati:
    - gli scopi del trattamento;
    - le basi legali che rendono lecito il trattamento;
    - l'adeguatezza, la pertinenza e i limiti in relazione alle finalità del trattamento;
    - le modalità di aggiornamento;
    - il periodo di conservazione;
    - le modalità di informazione degli interessati in merito al trattamento e di acquisizione del consenso;
    - i diritti degli interessati e le modalità di esercizio di tali diritti;
    - gli obblighi di responsabilità dei responsabili;
    - i rischi e le misure correlate adottate:
        - Controllo degli accessi
        - Modalità di archiviazione
        - Sicurezza degli archivi cartacei
        - Minimizzazione dei dati
        - Gestione delle postazioni informatiche
        - Lotta ai "malware"
        - Modalità di Backup
        - Attività di manutenzione

- Gestione delle politiche sulla privacy
- Gestione dei rischi
- Gestione del personale
- Vigilanza sulla protezione dei dati
- Sicurezza dell'hardware
- Sicurezza del sito web

- è stata definita la gravità e la probabilità del rischio;
- è stata effettuata una mappatura del rischio;
- sono state definite le azioni di adeguamento/miglioramento necessarie sia infrastrutturali che organizzative (Piano d'azione).

4 – Gestione delle comunicazioni esterne

Fermo restando che le regole per una comunicazione efficace a mezzo e-mail restano le medesime valide per gli scambi interni all'azienda *(3 – Identificazione, rintracciabilità e trattamento delle comunicazioni* interne/esterne*)*, per quanto concerne le comunicazioni verso l'esterno e dall'esterno verso l'azienda è necessario porre l'attenzione su alcuni punti fondamentali.

4.1 Informazione delle parti interessate esterne

Tutte le parti esterne all'azienda individuate a seguito dell'analisi di contesto esterno devono:

- **essere informate** in merito a CHI in azienda è stato individuato come loro interlocutore di riferimento; un'operazione di trasparenza da parte dell'azienda è l'adozione di un'azione di comunicazione mirata iniziale (es. I Clienti devono essere informati di quale dei Resp.li di settore è il loro interlocutore per tutto quello che concerne i servizi richiesti, gli obblighi contrattuali delle parti, le modalità di gestione dei reclami, dalle modalità di richiesta di nuove offerte, degli eventuali aggiornamenti prezzi.

  Per questi motivi Tecnocontrolli rende disponibile in consultazione sul proprio sito web, ad esempio, la seguente documentazione[2]:

  - Reg-2 u.r. Gestione_Comunicazioni&Privacy
  - Reg3b All1 u.r. Condizioni generali di contratto
  - Reg3b All 1 u.r. Tariffario Elenco prove e verifiche per certificazione S 1_1+_2+ - FPC_CLS_PI
  - RCFPCCPR u.r. Registro Aziende Certificate FPC-CPR

  Sul sito web è inoltre disponibile, scaricabile, tutta la modulistica per la raccolta dati dei richiedenti e le richieste di prove/certificazione, ad esempio:

  - RDAT u.r. Raccolta Dati CPR-CLS
  - RC CPR CLS u.r. Richiesta Certificazione S 1+_1_2+_ITT_CLS
- **essere gestite** nel tempo in base alle eventuali variazioni sia dei referenti interni aziendali che degli interlocutori esterni delle parti interessate.

4.2 Comunicazioni con le parti interessate esterne

Le comunicazioni/istanze provenienti da parti esterne all'azienda devono pervenire al diretto responsabile di riferimento[3] e quest'ultimo dovrà gestirle, tramite e-mail o attività di Outlook, interessando, eventualmente, altri referenti interni necessari per una corretta gestione/risoluzione e conseguente feedback alla/e parte/i interessata/e .

[2] *Elenco non esaustivo*

[3] *nel caso pervengano a mezzo e-mail direttamente agli indirizzi generici info@tecnocontrolli.it o odc@tecnocntrolli.it il ricevente dovrà in tempo reale inoltrarle a referenti interessato*

Il referente interno dovrà gestire le istanze provenienti dallo specifico interlocutore esterno a seconda del contenuto della comunicazione. Le Istanze possono essere:

- istanze di routine, quali ad esempio contratti/offerte a seguito di richiesta prove/certificazioni, richieste di variazione servizi, ecc.
- istanze eccezionali, quali, a titolo esemplificativo e non esaustivo, segnalazioni, reclami ricorsi, esiti non conformi delle attività di prova e/o delle verifiche di certificazione ecc.

Il referente interno dovrà gestire inoltre le comunicazioni del CAB verso gli Enti Esterni - es. obblighi di comunicazione del CAB previsti dall'art. 53 del Regolamento (UE) n. 305/2011 e dal p.to 5.4 dell'Allegato D del D. lgs. n. 106/2017[4] (ved. Par. 4.2.1 "Obblighi di comunicazione")

NB

Devono essere effettuate esclusivamente tramite PEC:

- le comunicazioni/decisioni del CAB in merito a ricorsi pervenuti tutte le comunicazioni con il ricorrente;
- gli invii della documentazione di valutazione della conformità inclusi i Certificati emessi.

Tutte le comunicazioni provenienti da soggetti esterni all'azienda devono essere chiuse con una risposta (feedback) anche se non espressamente richiesto dal mittente, questo al fine di assicurare che non rimangano

Le Comunicazioni verso le parti interessate esterne devono essere gestite sempre dal referente indicato a suo tempo al singolo interlocutore in modo che non si verifichino sovrapposizioni e/o incongruenze tra le comunicazioni verso quel determinato interlocutore e/o che si possa perdere traccia dello scambio di comunicazioni avvenuto.

Quanto sopra vale a tutti i livelli aziendali ed in particolare:

- una volta indicato ad un interlocutore esterno il suo referente, questo non deve essere bypassato da altri interlocutori (anche nel caso di superiori);
- se per qualsiasi ragione si dovesse sostituire un referente interno o si venisse contattati dall'esterno anche per questioni di propria competenza (es. questioni contabili o commerciali) ma assegnate formalmente ad altro referente interno, il ricevente o il sostituto dovrà interessare sempre il diretto responsabile e trasferire a questo l'onere di gestire le comunicazioni con l'interlocutore esterno;
- alcune eccezioni fisiologiche legate ad esempio alla gestione dei "clienti direzionali" che sono soggetti ad una gestione condivisa tra il l'Amministratore Unico e i Direttori Tecnici dei vari settori operativi, devono comunque prevedere sempre l'interessamento di tutte le parti interne interessate e una definizione dei livelli di interlocuzione con i Referenti dei clienti.

4.2.1 Obblighi di comunicazione CAB-NB

Nel caso specifico (ved. Nota 4 pié di pagina) è stata predisposta specifica mailing list per la trasmissione delle comunicazioni previste dalle disposizioni di legge cogenti (Reg. 2 All. 1 u.r. mailing list CAB-NB) oltre a mantenere costantemente aggiornato il registro delle aziende certificate disponibile in consultazione sul sito web del CAB-NB (RCFPCCPR u.r. Registro Aziende Certificate FPC-CPR)

[4] *Regolamento (UE) n. 305/2011 art. 53 "Obbligo d'informazione per gli organismi notificati " (…) comma 2. Gli organismi notificati forniscono agli altri organismi notificati ai sensi del presente regolamento che svolgono analoghi compiti di parte terza secondo i sistemi di valutazione e verifica della costanza della prestazione e per prodotti da costruzione che rientrano nell'ambito di applicazione della stessa specifica tecnica armonizzata, informazioni pertinenti sulle questioni connesse ai risultati negativi e, su richiesta, di risultati positivi emersi da tali valutazioni e/o verifiche.*
D. lgs. n. 106/2017 All.D (…) 5.4 La sospensione, il ritiro o la limitazione di un certificato o di un rapporto, adottati nel rispetto dell'Articolo 52 del Regolamento, è motivata. Detti provvedimenti sono comunicati immediatamente agli interessati e alle Amministrazioni competenti ed all'Autorità notificante in adempimento a quanto previsto dall'art 53 del Regolamento.