



## PROVINCIA AUTONOMA DI TRENTO

Reg. delib. n. 174

Prot. n.

### VERBALE DI DELIBERAZIONE DELLA GIUNTA PROVINCIALE

#### OGGETTO:

Adozione del Regolamento di attuazione dell'articolo 4, comma 4 bis, della legge provinciale 31 maggio 2012, n. 10 concernente il trattamento dei dati personali nell'ambito del registro unico dei controlli provinciali (RUCP).

Il giorno **12 Febbraio 2021** ad ore **10:09** nella sala delle Sedute  
in seguito a convocazione disposta con avviso agli assessori, si è riunita

#### LA GIUNTA PROVINCIALE

sotto la presidenza del

PRESIDENTE

**MAURIZIO FUGATTI**

Presenti:

VICEPRESIDENTE  
ASSESSORE

**MARIO TONINA**  
**MIRKO BISESTI**  
**ROBERTO FAILONI**  
**MATTIA GOTTARDI**  
**STEFANIA SEGNANA**  
**ACHILLE SPINELLI**  
**GIULIA ZANOTELLI**

Assiste:

IL DIRIGENTE

**LUCA COMPER**

Il Presidente, constatato il numero legale degli intervenuti, dichiara aperta la seduta

Nell'ambito del Piano di razionalizzazione dei controlli sulle imprese di cui all'articolo 4, comma 4 bis, della legge provinciale n. 10 del 2012 è stato istituito il Registro unico dei controlli provinciali (RUCP), sistema informatizzato unitario per i controlli effettuati dalla Provincia, dai suoi enti strumentali e dall'Azienda provinciale per i servizi sanitari, che può essere esteso ai controlli sulle imprese effettuati dal sistema delle autonomie locali.

I controlli pubblici alle imprese sono rappresentati da ispezioni e verifiche documentali, con l'esercizio di eventuali poteri di sanzione, revoca di finanziamenti o provvedimenti in autotutela. Il RUCP può costituire uno strumento strategico per la semplificazione, come dimostrano le migliori best practices internazionali in materia, in particolare nello svolgimento delle azioni di:

- a) programmazione temporale dei piani ispettivi e di controllo;
- b) gestione del fascicolo di controllo e predisposizione di check list;
- c) produzione di un verbale di attività ispettiva o di controllo;
- d) formazione del profilo di rischio dell'impresa;
- e) selezione del campione di imprese da controllare;
- f) utilizzo di elementi e informazioni derivanti dal controllo già effettuato da altra struttura.

Ai sensi dell'articolo 4, comma 4 ter, legge provinciale n. 10 del 2012 nel RUCP sono destinati a confluire anche i risultati dei controlli che saranno effettuati dal Nucleo preposto al controllo delle dichiarazioni sostitutive di certificazione e di atto di notorietà rese dalle imprese (articoli 46 e 47, decreto del presidente della repubblica 28 dicembre 2000 n. 445, testo unico in materia di documentazione amministrativa), subordinatamente all'avvenuta attivazione dello stesso.

Scopo essenziale del RUCP è pertanto quello di razionalizzare a livello complessivo l'attività pubblica di controllo sulle imprese, grazie ad uno strumento di coordinamento e di condivisione delle informazioni, che permetta di ridurre le sovrapposizioni e ridondanze, mediante procedure di controllo più efficaci, efficienti e ponderate in base al rischio inerente alle attività controllate, ferma restando l'adeguatezza della protezione degli interessi pubblici cui la funzione pubblica di controllo è preposta.

A seguito dell'entrata in vigore del GDPR 2016/679 (Regolamento generale sulla protezione dei dati), per permettere il pieno utilizzo di tale strumento si è resa necessaria la predisposizione di un regolamento che disciplini il trattamento dei dati all'interno del RUCP.

Dopo una prima fase di confronto interno, che ha vista coinvolta in particolare l'UMSE per la protezione dei dati personali, con nota prot. n. 34961 del 20 gennaio 2020 la bozza di regolamento proposto è stata inviata al Garante per la protezione dei dati personali ai fini dell'acquisizione del prescritto parere ai sensi dell'articolo 36 paragrafo 4, del regolamento UE 2016/679. Il parere del Garante è stato rilasciato in data 5 marzo 2020 (parere n. 63).

I rilievi principali avanzati in tale parere riguardavano l'individuazione più precisa delle tipologie di dati personali trattati, nel rispetto del principio di minimizzazione, i requisiti per il trattamento dei dati concernenti condanne penali e reati, le garanzie da prevedere nel caso di trattamento automatizzato dei dati, la precisa individuazione dei ruoli di titolare e responsabile del trattamento.

A seguito della ricezione del parere si è provveduto quindi ad adeguare il testo alle osservazioni presentate dal Garante oltre che alla nota di commento allo stesso formulata dall'UMSE per la protezione dei dati personali. Inoltre si è provveduto a dare copertura con legge al trattamento dei dati concernenti condanne penali e reati mediante le disposizioni introdotte con l'articolo 19 della l.p. 3/2020. Questa possibilità andrà eventualmente dettagliata in futuro tramite apposita integrazione al regolamento allegato, ovvero con ulteriore atto regolamentare, quando sarà chiara, in funzione

dell'attivazione compiuta dello strumento di condivisione dei dati realizzato tramite il RUCP, la tipologia di dati giudiziari trattati ed il loro ruolo.

Per le misure tecnico-informatiche attinenti la protezione dei dati e la regolazione degli accessi al RUCP si è infine consultata la società di sistema Trentino digitale SpA, che ha provveduto a convalidare il regolamento per le parti di competenza.

Il testo è stato quindi condiviso per le vie brevi con il servizio legislativo che ha fornito le proprie osservazioni e contribuito alla stesura definitiva del regolamento. In data 22 ottobre 2020 con nota prot. n. 649679 è stato richiesto al Servizio legislativo il parere di merito sulla proposta di regolamento, ricevuto con nota prot. n. 798390 di data 11 dicembre 2020.

Sono state infine sostanzialmente recepite le ulteriori osservazioni formulate dall'UMSE per la protezione dai dati personali con nota prot. n. 824806 del 21 dicembre 2020.

Considerato che il RUCP potrà in prospettiva essere utilizzato anche dalle amministrazioni comunali in una logica di sistema territoriale, il presente regolamento - del quale si propone l'approvazione quale parte integrante e sostanziale della presente deliberazione - è stato sottoposto al Consiglio delle autonomie locali, che si è espresso in data 27 gennaio 2021, con esito comunicato con nota 65323 di data 1 febbraio 2021 dando parere positivo.

Ciò premesso,

#### LA GIUNTA PROVINCIALE

- udita la relazione;
- vista la legge provinciale n. 10 del 2012;
- visto il GDPR 2016/679 (Regolamento generale sulla protezione dei dati);
- viste le disposizioni di legge richiamate nella relazione;
- visti i pareri citati in premessa;
- visto il parere del Consiglio delle Autonomie locali di cui alla nota 65323 di data 1 febbraio 2021;
- a voti unanimi, espressi nelle forme di legge,

#### d e l i b e r a

- 1) di approvare, per i motivi esposti in premessa, il “Regolamento di attuazione dell'articolo 4, comma 4 bis, della legge provinciale 31 maggio 2012, n. 10 concernente il trattamento dei dati personali nell'ambito del registro unico dei controlli provinciali (RUCP)”, nel testo allegato che costituisce parte integrante e sostanziale della presente deliberazione;
- 2) di incaricare il Presidente della Provincia di emanare, con suo Decreto, le disposizioni regolamentari di cui al precedente punto 1);
- 3) di disporre la pubblicazione del presente provvedimento sul sito internet istituzionale della Provincia autonoma di Trento.

Adunanza chiusa ad ore 14:00

Verbale letto, approvato e sottoscritto.

**Elenco degli allegati parte integrante**

001 Regolamento

IL PRESIDENTE  
Maurizio Fugatti

IL DIRIGENTE  
Luca Comper

## **REGOLAMENTO**

### **concernente**

***“Regolamento di attuazione dell’articolo 4, comma 4 bis, della legge provinciale 31 maggio 2012, n. 10 concernente il trattamento dei dati personali nell’ambito del registro unico dei controlli provinciali (RUCP)”***

### **Art. 1**

#### ***Registro unico dei controlli provinciali (RUCP)***

1. Il registro unico dei controlli provinciali (RUCP), istituito dall’articolo 4, comma 4 bis, della legge provinciale n. 10 del 2012, è un sistema informatizzato unitario dei controlli effettuati dalla Provincia e dai suoi enti strumentali, dall’Azienda provinciale per i servizi sanitari, dalle Comunità e dai Comuni sulle imprese che operano sul territorio provinciale. Il RUCP opera nell’ambito del sistema informativo elettronico trentino (SINET) e partecipa ai sistemi informativi nazionali ed europei, per le sezioni e nelle banche dati corrispondenti.
2. Nel RUCP affluiscono i dati contenuti nelle banche dati elencate nell’allegato A del presente regolamento.
3. Ai sensi dell’articolo 4, comma 4 ter, della legge provinciale n. 10 del 2012, confluiscono nel RUCP i risultati dei controlli effettuati dal nucleo preposto al controllo delle dichiarazioni sostitutive di certificazione e di atto di notorietà rese dalle imprese ai sensi degli articoli 46 e 47 del decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 (*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*), a seguito dell’attivazione a regime dello stesso.

### **Art. 2**

#### ***Finalità del trattamento***

1. Il RUCP è un sistema volto a razionalizzare l’attività di controllo sulle imprese mediante l’adeguata considerazione del rischio inerente alle attività controllate, al fine di garantire una migliore e più efficace protezione degli interessi pubblici tutelati mediante l’esercizio delle funzioni amministrative di vigilanza.
2. La Provincia e i suoi enti strumentali, l’Azienda provinciale per i servizi sanitari, le Comunità e i Comuni utilizzano i dati e le informazioni contenuti nel RUCP nell’esercizio delle spettanti attività di vigilanza, che includono ispezioni, verifiche, monitoraggi, e altri controlli, nonché l’esercizio di eventuali poteri di sanzione o autotutela; per tali finalità possono avvalersi del RUCP nello svolgimento, in particolare, delle seguenti azioni:

- a) programmazione temporale dei piani ispettivi e di controllo, tramite un calendario dei controlli;
- b) gestione del fascicolo di controllo, con la predisposizione di check list;
- c) produzione di un verbale di attività ispettiva o di controllo contenente, tra l'altro, l'esito del controllo effettuato sull'impresa;
- d) formazione del profilo di rischio dell'impresa anche attraverso indici automatizzati e algoritmi, per orientare l'individuazione di quantità e modalità dei controlli;
- e) selezione del campione di imprese da controllare;
- f) raccolta dei dati in forma anonima per finalità statistiche.

### **Art. 3**

#### ***Tipologie di dati personali nell'ambito del RUCP***

1. Nel RUCP sono contenute e trattate informazioni emergenti dall'attività di vigilanza nelle materie in cui la Provincia e gli altri soggetti previsti dall'articolo 4, comma 4 bis, della legge provinciale n. 10 del 2012 hanno competenza a svolgere controlli, quali:

- a) ambiente;
- b) regolarità e sicurezza sul lavoro;
- c) attività forestali e agricoltura;
- d) sanità e sicurezza alimentare;
- d) commercio; titoli, diritti ed attività economiche;
- e) contratti pubblici di lavori, servizi e forniture.

2. Nell'ambito del RUCP sono trattati i soli dati personali necessari al perseguimento delle finalità di legge elencati nell'allegato B) del regolamento, adeguati, pertinenti e limitati rispetto alle finalità di cui all'articolo 4, comma 4-bis della legge provinciale n. 10 del 2012 e dell'articolo 2. Tra questi possono essere trattati, in particolare, dati personali dei piccoli imprenditori e delle imprese individuali derivanti dalla seguente documentazione:

- a) documentazione acquisita ex ante, quale la notifica preliminare, o nel corso dell'ispezione;
- b) estremi dei verbali o riproduzione elettronica dei verbali;
- c) esiti del controllo.

Con riferimento alle osservazioni “a verbale” e alle dichiarazioni spontanee, confluiscono nel RUCP esclusivamente i dati personali necessari alle finalità del registro, selezionati dalla struttura procedente con esclusione di ogni automatismo.

3. Qualora venissero trattati nel RUCP dati giudiziari, con specifici regolamenti saranno individuati i motivi di rilevante interesse pubblico, le tipologie di dati, le operazioni effettuate, nonché le misure di sicurezza appropriate e specifiche ai sensi degli articoli 10 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR) e 2-octies del decreto legislativo 30 giugno 2003, n.196 (*Codice in materia di protezione dei dati personali*).

#### **Art. 4**

##### ***Modalità di trattamento dei dati personali***

1. Il trattamento è effettuato dal personale autorizzato con modalità informatiche e cartacee idonee a garantire la riservatezza, l'integrità e la disponibilità dei dati.

2. I dati personali e le informazioni sulle persone fisiche contenuti nel RUCP sono acquisiti e trattati nel rispetto dei principi di pertinenza e non eccedenza dei dati utilizzati in relazione alle finalità perseguite, in conformità all'articolo 5 del GDPR.

3. Se per le finalità di cui all'articolo 2, comma 2 è effettuato il trattamento automatizzato dei dati, tale trattamento avverrà nel rispetto delle garanzie previste dall'articolo 22 del GDPR, senza la produzione di decisioni basate unicamente su algoritmi, o automatismi che possano produrre effetti giuridici o che incidano in modo analogo significativamente sulla persona.

#### **Art. 5**

##### ***Responsabile e titolare del trattamento dei dati personali***

1. Il gestore del RUCP è il Responsabile del trattamento dei dati personali nell'ambito del sistema, come stabilito dall'articolo 28 del GDPR.

2. Ai sensi dell'articolo 4, comma 4 bis, della legge provinciale n.10 del 2012 resta ferma la titolarità dei trattamenti in capo alla Provincia e ai singoli enti che si avvalgono del RUCP.

#### **Art. 6**

##### ***Gestore del RUCP***

1. Il gestore informatico dei documenti, dei flussi documentali e degli archivi per conto della Provincia, è la società che gestisce il sistema informativo elettronico

(SINET) provinciale ai sensi della legge provinciale, 6 maggio 1980, n. 10 (*Istituzione di un sistema informativo elettronico provinciale*). Essa, in particolare:

- a) attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
- b) cura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- c) segnala comportamenti che paiono non conformi alle disposizioni del presente regolamento, o casi di condotta che potrebbero essere qualificati come abusi, alla struttura provinciale competente per la gestione del RUCP;
- d) tiene aggiornato e conserva il registro delle operazioni di raccolta, modifica, consultazione, interconnessione e cancellazione di dati, eseguite nei sistemi di trattamento automatizzati dei dati (log);
- e) garantisce l'adozione e l'aggiornamento di specifiche misure di sicurezza tecnico-informatiche nel caso di trattamenti di dati personali contenenti dati giudiziari;
- f) garantisce la predisposizione del piano per i casi previsti di disaster recovery secondo quanto previsto dalla disciplina statale in materia;
- g) segnala alla struttura provinciale competente per la gestione del RUCP la necessità di aggiornamento o integrazione dell'elenco di banche dati di cui all'allegato A.

## **Art. 7**

### ***Conservazione dei dati***

1. Nel rispetto della normativa sul trattamento dei dati personali, i dati vengono conservati sia su supporto cartaceo che su altro supporto all'interno del territorio dell'Unione europea. Per i termini di conservazione dei dati si fa riferimento ai massimari di scarto d'archivio e/o ad eventuali atti organizzativi che definiscano il termine di cancellazione.

2. Il Responsabile della conservazione dei dati e delle informazioni presenti nel RUCP è la struttura provinciale competente per la conservazione documentale dei dati di archivio della Provincia.

## **Art. 8**

### ***Modalità di accesso al RUCP***

1. Possono accedere alle informazioni contenute nel RUCP solo gli utenti preventivamente identificati e autorizzati dal gestore del sistema.
2. L'accesso al RUCP può essere consentito in via ordinaria, per le normali attività di controllo ed ispettive e straordinaria, per interventi tecnici di backup, conservazione, download o upload di dati inerenti il RUCP.
3. L'accesso è effettuato tramite user-id e password fornite ad utenti identificati. Sono previste inoltre tutte le altre misure di sicurezza ivi collegate, quali la scadenza delle password e la disabilitazione in caso di dimissioni.
4. L'autenticazione per l'identificazione avviene previa assegnazione, da parte della società che gestisce il sistema informativo elettronico provinciale di credenziali di accesso individuali a seguito di richiesta scritta dei nominativi da abilitare.
5. All'impresa controllata può essere consentito l'accesso al RUCP, mediante autenticazione, limitatamente ai dati che la riguardano, durante tutte le fasi del procedimento, tranne quelle sottoposte a attività istruttoria o segreto statistico.
6. Per garantire l'accesso selettivo degli utenti è prevista l'associazione esplicita dell'utente ad una struttura organizzativa e ad un procedimento, in modo da consentire la visibilità delle informazioni in base al profilo assegnato all'utente. Tale associazione consente quindi una visibilità completa, correlata ad un sottoinsieme di procedimenti di controllo.
7. Gli enti abilitati al sistema possono consultare gli esiti dei controlli effettuati sulle imprese per quanto necessario allo svolgimento delle proprie competenze istituzionali. Gli addetti al trattamento possono effettuare ricerche sui controlli relativi alle imprese per quanto necessario allo svolgimento dei procedimenti loro affidati.

## **Art. 9** **Misure di sicurezza**

1. Il Responsabile del trattamento mette in pratica tutte le misure di sicurezza tecniche e organizzative ritenute necessarie a garantire l'integrità, la conservazione e la sicurezza dei dati raccolti, nonché la minimizzazione dei dati personali, in conformità alla normativa sulla protezione dei dati personali.
2. In particolare, il trattamento dei dati personali avviene per impostazione predefinita del sistema in relazione ai soli trattamenti individuati per legge o regolamento, tenuto conto dell'ambito di applicazione, del contesto e delle finalità del trattamento dei dati personali, nonché dei rischi, attuali o potenziali, anche di tipo informatico, gravanti sugli interessati. Ai fini della verifica della correttezza e legittimità del trattamento dei dati, sono registrati, in appositi file di log, le seguenti informazioni: il soggetto (codice

identificativo) che ha effettuato l'accesso, la data e l'ora dell'accesso, l'operazione effettuata, l'indirizzo IP della postazione di lavoro e del server interconnesso, i dati trattati. I log devono essere integri e non alterabili, sono protetti, con idonee misure, contro ogni uso improprio, vengono conservati per almeno 24 mesi e sono resi accessibili solo ad addetti espressamente autorizzati. Restando escluso l'utilizzo per la verifica della liceità dei trattamenti, in singoli casi, i dati contenuti nei file di log possono essere trattati solo in forma anonima. Allo specifico fine di assicurare la riservatezza, integrità e disponibilità dei dati, sono utilizzati sistemi di audit log per la verifica periodica degli accessi ai dati e per il rilevamento delle anomalie.

3. Le misure di sicurezza adottate riguardano:

a) la regolazione degli accessi al sistema;

b) la tenuta e conservazione del registro delle attività e valutazione di impatto sulla protezione dei dati;

c) il sistema di abilitazioni informatiche;

d) altre misure di sicurezza informatica (quali utilizzo di firewall, antivirus, copie di back up, protocollo https, log di sistema) nonché l'analisi periodica del sistema e la verifica della vulnerabilità del sistema ad attacchi informatici;

e) procedure di recupero e ripristino dati in caso di disaster recovery.

4. Per la notifica di eventuali violazioni, Titolari e Responsabili del trattamento sono tenuti a conformarsi agli articoli 33 e 34 del GDPR e alle disposizioni attuative statali e provinciali.

5. L'applicazione utilizzata per il caricamento dei dati è di tipo web, non richiede l'installazione né prevede l'archiviazione di dati o informazioni sulle postazioni di lavoro. Il RUCP si avvale degli stessi servizi infrastrutturali di funzionamento già utilizzati per il Sistema informativo elettronico trentino (SINET).

6. In conformità alla normativa sulla tutela dei dati personali, i singoli titolari del trattamento curano la tenuta dei registri delle attività di trattamento, in cui sono precisati, tra l'altro, durata del trattamento, collocazione fisica dei dati trattati, e misure di sicurezza adottate. Il registro viene periodicamente aggiornato anche tramite valutazione dell'impatto del rischio sulle tipologie di trattamento di cui all'articolo 35, comma 1 e 4, del regolamento generale sulla protezione dei dati (UE/2016/679).

7. Per le tecnologie informatiche si applica quanto previsto dalla disciplina statale in materia ed in particolare dalle linee guida dell'Agenzia per l'Italia digitale (AGID) in tema di marcatura dei documenti normativi, caratterizzazione dei sistemi cloud per la pubblica amministrazione e di data center. Costituiscono altresì misure di sicurezza

straordinarie avverso il cosiddetto rischio informatico l'analisi periodica del sistema e la verifica della vulnerabilità del sistema ad attacchi informatici.

8. Si applica, in caso di disaster recovery, la disciplina statale in materia e in particolare le linee guida AGID sulla continuità dei dati. Laddove si renda necessario interrompere il flusso dati per esigenze organizzative, e di sicurezza o per adeguamento a modifiche legislative, le parti concorderanno tempestivamente modalità alternative di accesso ai dati.

#### **Art. 10**

#### ***Esercizio dei diritti in materia di tutela dei dati personali***

1. Le persone fisiche che ritengono violato un loro diritto a causa di trattamenti effettuati nell'ambito del RUCP, possono sempre contattare il Responsabile del trattamento o ricorrere al difensore civico digitale presso l'AGID per i problemi connessi alle tecnologie informatiche utilizzate nel RUCP o nelle altre banche dati o sistemi informativi o esercitare le altre azioni previste dal GDPR e dalla normativa statale in materia.

*Allegato A*

*BANCHE DATI CONSULTABILI DAL RUCP*

**CCIAA: ANAGRAFE DELLE IMPRESE – SISTEMA PARIX**

**BASI DATI RIGUARDANTI:**

- controlli in materia di Ambiente
- controlli sui Cantieri
- controlli per sicurezza sul lavoro e igiene

## *Allegato B*

### *DATI PERSONALI CHE POSSONO ESSERE CONTENUTI E TRATTATI NEL RUCP*

- 1) Ragione sociale/denominazione, sede legale ed altri dati identificativi della società/impresa
- 2) Dati anagrafici, codice fiscale e/o partita iva, ruolo nell'azienda o nel cantiere relativi alle seguenti figure:
  - a) proprietario
  - b) legale rappresentante
  - c) committente del cantiere
  - d) responsabile dei lavori
  - e) coordinatore per quanto riguarda la sicurezza
  - f) altre figure specifiche previste dalla normativa di riferimento, individuate in relazione agli specifici procedimenti di controllo implementati nel registro
- 3) dati personali che sono indicati nel verbale mediante la compilazione degli elementi minimi individuati nell'Allegato C
- 4) esiti del controllo (anche riferito alle figure di cui sopra)
  - i) conforme/non conforme
  - ii) specifica non conformità (con riferimento a norma)
  - iii) diffida (eventuale)
  - iv) prescrizione (eventuale)
  - v) sanzioni previste
  - vi) eventuali osservazioni a verbale. Le informazioni di carattere personale destinate a confluire nel registro in quanto annotate nei verbali possono emergere dalla richiesta, da parte di persone fisiche presenti, di far annotare qualche osservazione specifica o di merito o da note riguardanti persone fisiche.

*Allegato C*  
**ELEMENTI MINIMI DEL VERBALE DI ACCERTAMENTO**

*Ente esecutore del controllo:*  
[anno/numero] del Verbale di accertamento Prot. n.

*Ente delegante (se presente)*

*Funzionario verbalizzante:*

*Impresa controllata:*

*Sede:*

*Stabilimento:*

*Legale rappresentante:*

*Settore del controllo:*

*Base legale del controllo:*

*Tipologia di controllo:*

*Sono presenti i signori:*

*Vengono contestate le seguenti infrazioni:*

*L'impresa controllata*

- rilascia le seguenti dichiarazioni spontanee e osservazioni:*
- formula, in contraddittorio, le seguenti controdeduzioni/ riserve:*

*Si allegano al presente atto:*

Il presente verbale, redatto in almeno due copie, viene chiuso alle ore \_\_\_\_\_  
del giorno \_\_\_\_\_ e chiuso nella data e ore indicate e dalle parti:

- firmato:*
- non firmato per i seguenti motivi: irreperibilità; impedimento; rifiuto a firmare;*

PER I VERBALIZZANTI

PER L'IMPRESA CONTROLLATA