

Comune di _____

Prov. di _____

PRIVACY - 2018



Adeguamento al Regolamento Europeo 679/2016, verifica
Misure minime di sicurezza per le Pubbliche Amministrazioni
(Direttive AgID in circolare n. 2/2017)

Prima valutazione

del _____/2022

AVVERTENZA ALL'USO DEL MODELLO

*Il presente modello serve per attuare l'Audit nell'ente locale, ovvero per riscontrare lo "stato dell'arte" sul trattamento dei dati effettuato dall'ente locale. **Audit**, vuol dire letteralmente "intervista". Il modello *Check list*, ovvero questionario, **va restituito dal Titolare del trattamento al RPD. Leggere le istruzioni della pag. 5 della Check list.***

STRUTTURA ORGANIZZATIVA DEL PERSONALE

Dati dell'ente locale

Nome ente _____

Indirizzo sede _____

Cap _____

Città _____

Telefono _____

Codice Ipa _____

(indice pa se presente) _____

Indirizzo sito internet _____

Indirizzo e-mail _____

Indirizzo PEC _____

Dati del Sindaco

Nome _____

Cognome _____

Recapito telefonico _____

Indirizzo e-mail _____

Dati del Segretario / Segretario generale

Nome _____
Cognome _____
Recapito telefonico _____
Indirizzo e-mail _____

Dati del Direttore generale *(se presente)*

Nome _____
Cognome _____
Recapito telefonico _____
Indirizzo e-mail _____

Sedi distaccate del Comune *(se presenti)*

Sede 1

Uffici distaccati _____
Indirizzo _____
Cap _____
Città _____
Telefono _____

Sede 2

Uffici distaccati _____
Indirizzo _____
Cap _____
Città _____
Telefono _____

AREE/SETTORI IN CUI È SUDDIVISO L'ENTE

Area/Settore _____

Numerazione e denominazione

degli uffici _____

Nome Responsabile _____

Area/Settore _____

Numerazione e denominazione

degli uffici _____

Nome Responsabile _____

Area/Settore _____

Numerazione e denominazione

degli uffici _____

Nome Responsabile _____

AZIENDE ESTERNE CON CUI L'ENTE COLLABORA REGOLARMENTE
--

Ragione sociale _____

Indicare il motivo

della collaborazione _____

Dati personali relativi all'azienda raccolti dall'ente:

☐ SI – ☐ NO

(in caso affermativo indicare se siano anche) ☐ sensibili – ☐ giudiziari

Esistenza di informativa per azienda e/o consenso

☐ SI – ☐ NO

Partita IVA _____

Recapito telefonico _____

Indirizzo e-mail _____

Ragione sociale

Indicare il motivo

della collaborazione

Dati personali dell'azienda raccolti dall'ente:

☐ SI – ☐ NO

(in caso affermativo indicare se siano anche) ☐ sensibili – ☐ giudiziari

Esistenza di informativa per azienda e/o consenso

☐ SI – ☐ NO

Partita IVA

Recapito telefonico

Indirizzo e-mail

RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

(se già presente)

Persona fisica interna all'ente locale

Nome

Cognome

Recapito telefonico

Indirizzo e-mail

Eventuale contitolare (per enti associati) (se già presente)

Nome

Cognome

Recapito telefonico

Indirizzo e-mail

Esiste il regolamento per il trattamento dei dati sensibili e giudiziari

☐ SI – ☐ NO

(artt. 20-22 D.Lgs. n. 196/2003)?

AUDIT: STEP N. 1

Istruzioni per la check list dell'ente locale Titolare del trattamento

La presente check list serve per verificare lo “stato dell’arte”, del trattamento dei dati effettuato nell’ente locale.

Si tratta di riscontrare come viene effettuato il trattamento nei diversi uffici dell’ente locale e quali misure di sicurezza e di garanzie siano già presenti a tutela della riservatezza di ogni interessato.

La check list rappresenta l’audit iniziale dell’ente locale e servirà per rilevare le non conformità alla disciplina del Regolamento europeo coordinata con il D.Lgs. n. 196/2003, da sistemare.

Dovrà essere sempre conservata ai fini di eventuale ispezione e dovrà rappresentare il termine di paragone anche per le migliorie future individuate tramite successivi audit. Va infatti precisato che le misure correttive, così come le successive migliorie vanno pianificate e non sono di immediata realizzazione.

La check list, pensata appositamente per l’ente locale, si basa sulla sua struttura organizzativa, posto che il trattamento dei dati personali può essere presente in diversa misura in ogni settore/Area dell’ente.

Ne consegue che dovranno essere somministrati gli appositi questionari di settore ai responsabili di Area e restituiti al titolare del trattamento. Successivamente verrà stilato un unico questionario che il titolare del trattamento consegnerà al RPD (interno o esterno).

Nella modulistica proposta, pertanto, si mettono a disposizione il questionario completo definitivo in word ed i questionari da inviare ai responsabili interni all’ente di ogni settore in formato word e pdf (l’ente può scegliere quale formato inviare).

Si fa presente che il contenuto della check list è conforme:

- ai principi per audit certificabili quali uni27001 per essere sicuri in caso di verifiche ispettive;
- alle misure indicate dal Garante italiano nei vari pareri e previste nell’allegato B del Codice della Privacy, D.Lgs. n. 196/2003, ad oggi ancora vigente;
- alle indicazioni fornite nella circolare 18 aprile 2017, n. 2 dall’Agid, preposta all’emanazione di regole, standard e guide tecniche, nonché di vigilanza e controllo sul rispetto delle norme del C.A.D. e sulla sicurezza informatica. Tali misure di sicurezza a tutela della riservatezza individuate dall’Agid, come indicato nella circolare stessa, vanno applicate in tutte le pubbliche amministrazioni, enti locali inclusi.

Il contenuto della check list si articola:

- nei dati sulla struttura organizzativa dell’ente: articolazioni in settori/Aree e sedi distaccate dell’ente locale. Non è necessario allegare la pianta organica dell’ente locale; si consiglia però di mettere bene in evidenza le misure di protezione per gli accessi dall’esterno nei locali dell’ente locale;
- nella indicazione per ogni area del personale che è addetto al trattamento dei dati personali e delle modalità (cartacee o elettroniche) con cui esso avviene;
- nella indicazione delle misure già in essere nell’ente per garantire il rispetto dei diritti degli interessati (es. registri cartacei chiusi in armadietti, password, uso di pseudonimi ecc.);
- in una parte da compilare a cura del CED o dell’amministratore di sistema con cui viene effettuato l’inventario dei dispositivi informatici e delle misure adottate. In tale sezione sono elencate le

misure indicate dall'Agid (si ribadisce, conformi a quelle presenti nell'allegato B del D.Lgs. n. 196/2003) e viene verificato se esse siano già presenti nell'ente.

La compilazione del questionario servirà al RPD come base di partenza per riscontrare quali sono i trattamenti che l'ente effettua ed in che modalità, quali sono le fonti di rischio per gli interessati e riscontrare già eventuale presenza di non conformità che dovranno essere corrette a conclusione del processo di Gestione Privacy.

Relativamente alle misure dell'Agid sulla sicurezza informatica del trattamento dei dati personali, si fa presente che non tutte devono necessariamente essere adottate dall'ente locale e né devono essere adottate nello stesso momento; spetta al RPD valutarne la necessità e la tempistica di introduzione di quelle mancanti nell'ente.

Il primo audit serve per eliminare le non conformità dei trattamenti dei dati mentre le migliorie ed ulteriori misure correttive trascurabili possono essere riscontrate con audit successivi e pianificate e programmate da questi. Ricordiamo che l'ente locale deve procedere a verifiche di riesame ogni sei mesi o almeno una volta l'anno tramite il proprio RPD. A tali verifica si procede con nuovi audit.

SICUREZZA LOGISTICA

Sono state stipulate assicurazioni?

☐ SI – ☐ NO

(in caso affermativo indicare quali) _____

Da compilare per ogni sede dell'ente locale

Accesso all'edificio/edifici dell'ente

Sede 1

Il perimetro esterno è protetto da possibili intrusioni?

☐ SI – ☐ NO

(in caso affermativo riportare come – es. reti, ringhiere...) _____

Quanti accessi sono presenti? (riportare il numero) _____

Gli accessi dei dipendenti sono controllati?

☐ SI – ☐ NO

(in caso affermativo riportare come – es. citofono/badge/guardia...) _____

Gli accessi dei cittadini sono controllati?

☐ SI – ☐ NO

(in caso affermativo riportare come – es. citofono/ guardia...) _____

È presente un impianto di videosorveglianza?

☐ SI – ☐ NO

Chi può accedere dopo orario chiusura uffici al pubblico?

(indicare nome e cognome) _____

È presente un sistema di allarme?

☐ SI – ☐ NO

(in caso affermativo indicare di che tipo e se con collegamento citofonico) _____

AREE / SETTORI DELL'ENTE

Area/Settore _____

Responsabile

Nome _____

Cognome _____

Sono presenti impianti antincendio? ☐ SI – ☐ NO

(eventuali note) _____

Sono presenti rilevatori di fumo? ☐ SI – ☐ NO

(eventuali note) _____

Sono trattati dati personali? ☐ SI – ☐ NO

(in caso affermativo specificare)

Dati del personale dipendente ☐ SI – ☐ NO

Dati esterni (cittadini e fornitori) ☐ SI – ☐ NO

(in caso affermativo, quali: es. anagrafici, identificativi, sensibili, giudiziari, di minori ecc.) _____

Indicare se i dati sopra indicati sono comunicati all'esterno ☐ SI – ☐ NO

(in caso affermativo, indicare a chi) _____

I DATI PERSONALI sono trattati dall'ufficio per ☐ finalità perseguite ☐ adempimenti di legge

Ci sono dati del settore che sono pubblicati sul sito internet del Comune? ☐ SI – ☐ NO

(in caso affermativo, indicare quali dati; se noto e predeterminato indicare per quanti giorni ed in base a quale norma di legge) _____

Dati pubblicati _____

Norma di legge (es. D.Lgs. n. 33/2013) _____

Periodo di pubblicazione: ☐ non noto – ☐ noto

(se noto) per giorni _____ (es. albo pretorio 15 gg.)

Elenco personale che tratta i dati personali per il settore:

1) Nome _____

Cognome _____

Ruolo (dipendente - PO - funzionario) _____

Indirizzo E-mail _____

2) Nome _____

Cognome _____

Ruolo (dipendente - PO - funzionario) _____

Indirizzo E-mail _____

I dati sono trattati conservati:

☐ modalità cartacea – ☐ modalità elettronica – ☐ modalità cartacea ed elettronica

Per conservazione cartacea

Armadio-registro chiuso a chiave

(specificare come sono conservati) _____

Indicare il personale che accede a tali dati ☐ autorizzato – ☐ non autorizzato

(indicare come) _____

I cittadini hanno accesso a tali dati?

☐ SI – ☐ NO

(in caso affermativo, indicare come) _____

Dati sensibili e giudiziari se presenti sono conservati a parte?

☐ SI – ☐ NO

(in caso affermativo, indicare come) _____

Sono usati pseudonimi nei documenti?

☐ SI – ☐ NO

Per conservazione elettronica

Attribuzione agli incaricati di codici identificativi (*parola chiave*) composti da almeno otto caratteri, *oppure*, nel caso lo strumento elettronico non lo consenta, da un numero di caratteri pari al massimo consentito: ☐ SI – ☐ NO

–

è modificata la parola chiave da parte dell'incaricato al primo utilizzo: ☐ SI – ☐ NO

successivamente è modificata ogni _____

–disattivazione dei codici identificativi in caso di perdita della qualità degli stessi o di mancato utilizzo per un pe

- protezione degli elaboratori contro i rischi di intrusioni, mediante l'utilizzo di appositi programmi: ☐ SI – ☐ NO
- verifica dell'efficacia e dell'aggiornamento del software antivirus, con cadenza _____
- applicazione di tecniche di pseudonimizzazione ai dati personali trattati: ☐ SI – ☐ NO
- esistenza di sistemi di copiatura e conservazione di archivi elettronici, misure idonee a ripristinare tempestivamente

L'Ufficio/Area fa uso di informatica:

☐ SI – ☐ NO

ULTERIORI DOMANDE GENERALI NON PER SINGOLA AREA

Formazione del personale sul trattamento dei dati:

☐ SI – ☐ NO

Periodicità degli aggiornamenti sulla privacy _____

Circolari interne ed istruzioni agli incaricati periodiche:

☐ SI – ☐ NO

Delibere di Consiglio e Giunta hanno dati sensibili (es. nome di disabili)?

☐ SI – ☐ NO

Tali dati sono pubblicati sul sito internet dell'Ente? ☐ SI, ma non per esteso

☐ NO, non sono pubblicati

☐ Sono resi anonimi

Le richieste di accesso ai dati personali sono sempre acconsentite?

☐ SI – ☐ NO

(in caso negativo, indicare per quali motivi non sono consentite) _____

MISURE DI SICUREZZA INFORMATICHE

(da compilare a cura del C.E.D. o amministratore di sistema)

(Le presenti domande sono necessarie per essere conformi anche agli obblighi di sicurezza predisposti dall'Agid per le pubbliche amministrazioni e a cui bisognava adeguarsi entro il 31 dicembre 2017 - Circolare 18 aprile 2017, n. 2/2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni pubblicata in G.U. n. 103 del 5 maggio 2017). Non esistono sanzioni in caso di mancato adeguamento ma tali misure garantiscono la sicurezza del trattamento dei dati personali e quindi nel sistema privacy dell'ente e in fase di audit vanno considerate. Il RPD poi valuterà la necessità di adottare – e la rispettiva tempistica – quelle non presenti nell'ente locale.

Dati dell'Amministratore di Sistema

- ☐ Interno (dipendente dell'Ente locale)
- ☐ Esterno (collaboratore esterno pubblico o privato)

Persona fisica

Nome _____

Cognome _____

Recapito telefonico _____

Indirizzo mail _____

Azienda

Ragione sociale _____

Partita IVA _____

Recapito telefonico _____

Indirizzo mail _____

Inventario dei dispositivi informatici del settore

(prenderlo da altri documenti dell'ente locale, es. se esiste ancora un documento sulla sicurezza, oppure dall'inventario)

Da redigere per ogni Area dell'ente locale

AREA/SETTORE _____

(Se esiste già un inventario dei dispositivi informativi allegarlo oppure utilizzare lo schema proposto)

Dispositivo	Utilizzo in locale	Utilizzo in rete	Sistema Operativo	Modello	Antivirus	Firewall	ISP
Pc							
Tablet							

--	--	--	--	--	--	--	--

AREA/SETTORE _____

(Se esiste già un inventario dei dispositivi informativi allegarlo oppure utilizzare lo schema proposto)

Dispositivo	Utilizzo in locale	Utilizzo in rete	Sistema Operativo	Modello	Antivirus	Firewall	ISP
Pc							
Tablet							

AREA/SETTORE _____

(Se esiste già un inventario dei dispositivi informativi allegarlo oppure utilizzare lo schema proposto)

Dispositivo	Utilizzo in locale	Utilizzo in rete	Sistema Operativo	Modello	Antivirus	Firewall	ISP
Pc							
Tablet							

Inventario dei dispositivi

Esiste già l'inventario dei dispositivi informatici?

☐ SI – ☐ NO

(da fare – nel caso non esista)

L'inventario viene mantenuto aggiornato quando si collegano nuovi dispositivi in rete

(es. nuovo Pc)?

☐ SI – ☐ NO

Il processo di aggiornamento è automatico?

☐ SI – ☐ NO

È stato redatto un inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP?

☐ SI – ☐ NO

Inventario dei software

È stato stilato un elenco di software autorizzati e relative versioni, necessari per ciascun tipo di sistema? ☐ SI – ☐ NO

È vietato l'utilizzo di software non compresi nell'elenco? ☐ SI – ☐ NO

Viene eseguita una scansione regolare ai sistemi per rilevare presenza di software non autorizzati? ☐ SI – ☐ NO

Configurazioni protette

Vengono utilizzate configurazioni sicure standard per la protezione dei sistemi operativi? ☐ SI – ☐ NO

Viene definita e impiegata una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione? ☐ SI – ☐ NO

I sistemi compromessi sono stati ripristinati usando la configurazione standard? ☐ SI – ☐ NO

Le immagini di installazione sono memorizzate offline? ☐ SI – ☐ NO

Le operazioni remote sono eseguite tramite connessioni protette?
(*protocolli intrinsecamente sicuri o su canali sicuri*)? ☐ SI – ☐ NO

Ad ogni cambiamento significativo della configurazione viene fatta una scansione con strumenti automatici che generino report sulle vulnerabilità più critiche? ☐ SI – ☐ NO

Gli strumenti utilizzati per la scansione sono aggiornati? ☐ SI – ☐ NO

Sono presenti sistemi separati dalla rete? ☐ SI – ☐ NO

L'aggiornamento dei sistemi separati dalla rete (*es. air gapped*) viene eseguito tenendo conto delle specifiche criticità? ☐ SI – ☐ NO

Gestione privilegi di amministratore

I privilegi di amministrazione sono limitati ai soli utenti che ne hanno competenza o eventualmente hanno necessità di modificare la configurazione della rete? ☐ SI – ☐ NO

Viene registrato ogni accesso eseguito usando tali utenze? ☐ SI – ☐ NO

È stato stilato un inventario delle suddette utenze? ☐ SI – ☐ NO

Sono state redatte debite e ufficiali autorizzazioni all'utilizzo di queste utenze? ☐ SI – ☐ NO

Prima di collegare alla rete un nuovo dispositivo le credenziali predefinite sono state modificate coerentemente alle utenze amministrative in uso? ☐ SI – ☐ NO

Viene usata un'autenticazione a più fattori per le utenze amministrative?

(es. pin + tesserino, impronta + password...)

☐ SI – ☐ NO

In caso contrario la password contiene almeno 14 caratteri?

☐ SI – ☐ NO

Le credenziali delle utenze amministrative sono sostituite con sufficiente frequenza?

(6 o 3 mesi)

☐ SI – ☐ NO

Viene impedito che le stesse password vengano riutilizzate a distanza di tempo troppo breve?

☐ SI – ☐ NO

Le utenze con privilegi sono completamente distinte da quelle senza privilegi?

(diverse credenziali)

☐ SI – ☐ NO

Le utenze (tutte) sono nominative e associabili a una sola persona?

☐ SI – ☐ NO

Le credenziali permettono di risalire a chi ne fa uso?

☐ SI – ☐ NO

Le credenziali amministrative sono conservate in modo da garantirne la disponibilità? ☐ SI – ☐ NO

Le credenziali amministrative sono conservate in modo da garantirne la riservatezza? ☐ SI – ☐ NO

Per l'autenticazione vengono usati certificati digitali?

☐ SI – ☐ NO

Se sì, le chiavi private sono adeguatamente conservate?

☐ SI – ☐ NO

Difese contro malware

È stato installato l'antivirus su ogni sistema connesso alla rete locale?

☐ SI – ☐ NO

L'antivirus si aggiorna automaticamente?

☐ SI – ☐ NO

È stato installato un firewall su ogni dispositivo?

☐ SI – ☐ NO

È stato installato un Sistema di Prevenzione dalle Intrusioni su ogni dispositivo?

☐ SI – ☐ NO

L'uso di dispositivi esterni è limitato a situazioni in cui è necessario per l'ente locale? ☐ SI – ☐ NO

L'apertura automatica dei messaggi di posta elettronica è attiva?

☐ SI – ☐ NO

L'anteprima automatica dei contenuti dei file è attiva?

☐ SI – ☐ NO

Quando dei supporti removibili vengono connessi, vengono scansati contro eventuali malware?

☐ SI – ☐ NO

Il contenuto delle email è scansato prima che il messaggio venga ricevuto?

(antispam...)

☐ SI – ☐ NO

Il contenuto del traffico web è filtrato?

☐ SI – ☐ NO

Esiste un elenco delle tipologie di file il cui utilizzo è strettamente necessario?

☐ SI – ☐ NO

I file non appartenenti a questa categoria vengono bloccati durante la navigazione in rete?

☐ SI – ☐ NO

Backup

Viene effettuata settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il ripristino del sistema? ☐ SI – ☐ NO

I supporti fisici su cui sono salvate le copie sono conservati in luoghi protetti? ☐ SI – ☐ NO

I dati nelle copie sono cifrati? ☐ SI – ☐ NO

I dati vengono salvati usando un servizio di cloud computing? ☐ SI – ☐ NO

Se sì, i dati sono cifrati prima della trasmissione su cloud? ☐ SI – ☐ NO

I supporti fisici delle copie sono permanentemente collegati ai dispositivi e/o alla rete?
(o accessibili da essi?) ☐ SI – ☐ NO

Protezione dati

Sono stati associati dei requisiti di riservatezza alle categorie identificate?
(distinguere eventualmente per uffici) _____ ☐ SI – ☐ NO

Sono state applicate particolari misure di protezione ai dati più rilevanti?
(distinguere eventualmente per uffici) _____ ☐ SI – ☐ NO

I dati rilevanti sono protetti con crittografia?
(distinguere eventualmente per uffici) _____ ☐ SI – ☐ NO

VIDEOSORVEGLIANZA E CONTROLLO A DISTANZA

Inventario delle videocamere

(Includere anche eventuali monitor o registratori. Se già disponibile allegarlo oppure utilizzare lo schema proposto)

ID DEVICE (ai fini del SIGP)	Fissa/rotante	Lunghezza focale	Profondità di campo	Zoom	Raggio d'azione	Angolo di campo	Angolo regolabile

Almeno una telecamera rischia di inquadrare il personale durante il lavoro? ☐ SI – ☐ NO

Le videocamere registrano immagini? ☐ SI – ☐ NO

È stato nominato un responsabile? ☐ SI – ☐ NO

(in caso affermativo) ☐ interno – ☐ esterno

È stata predisposta un'informativa minima con i riferimenti per risalire alla info completa? ☐ SI – ☐ NO

Sono stati predisposti i cartelli contenenti la suddetta informativa? ☐ SI – ☐ NO

L'accesso alle immagini dipende dal possesso di credenziali? ☐ SI – ☐ NO

Le credenziali necessarie sono in possesso di una singola persona? ☐ SI – ☐ NO

Le credenziali sono personali e univocamente legate a ogni singola persona? ☐ SI – ☐ NO

È possibile risalire agli accessi avvenuti alle immagini? ☐ SI – ☐ NO

Le immagini sono strettamente necessarie per lo scopo prefissato? ☐ SI – ☐ NO

Ci sono sistemi di videosorveglianza in prossimità di:

☐ Locali interni aperti al pubblico (indicare quali) _____

☐ Locali interni accessibili al solo personale (indicare quali) _____

☐ Per sicurezza urbana, nelle vie strategiche, vicino a scuole, parcheggi e giardini pubblici
(indicare quali) _____

Il sistema di videosorveglianza è dotato di sistemi intelligenti?

(riconoscimento facciale, riconoscimento biometrico, combinazione di dati...)

☐ SI – ☐ NO

In caso di registrazione, la cancellazione delle immagini avviene entro: *(distinguere sicurezza urbana da videosorveglianza dentro ente locale se presente)* ☐ 24h ☐ 48h ☐ 72h ☐ una settimana

I locali contenenti i monitor hanno accesso controllato?

☐ SI – ☐ NO

I supporti sono custoditi in armadi chiusi a chiave?

☐ SI – ☐ NO

Le immagini conservate sono state previamente cifrate?

☐ SI – ☐ NO

È stato rilasciato un attestato di conformità da un fornitore esterno?

☐ SI – ☐ NO

DATI STORICI PER UNA CORRETTA ANALISI DEI RISCHI

Ci sono stati furti o tentativi di furto negli ultimi anni?

☐ SI – ☐ NO

Si sono verificati accessi non autorizzati all'ente locale?

☐ SI – ☐ NO

Ci sono stati atti vandalici negli ultimi anni?

☐ SI – ☐ NO

Sono stati danneggiati archivi contenenti dati?

☐ SI – ☐ NO

Sono stati danneggiati impianti informatici?

☐ SI – ☐ NO

Ci sono stati danni a impianti complementari? *(dovuti a incendi, temporali ecc.)*

☐ SI – ☐ NO

Ci sono stati blackout improvvisi?

☐ SI – ☐ NO

Si sono registrati attacchi informatici di recente?

☐ SI – ☐ NO

Data _____

Firma del Titolare del trattamento dati
