CITTA' DI AIROLA
Provincia di Benevento

Documento di analisi e adeguamento della struttura organizzativa comunale al Regolamento UE e alla vigente normativa nazionale in materia di privacy (D.lgs n.196/2003 e D.lgs n.101/2018)

Allegato B) al Regolamento Comunale **per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali**

pietraroja@pec.cstsannio.it

SCOPO GDPR/RGPD

Il regolamento generale sulla protezione dei dati (in inglese General Data Protection Regulation), ufficialmente regolamento (UE) n. 2016/679 e meglio noto con la sigla GDPR/RGPD, è un regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy.

Con questo regolamento, la Commissione europea intende rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione europea e dei residenti nell'Unione europea, sia all'interno che all'esterno dei confini dell'Unione europea (UE).

Il testo, adottato il 27 aprile 2016, è stato pubblicato sulla Gazzetta Ufficiale Europea il 4 maggio 2016 ed è entrato in vigore il 25 maggio dello stesso anno.

Il testo obbliga tutti i titolari del trattamento dei dati (anche con sede legale fuori dall'Unione europea) che trattano dati di residenti nell'Unione europea ad osservare e adempiere agli obblighi previsti. Gli obiettivi principali della Commissione europea nel GDPR sono quelli di restituire ai cittadini il controllo dei propri dati personali e di semplificare il contesto normativo che riguarda gli affari internazionali unificando e rendendo omogenea la normativa privacy dentro l'UE. Dalla sua entrata in vigore, il RGPD ha sostituito i contenuti della direttiva sulla protezione dei dati (Direttiva 95/46/CE). L' Italia ha recepito i nuovi principi attraverso l'art. 13 della legge 163/2017, che ha attribuito al Governo la delega ad adottare, entro sei mesi, uno o più provvedimenti rivolti ad abrogare le norme del codice per la protezione dei dati personali (dlgs.n. 196/2003) con esso incompatibili e a modificarlo al fine di dare puntuale attuazione allo stesso RGPD; a tal fine è stato emanato e pubblicato il D.lgs n. 101/2018 recante Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679.

PRIORITA' PER LE PUBBLICHE AMMINISTRAZIONI

La principale novità introdotta dal regolamento è il principio di "responsabilizzazione" (cd. accountability), che attribuisce direttamente ai titolari del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali (art. 5). In quest'ottica, la nuova disciplina impone alle amministrazioni un diverso approccio nel trattamento dei dati personali, prevede nuovi adempimenti e richiede un'intensa attività di adeguamento a partire dal 25 maggio 2018.

Al fine di fornire un primo orientamento il Garante per la protezione dei dati personali ha suggerito alle Amministrazioni pubbliche di avviare, con assoluta priorità:

- la designazione del Responsabile della protezione dei dati;
- l'istituzione del Registro delle attività di trattamento;
- la notifica delle violazioni dei dati personali.

LA DESIGNAZIONE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)

Questa nuova figura, che il regolamento richiede sia individuata in funzione delle qualità professionali e della conoscenza specialistica della normativa e della prassi in materia di protezione dati, costituisce il fulcro del processo di attuazione del principio di "responsabilizzazione". Il diretto coinvolgimento del RPD/DPO in tutte le questioni che riguardano la protezione dei dati personali, sin dalla fase transitoria, è sicuramente garanzia di qualità del risultato del processo di adeguamento in atto. In questo ambito, sono da tenere in attenta considerazione i requisiti normativi relativamente a: posizione (riferisce direttamente al vertice), indipendenza (non riceve istruzioni per quanto riguarda l'esecuzione dei compiti) e autonomia (attribuzione di risorse umane e finanziarie adeguate).

1.1.1 L'ISTITUZIONE DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Essenziale è avviare quanto prima la ricognizione dei trattamenti svolti e delle loro principali caratteristiche (finalità del trattamento, descrizione delle categorie di dati e interessati, categorie di destinatari cui è prevista la comunicazione, misure di sicurezza, tempi di conservazione, e ogni altra informazione che il titolare ritenga opportuna al fine di documentare le attività di trattamento svolte) funzionale all'istituzione del registro. La ricognizione sarà l'occasione per verificare anche il rispetto dei principi fondamentali (art. 5), la liceità del trattamento (verifica dell'idoneità della base giuridica, artt. 6, 9 e 10) nonché l'opportunità dell'introduzione di misure a protezione dei dati fin dalla progettazione e per impostazione (privacy by design e by default, art. 25), in modo da assicurare, entro il 25 maggio 2018, la piena conformità dei trattamenti in corso (cons. 171).

PRIVACY BY DESIGN

Con l'espressione **"privacy by design"**, pertanto il Regolamento Europeo intende richiamare l'attenzione dei titolari sull'esigenza che la protezione dei dati personali venga garantita **"fin dalla progettazione"**. A questo proposito, l'art. 25, paragrafo 1 del Regolamento stabilisce che **il titolare del trattamento dei dati personali** deve **adottare delle misure tecniche e organizzative idonee** a dare concreta attuazione a quelle che sono le disposizioni e i principi in materia di protezione dei dati e garantire in questo modo i diritti degli interessati. Una delle particolarità di questa norma sta nel fatto che la predisposizione delle misure necessarie è prescritta sia nel momento in cui il titolare del trattamento deve determinare i mezzi del trattamento stesso, sia quando pone in essere le vere e proprie operazioni di trattamento. Va ricordato, ad ogni modo, che ciascun titolare, nell'attuare le misure previste, dovrà sempre tenere conto dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei diversi rischi aventi probabilità e gravità variabili per i diritti e le libertà delle persone fisiche. Questo significa, in concreto, che il titolare non sarà compliance se applicherà delle misure standard e predeterminate a diverse tipologie di trattamento, ma dovrà sempre procedere ad un'analisi realistica e specifica del singolo contesto di riferimento.

PRIVACY BY DEFAULT

Il secondo concetto introdotto dal GDPR, sempre all'art. 25, è invece quello di **"privacy by default".** Con questa espressione il legislatore europeo ha affermato la necessità che la protezione dei dati personali sia garantita **"per impostazione predefinita",** ossia la necessità della tutela della vita privata dei cittadini "di default" appunto. Questo implica che i dati personali che vengono raccolti in occasione di registrazioni a servizi telematici o della stipula di contratti, o in breve in ogni caso in cui ciascuno renda i propri dati ad un terzo, devono essere trattati sempre attraverso un percorso di politica amministrativa interna che ne tuteli la diffusione. Intanto, ne deriva che tutte le valutazioni che il titolare del trattamento deve effettuare in tema di protezione dei dati personali devono essere compiute a monte, cioè prima di procedere al trattamento dei dati vero e proprio. Il titolare deve svolgere un'analisi preventiva della situazione complessiva e adottare un approccio pratico che si dovrà, a sua volta, concretizzare in una serie di attività specifiche e dimostrabili. Le soluzioni a cui il titolare del trattamento potrà affidarsi potranno consistere, ad esempio, nella riduzione al minimo del trattamento dei dati personali, nella pseudonimizzazione dei dati personali, nella massima trasparenza sulle finalità e sulle modalità del trattamento di dati personali, nel consentire all'interessato di controllarne il trattamento rendendo facilmente ed effettivamente esercitabili i diritti previsti dal Regolamento. Inoltre, il titolare dovrà attenersi a questi criteri in tutte le fasi di trattamento: nella fase dello sviluppo, della progettazione, della raccolta, della selezione e dell'utilizzo di dati personali e sempre alla luce di un'attenta analisi del contesto specifico di riferimento. Infine, l'art. 25 del GDPR incoraggia l'adozione di appositi **meccanismi di certificazione** (nonché di sigilli o marchi specifici) della protezione dei dati personali, aventi la precisa funzione di consentire ai titolari e ai responsabili del trattamento dei dati di dimostrare la conformità dei trattamenti che sono stati posti in essere al Regolamento. Meccanismi di certificazione che, per il momento non sono ancora stati previsti né definiti in modo più concreto, ma che, qualora resi reali, potranno senz'altro costituire un importante punto di riferimento e uno strumento fondamentale per dimostrare la propria compliance.

1.1.2 LA NOTIFICA DELLE VIOLAZIONI DEI DATI PERSONALI (CD. DATA BREACH)

Fondamentale appare anche, nell'attuale contesto caratterizzato da una crescente minaccia alla sicurezza dei sistemi informativi, la pronta attuazione delle nuove misure relative alle violazioni dei dati personali, tenendo in particolare considerazione i criteri di attenuazione del rischio indicati dalla disciplina e individuando quanto prima idonee procedure organizzative per dare attuazione alle nuove disposizioni.

Il Comune di Airola, in qualità di Titolare del trattamento dei dati personali, rappresentato dal Sindaco pro tempore Rappresentante Legale, ha avviato l'adeguamento verso il nuovo regolamento, individuando innanzitutto, così come previsto dalla nuova normativa, un "**DPO** o **RPD – Responsabile per la Protezione dei Dati**" dell'Ente, che ha provveduto alla stesura del presente documento con il preciso scopo di segnalare tutte le misure necessarie per la messa in sicurezza dell'Ente nel rispetto della nuova normativa in vigore. Sono state, quindi, individuate diverse azioni necessarie al raggiungimento dell'obiettivo che hanno visto un intervento stratificato su diversi livelli ed in particolare:

- livello fisico
- livello logico
- livello organizzativo.

1.2 DOCUMENTO DI ANALISI E DI ADEGUAMENTO DELLA STRUTTURA COMUNALE AL RGPD

Il presente documento, redatto dal già nominato RPD - CST Sannio.it Ing. Carmine Basco, si pone l'obiettivo di rappresentare lo scenario in essere all'interno dell'Ente per quanto concerne il sistema di gestione privacy e pone la sua maggiore attenzione sulle misure correttive da adottare per l'adeguamento al nuovo regolamento europeo RGPD 679/2016; è un documento organico che parte dall'analisi dei rischi propri del sistema informativo, tenuto conto dei dati trattati dall'Ente, per mettere a fuoco una serie di contromisure di vario tipo necessarie per il raggiungimento di idonee misure di sicurezza anche in conformita'agli obiettivi strategici dell'Agenzia Digitale. Pertanto, sotto l'aspetto operativo, la strategia da adottare per il raggiungimento di tali misure comprenderà:

- un insieme di adempimenti che potranno essere attuati con costi limitati ma che innalzeranno significativamente il livello di sicurezza;
- l'adozione di alcuni criteri di sicurezza che individueranno uno o più metodi per definire e mettere in atto il sistema di sicurezza ottimale attraverso soluzioni in grado di sensibilizzare il personale dipendente ai quali sono indirizzati ed accrescere così la cultura della sicurezza all'interno dell'Ente.

Il presente Documento, redatto nella forma di manuale secondo la norma ISO 9000, viene aggiornato periodicamente a cura dello stesso RPD

Il Documento descrive e definisce:

- le responsabilità, nonché le istruzioni impartite ai soggetti preposti al trattamento (Responsabili e incaricati sub responsabili del trattamento);
- le azioni per la gestione dei rischi e per l'adozione delle misure di sicurezza, gli adempimenti necessari sia a rilevanza cosiddetta interna sia esterna.

Il Documento viene tenuto dal Titolare dei trattamenti che può decidere di affidarne la tenuta al RPD o al Segretario Generale, così come per il Registro Unico dei trattamenti, sotto la responsabilità del medesimo Titolare.

Esso è aggiornato costantemente dal DPO dell'Ente, che ne cura:

- la revisione annuale, formulando le proposte di modifica e di integrazione al Titolare;
- la corretta applicazione e conservazione del Documento;

Lo stato di revisione del documento è riportato in basso al centro, nella griglia di piè di pagina, contraddistinto da due numeri progressivi (Rev. 1.0): il primo numero verrà incrementato in caso di modifiche sostanziali al documento, mentre il secondo sarà incrementato in caso di modifiche di minore rilevanza. A fianco al numero di revisione viene sempre indicata la data di approvazione da parte del titolare del trattamento dati.

2 DEFINIZIONI ED ACRONIMI

Sigla	Descrizione
DA-GDPR	Documento di adeguamento al GDPR
CED	Centro Elaborazione Dati
DPO o RPD	Responsabile per la protezione dei dati personali
trattamento	qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
titolare del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

limitazione di trattamento	il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
dato personale	qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
profilazione	qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
pseudonimizzazione	il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
dati sensibili	i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale
dati giudiziari	i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale
dato anonimo	il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile
destinatario	la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.
Responsabile del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
incaricato del trattamento	colui che deve elaborare i dati personali ai quali ha accesso, attenendosi alle istruzioni, impartite per iscritto, del titolare o del responsabile, e che opera sotto la loro diretta responsabilità
interessato	la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali
terzo	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
consenso dell'interessato	qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
comunicazione	il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione
archivio	qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
diffusione	il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque

	forma, anche mediante la loro messa a disposizione o consultazione
sicurezza dei dati	Adeguate, idonee e preventive misure di sicurezza, definite e implementate dal Titolare, atte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
cessazione trattamento dati	il caso in cui i dati possono essere distrutti, salvo obblighi di conservazione, ceduti o conservati per fini esclusivamente personali
banca dati	qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati, tali da facilitarne il trattamento. La definizione comprende le banche dati sia su supporto cartaceo che su supporto informatico.
Garante	l'autorità istituita ai sensi della legge, avente le funzioni di garantire il rispetto della disciplina, promuoverne la conoscenza, assicurare la corretta interpretazione delle norme e svolgere attività di repressione degli illeciti commessi in violazione degli obblighi in materia di protezione dei dati. In particolare, in funzione di tutela dei diritti dell'interessato, la sua funzione si esplica attraverso interventi di carattere inibitorio, cautelare o sanzionatorio finalizzati alla risoluzione dei conflitti tra i soggetti che trattano i dati e gli interessati.
notificazione data breach	comunicazione al Garante, da parte del RPD di eventuali violazioni riscontrate sul trattamento dei dati personali
strumenti elettronici	gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento
autenticazione informatica	l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità
credenziali di autenticazione	i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
parola chiave	componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica
profilo di autorizzazione	l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti
blocco	la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento
amministratore di sistema	con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del Provvedimento del Garante del 27/11/2008 vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi
violazione dei dati personali	la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
dati genetici	i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
dati biometrici	i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
dati relativi alla salute	i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

rappresentante	la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
impresa	la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
gruppo imprenditoriale	un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
autorità di controllo	l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

3 ALLEGATI

Sigla	Descrizione
RUT	Registro Unico Trattamenti
RDB	Registro Data Breach
INF	Modello Informativa agli Interessati
NOMINE	Nomina DPO Nomina dei Responsabili del trattamento contenenti le nuove Clausole contrattuali Designazioni dei soggetti interni autorizzati al trattamento: Responsabili Area/Settore/Servizio e Incaricati di Area funzionale

4 SCENARIO NORMATIVO

4.1 DISPOSIZIONI GENERALI

L'entrata in vigore della nuova disciplina in materia di gestione del trattamento dei dati personali è stata ispirata dall'esigenza di introdurre una regolamentazione più rigida, rispetto al passato, quanto all'utilizzo dei dati personali, puntando su di una maggiore tutela, responsabilizzazione e consapevolezza delle grandi risorse che si celano dietro l'uso degli stessi.
Il GDPR, in realtà, non contiene una formale bipartizione tra titolari pubblici e privati e non contiene nemmeno norme specifiche dedicate al settore privato e pubblico, ma si occupa in generale delle condizioni di liceità del trattamento (v. art. 6 e art. 9, comma 2, per i dati sensibili), anche se poi, come vedremo tra breve, alcune di esse riguardano esclusivamente lo svolgimento di attività pubbliche.
Il nuovo Regolamento, quindi, non si sofferma sulla natura pubblica o privata del titolare del trattamento, ma sulla tipologia di trattamento, che scaturisce dall'attività svolta dal titolare.
A differenza del Codice Privacy (D.Lgs. n. 196/2003), il nuovo regolamento europeo non contiene la suddivisione tra condizioni di liceità applicabili a soggetti privati e condizioni valide per i soggetti pubblici, come accadeva con il Capo II del Codice Privacy, dove, ad eccezione del settore sanitario, si menzionava l'istituto del consenso quale elemento distintivo tra titolari privati e titolari pubblici.

In effetti, tra gli stessi presupposti di liceità del trattamento dei dati personali il GDPR all'art. 6, lett. e) fa riferimento alla necessarietà del trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, caso tipico, naturalmente dell'ente pubblico.

E' opportuno soffermarsi sull'art. 9 del GDPR che tra le eccezioni al divieto generale di trattare dati personali sensibili fa rientrare:

- il trattamento necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- il trattamento necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
- il trattamento necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;
- il trattamento necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale.
- il trattamento necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

L'art. 10 del GDPR, poi, con riferimento al trattamento dei dati giudiziari chiarisce che lo stesso deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Anche un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Altra norma di sicuro interesse per l'indubbia rilevanza in materia pubblicistica è rappresentata dall'art. 23 del GDPR che chiarisce come il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento possa limitare, mediante specifiche misure legislative, la portata di alcuni fondamentali obblighi e diritti degli interessati qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare tra gli altri: la sicurezza nazionale; la difesa; la sicurezza pubblica; la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione

o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale; la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari.

4.2 CAMPO DI APPLICAZIONE DEL NUOVO REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Il nuovo regolamento europeo GDPR 679/2016 si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi. Non si applica invece ai trattamenti di dati personali:

- effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
- effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;
- effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
- effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione, si applica il regolamento (CE) n. 45/2001. Il regolamento (CE) n. 45/2001 e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali devono essere pertanto adeguati ai principi e alle norme del presente regolamento conformemente all'articolo 98.

I trattamenti pertanto svolti in seno al Comune rientrano nell'ambito di questa ultima sfera.

Il nuovo regolamento non pregiudica pertanto l'applicazione della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva.
Il regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati, protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.
Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio.

4.2.1 VALUTAZIONE D´IMPATTO DELLA PROTEZIONE DEI DATI (DPIA)

Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l´autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.
Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo, perché esprime chiaramente la responsabilizzazione (accountability) dei titolari nei confronti dei trattamenti da questi effettuati. I titolari sono infatti tenuti non soltanto a garantire l´osservanza delle disposizioni del regolamento, ma anche a dimostrare adeguatamente in che modo garantiscono tale osservanza; la valutazione di impatto ne è un esempio.
Nell'ambito del Comune di Airola è necessario portare a conoscenza del Titolare del trattamento dei dati personali che la realizzazione di un eventuale nuovo impianto di videosorveglianza dislocato sul territorio dovrà prevedere da parte della ditta affidataria l'elaborazione di un documento concernente la valutazione d'impatto (DPIA) che assicuri la corretta progettazione e gestione dell'impianto nel pieno rispetto del fondamentale principio fissato nel regolamento 2016/679, ossia la protezione dei dati fin dalla fase di progettazione (data protection by design) di qualsiasi trattamento. La valutazione di impatto costituisce una buona prassi al di là dei requisiti di legge, poiché attraverso di essa il titolare può ricavare indicazioni importanti e utili a prevenire incidenti futuri.

4.2.2 IL REGISTRO UNICO DEI TRATTAMENTI

Ogni titolare del trattamento e, ove applicabile, il suo rappresentante gestiscono e aggiornano un registro delle attività di trattamento svolte sotto la propria responsabilità.
Tale registro contiene tutte le seguenti informazioni:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento e delle categorie di dati personali, una descrizione delle categorie di interessati;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1. 2. (considerando 2 e art. 30).

In allegato al presente documento si riporta la versione del suddetto registro adottato dall'Ente secondo il seguente schema:

ENTE TITOLARE DEL TRATTAMENTO	COMUNE DI
indirizzo	
n. tel.	
mail	
PEC	
Delegato del Titolare (eventuale)	
indirizzo	
n. tel.	
mail	
PEC	

TRATTAMENTO																														
n. ordine	Processo/Macro Attività	Descrizione	Finalità oltre ad artt.li 822 e 824 CC (demanio Pubblico) e D.lgs 42/2004 (patrimonio culturale nazionale)	Principale base giuridica	Designato/Delegato al trattamento (interno) e/o Responsabile del trattamento (esterno)	Categorie trattamento																								
						Raccolta	Registrazione	Organizzazione	Strutturazione	Conservazione	Modifica	Estrazione	Consultazione	Uso	Comunicazione	Diffusione	Raffronto	Interconnessione	Archiviazione	Limitazione	Cancellazione	Distruzione

4.3 LA SICUREZZA DEI DATI E DEI SISTEMI INFORMATIVI

Come noto la sicurezza nell'informatica equivale ad attuare tutte le misure e tutte le tecniche necessarie per proteggere l'hardware, il software ed i dati dagli accessi non autorizzati (intenzionali o meno), per garantirne la riservatezza, nonché eventuali usi illeciti, dalla divulgazione, modifica e distruzione. Si include, quindi, la sicurezza del cuore del sistema informativo, cioè il centro elettronico dell'elaboratore stesso, dei programmi, dei dati e degli archivi.

Riguardo l'aspetto "sicurezza" connesso alla rete telematica essa può essere considerata una disciplina mediante la quale ogni organizzazione che possiede un insieme di beni, cerca di proteggerne il valore adottando misure che contrastino il verificarsi di eventi accidentali o intenzionali che possano produrre un danneggiamento parziale o totale dei beni stessi o una violazione dei diritti ad essi associati. Un bene può essere un'informazione, un servizio, una risorsa hardware o software e può avere diversi modi possibili di interazione con un soggetto (persona o processo). Se, ad esempio, il bene è un'informazione, ha senso considerare la lettura e la scrittura (intesa anche come modifica e

cancellazione); se invece il bene è un servizio, l'interazione consiste nella fruizione delle funzioni offerte dal servizio stesso.
Nell'ottica del regolamento europeo n. 2016/679 questo concetto di sicurezza informatica ha assunto un significato più attuale alla luce anche dei sempre più numerosi attacchi ed incidenti di natura informatica che lasciano intuire una preoccupante tendenza alla crescita di tale fenomeno.
In particolare negli ultimi tempi si è assistito ad una rapida evoluzione della minaccia che possiamo definire "cibernetica" che è divenuta un bersaglio specifico per alcune tipologie di attaccanti particolarmente pericolosi.
I pericoli legati a questo genere di minaccia sono particolarmente gravi per due ordini di motivi:
il primo è la quantità di risorse che gli attaccanti possono mettere in campo, che si riflette sulla sofisticazione delle strategie e degli strumenti utilizzati;
il secondo è rappresentato dal fatto che il primo obiettivo perseguito è il mascheramento dell'attività, in modo tale che questa possa procedere senza destare sospetti.
La combinazione di questi due fattori fa sì che, a prescindere dalle misure minime di sicurezza previste dal nostro codice in materia di protezione dei dati personali, (antivirus, firewall, difesa perimetrale, ecc.) bisogna fare particolare attenzione alle attività degli stessi utenti che devono rimanere sempre all'interno dei limiti previsti. Infatti elemento comune e caratteristico degli attacchi più pericolosi è l'assunzione del controllo remoto della macchina attraverso una scalata ai privilegi.
Naturalmente le misure preventive, destinate ad impedire il successo dell'attacco, devono essere affiancate da efficaci strumenti di rilevazione, in grado di abbreviare i tempi, oggi pericolosamente lunghi, che intercorrono dal momento in cui l'attacco primario è avvenuto e quello in cui le conseguenze vengono scoperte.
In tale quadro di protezione diventa fondamentale l'analisi delle vulnerabilità del sistema informatico.
In primo luogo le vulnerabilità sono l'elemento essenziale per la scalata ai privilegi che è condizione determinante per il successo dell'attacco; pertanto la loro eliminazione è la misura di prevenzione più efficace.
Secondariamente si deve considerare che l'analisi dei sistemi è il momento in cui è più facile rilevare le alterazioni eventualmente intervenute e rilevare un attacco in corso.
Pertanto nell'ottica del legislatore comunitario per sicurezza delle reti e dell'informazione bisogna intendere la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica (CERT), gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza.
Ciò ovviamente comprende anche misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica.
Per mantenere la sicurezza e prevenire trattamenti in violazione al GDPR, il titolare del trattamento o il responsabile del trattamento deve valutare anche il rischio informatico che può essere definito come il rischio di danni economici (rischi diretti) e di reputazione (rischi indiretti) derivanti dall'uso della tecnologia, intendendosi con ciò sia i rischi impliciti nella tecnologia (i cosiddetti rischi di natura endogena) che i rischi derivanti dall'automazione, attraverso l'uso della tecnologia, di processi operativi aziendali (i cosiddetti rischi di natura esogena).
In particolare questi ultimi possono essere:

- danneggiamento di hardware e software;
- errori nell'esecuzione delle operazioni nei sistemi;
- malfunzionamento dei sistemi;
- programmi indesiderati.

Vanno ovviamente predisposte specifiche misure per limitare tali rischi, quali la cifratura. Tali misure devono assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.
Nel GDPR un chiaro riferimento alle misure di sicurezza già si trova nell'art. 22 quando si chiarisce che il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento (principio di accountability).

Mentre, più nello specifico, l'art. 32 del Regolamento ne parla a proposito della sicurezza del trattamento. Tenuto conto, quindi, dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono tra l'altro, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

In particolare, quindi, si pone l'accento sulla pseudonimizzazione intesa come un particolare trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
Inoltre per la prima volta si parla di resilienza dei sistemi informatici intesa come la capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire la disponibilità dei servizi erogati.
Notevole rilevanza viene attribuita dal legislatore comunitario anche al disaster recovery, per cui diventa fondamentale predisporre uno specifico piano con il quale si intende fornire servizi volti all'analisi dei rischi di inoperatività del sistema EDP (informatico) e delle misure da adottare per ridurli, nonché la messa a punto del vero e proprio piano di emergenza informatica, che ricomprende, in particolare, procedure per l'impiego provvisorio di un centro di elaborazione dati alternativo o comunque l'utilizzo di macchine di soccorso da utilizzare in attesa della riattivazione.

4.3.1 VERIFICA MISURE MINIME DI ADEGUATEZZA AGID - GDPR

Le misure minime di sicurezza informatica per le PA, che contengono le indicazioni per valutare e innalzare il livello di sicurezza informatica dell'Ente, dovevano essere adottate dalle amministrazioni entro il 31 dicembre 2017. L'obiettivo del documento – pubblicato in Gazzetta Ufficiale - era quello di fornire alle pubbliche amministrazioni un riferimento pratico per valutare e migliorare il proprio livello di sicurezza informatica, al fine di contrastare le minacce più comuni e frequenti a cui sono soggette le PA. Il documento era già stato emanato e reso disponibile da AgID e dal CERT–PA da aprile 2016.

Le "Misure minime di sicurezza informatica per la PA" prevedono tre diversi livelli di attuazione: **il livello minimo** stabilisce i criteri di base ai quali ogni pubblica amministrazione deve essere conforme, in termini tecnologici, organizzativi e procedurali. I livelli successivi prevedono strumenti di protezione più completi.

Considerato che il nuovo regolamento GDPR "rifonda" le misure minime di sicurezza che sono alla base del sistema di protezione dei dati personali, l'analisi del DPO su tali aspetti, è stata condotta ritenendo comunque utile ed opportuno un riferimento comparativo delle rilevazioni, con quanto previsto e standardizzato dalla circolare AGID 2/2017; tale attività ha consentito infatti allo scrivente di ritenere adeguate/idonee (non idonee/non adeguate) le misure adottate dall'Ente in quanto compatibili con lo standard previsto da AGID. L'analisi condotta, mediante l'utilizzo di un particolare tool, ha consentito di valutare la compliance, sulla base di un modello di riferimento di gestione elaborato da AISIS, dell'adeguamento al GDPR e la compliance ai requisiti minimi di sicurezza di AGID che sono obbligatori per la Pubblica Amministrazione. Vengono di seguito riportati i risultati ottenuti:

DATA INVENTORY						
			©Aisis 2017			
	Domande	Risposte (rispondere apponendo una "X")				Note
	DATA INVENTORY					
1	Esistenza mappa applicativa del sistema informativo aziendale	sì	copertura superiore al 50% degli utilizzatori	Inferiore al 50% dei sistemi	no	
	Valutazione attuale	X				
2	Esistenza elenco degli applicativi in uso	sì	copertura superiore al 50% degli utilizzatori	Inferiore al 50% dei sistemi	no	
	Valutazione attuale	X				
3	Esistenza di documentazione tecnica della struttura del Database per applicativo	sì	copertura superiore al 50% degli utilizzatori	Inferiore al 50% dei sistemi	no	
	Valutazione attuale				X	
4	Esistenza documentazione formale della allocazione fisica del dati sui server	sì	copertura superiore al 50% degli utilizzatori	Inferiore al 50% dei sistemi	no	
	Valutazione attuale	X				
5	Esistenza procedure formalizate di backup per singolo applicativo/Database	sì	copertura superiore al 50% degli utilizzatori	Inferiore al 50% dei sistemi	no	
	Valutazione attuale	X				
6	Esistenza di procedure di gestione delle basi dati (patching, manutenzione..)	sì	copertura superiore al 50% degli utilizzatori	Inferiore al 50% dei sistemi	no	
	Valutazione attuale	X				
7	Esistenza procedure formalizzate di restore	sì	copertura superiore al 50% degli utilizzatori	Inferiore al 50% dei sistemi	no	
	Valutazione attuale	X				

RISCHI E IMPATTI						©Aldo 2017	
	Domande	Risposte (rispondere apponendo una "X")					Note
	RISCHI ESTERNI (legati ai Fornitori)						
1	Instabilità mercato (pressioni competitive/solidità fornitore)	alta	media	bassa	irrilevante		
				X			
2	Quali impatti in caso di eventuale indisponibilità fornitore	indisponibilità sistema processo gestito manualmente	impatto medio sulla funzionalità del processo	impatto limitato su alcuni sistemi e servizi	bassi impatti		
				X			
3	Non conformità dei fornitori agli SLA concordati	non definiti da contrattuali	Sla definiti ma difficilmente misurabili	Sla definiti e monitorati con strumenti sw del fornitore	Sla definiti e monitoarti internamente		
		X					
4	Variazioni normativa di settore	modifiche periodiche che richiedono modifiche sw	modifiche periodiche	modifiche non frequenti	Stabile		
				X			
	RISCHI INTERNI (legate alle modalità di trattamento)						
5	Formazione e change su privacy e sicurezza agli utilizzatori di ICT	no	inferiore al 50% dei sistemi	copertura superiore al 50% degli utilizzatori	si		
			X				
6	Esistenza e manutenzione Elenco trattamenti	no	inferiore al 50% dei sistemi	copertura superiore al 50% degli utilizzatori	si		
					X		
7	Esistenza censimento delle risorse e sistemi in rete	no	inferiore al 50% dei sistemi	copertura superiore al 50% degli utilizzatori	si		
					X		
8	IDM e logging	no	inferiore al 50% dei sistemi	copertura superiore al 50% degli utilizzatori	si		
					X		
	RISCHI TECNOLOGICI						
9	Danneggiamenti fisici server farm (incendio, allagamento, crollo) e interruzione funzionamento server farm	in caso di indisponibilità il processo non può essere gestito manualmente	in caso di indisponibilità il processo viene gestito manualmente	server in cluster	server in cloud		
			X				
10	Interruzione rete dati e rete fonia	in caso di indisponibilità il processo non può essere gestito manualmente	in caso di indisponibilità il processo viene gestito manualmente	work around con utilizzo pc stand alone	rete dati e fonia ridondata e sla fornitore h24		
			X				
11	Interruzione servizi applicativi, interruzione sistema di integrazione, anomalie database	in caso di indisponibilità il processo non può essere gestito manualmente	in caso di indisponibilità il processo viene gestito manualmente	work around con utilizzo pc stand alone	assistenza e sla fornitore h24		
			X				
12	Accessi non autorizzati ai sistemi e al db, copia non autorizzata di dati, manomissione e falsificazione dati	possibili	possibili ma non probabili	monitoraggio accessi	monitoraggio degli accessi e log amministratori sistema		
				X			
	RISCHI GESTIONALI (legati al Team ICT)						
13	Esistenza Piano di adeguamento alla compliance (obiettivi e output formalmente definiti)	non definiti	definiti ma non formalizzati	definiti ma formalizzati solo per 50% dei sistemi	definiti e formalizzati		
		X					
14	Definizione ruoli (chiara definizione responsabili, identificazione degli amministratori, definizione k-users)	non definiti	definiti ma non formalizzati	definiti ma formalizzati solo per 50% dei sistemi	definiti e formalizzati		
					X		
15	Attività di monitoraggio e controllo	non definito	poco definito	monitoraggio manuale periodico dei principali sistemi	utilizzo di medotodologia e strumenti autorutilizzati per monitoraggio periodico delle attività		
					X		
16	Rischi legati al quadro delle Risorse e skill disponibili (capacity)	risorse non preparate e non adeguate	capacity in fase di valutazione	risorse in corso di formazione	skill e risorse adeguate		
		X					

MISURE ORGANIZZATIVE

©Aisis 2017

	Domande	Risposte (rispondere apponendo una "X")				Note
	MISURE ORGANIZZATIVE					
1	Esistenza modello organizzativo Privacy per applicazione 196/03	si manutenuto	si in corso di revisione	si obsoleto	no	
	Valutazione attuale			X		
2	Adeguamento del modello al GDPR	si	si in corso di predisposizione	Progetto proposto alla direzione	no	
	Valutazione attuale		X			
3	Procedure organizzative formalizzate per definizione Titolarità, Co-Titolarità, Nomina Responsabili e Autorizzati	si	si in corso di predisposizione	Progetto proposto alla direzione	no	
	Valutazione attuale		X			
4	Presenza formalizzata del DPO	si	in corso di approvazione	in corso di individuazione	no	
	Valutazione attuale	X				
5	Definizione delle informative e dei consensi	si	si per la maggior parte delle funzioni	parzialmente per alcune funzioni	no	
	Valutazione attuale	X				
6	Esistenza sistema di gestione documentale della privacy	si	si per la maggior parte delle funzioni	parzialmente per alcune funzioni	no	
	Valutazione attuale			X		
7	Esistenza sistema di monitoring delle procedure privacy e sicurezza	si	si per la maggior parte delle funzioni	parzialmente per alcune funzioni	no	
	Valutazione attuale			X		

MISURE TECNICHE

©Aisis 2017

	Domande	Risposte (rispondere apponendo una "X")				Note
	MISURE TECNICHE					
1	Inventario e assessment delle tecnologie in essere	si	copertura superiore al 50% dei sistemi	Inferiore al 50% dei sistemi	no	
	Valutazione attuale	X				
2	Esistenza di sistema di Identy Management	si	solo per gli applicativi core	Utilizzo funzioni base del dominio	no	
	Valutazione attuale	X				
3	Esistenza sistema di SSO	si	solo per gli applicativi core	procedura manuale	no	
	Valutazione attuale			X		
4	Esistenza di procedure formalizzate per la business continuity e il disaster recovery	si	copertura superiore al 50% dei sistemi	Inferiore al 50% dei sistemi	no	
	Valutazione attuale	X				
5	Esistenza di procedure/sistemi per logging (degli eventi)	si	copertura superiore al 50% dei sistemi	Inferiore al 50% dei sistemi	no	
	Valutazione attuale	X				
6	Esistenza di procedure/sistemi per logging degli amministratori	si	copertura superiore al 50% dei sistemi	Inferiore al 50% dei sistemi	no	
	Valutazione attuale	X				

MISURE APPLICATIVE

©Aisis 2017

	Domande	Risposte (rispondere apponendo una "X")				Note
	MISURE APPLICATIVE					
1	Pseudoanonimizzazione e encryption	si	copertura superiore al 50% dei sistemi	Inferiore al 50% dei sistemi	no	% sul numero delle basi dati coperte
	Valutazione attuale				X	
2	Gestione unificata e centralizzata dell'informativa, dei consensi e delle revoca	si con piattaforma specifica	si con integrazioni	parzialmente	no	
	Valutazione attuale				X	
3	Formalizzazione procedura per portabilità dei dati vs cittadino (art 20 GDPR)	si	solo per gli applicativi core	solo per dati amministrativo-contabili	no	
	Valutazione attuale				X	
4	Esistenza analisi tipologia dei dati trattati per singolo db	si	copertura superiore al 50% dei sistemi	Inferiore al 50% dei sistemi	no	
	Valutazione attuale				X	

DATA INVENTORY	As Is	Best
Esistenza mappa applicativa del sistema informativo aziendale	100	100
Esistenza elenco degli applicativi in uso	100	100
Esistenza di documentazione tecnica della struttura del Database per applicativo	20	100
Esistenza documemtazione formale della allocazione fisica del dati sui server	100	100
Esistenza procedure formalizate di backup per singolo applicativo/Database	100	100
Esistenza di procedure di gestione delle basi dati (patching, manutenzione..)	100	100
Esistenza procedure formalizzate di restore	100	100

GESTIONE RISCHI	As Is	Best
Rischi Esterni	65	100
Rischi interni	88,75	100
Rischi Tecnologici	61,25	100
Rischi Manageriali	60	100

MISURE ORGANIZZATIVE	As Is	Best
Esistenza modello organizzativo Privacy per applicazione 196/03	40	100
Adeguamento del modello al GDPR	65	100
Procedure organizzative formalizzate per definizione Titolarità, Co-Titolarità, Nomina Responsabili e Autorizzati	65	100
Presenza formalizzata del DPO	100	100
Definizione delle informative e dei consensi	100	100
Esistenza sistema di gestione documentale della privacy	40	100
Esistenza sistema di monitoring delle procedure privacy e sicurezza	40	100

MISURE TECNICHE	As Is	Best
Inventario e assessment delle tecnologie in essere	100	100
Esistenza di sistema di Identy Management	100	100
Esistenza sistema di SSO	40	100
Esistenza di procedure formalizzate per la business continuity e il disaster recovery	100	100
Esistenza di procedure/sistemi per logging (degli eventi)	100	100
Esistenza di procedure/sistemi per logging degli amministratori	100	100

MISURE APPLICATIVE	As Is	Best
Pseudoanonimizzazione e encryption	20	100
Gestione unificata e centralizzata dell'informativa, dei consensi e delle revoca	20	100
Formalizzazione procedura per portabilità dei dati vs cittadino (art 20 GDPR)	20	100
Esistenza analisi tipologia dei dati trattati per singolo db	20	100

RISCHI ESTERNI (legati ai Fornitori)	As Is	Best
Instabilità mercato (pressioni competitive/solidità fornitore)	40	20
Quali impatti in caso di eventuale indisponibilità fornitore	40	20
Non conformità dei fornitori agli SLA concordati	100	20
Variazioni normativa di settore	40	20

RISCHI INTERNI (legate alle modalità di trattamemto)	As Is	Best
Formazione e change su privacy e sicurezza agli utilizzatori di ICT	65	20
Esistenza e manutenzione Elenco trattamenti	20	20
Esistenza censimento delle risorse e sistemi in rete	20	20
IDM e logging	20	20

RISCHI TECNOLOGICI	As Is	Best
Danneggiamenti fisici server farm (incendio, allagamento, crollo) e interruzione funzionamento server farm	65	20
Interruzione rete dati e rete fonia	65	20
Interruzione servizi applicativi, Interruzione sistema di integrazione, anomalie database	65	20
Accessi non autorizzati ai sistemi e al db, copia non autorizzata di dati, manomissione e falsificazione dati	40	20

RISCHI GESTIONALI (legati al Team ICT)	As Is	Best
Esistenza Piano di adeguamento alla compliance (obiettivi e output formalmente definiti)	100	20
Definizione ruoli (chiara definizione responsabili, identidicazione degi amministratori, definizione k-users)	20	20
Attività di monitoraggio e controllo	20	20
Rischi legati al quadro delle Risorse e skill disponibili (capacity)	100	20

	As Is	Best
DATA INVENTORY	100,00	100,00
GESTIONE RISCHI/IMPATTI	68,75	100,00
MISURE ORGANIZZATIVE	64,29	100,00
MISURE TECNICHE	90,00	100,00
MISURE APPLICATIVE	20,00	100,00
RISCHI ESTERNI (legati ai Fornitori)	55,00	20,00
RISCHI INTERNI (legate alle modalità di trattamemto)	20,00	20,00
RISCHI TECNOLOGICI	58,75	20,00
RISCHI GESTIONALI (legati al Team ICT)	60,00	20,00

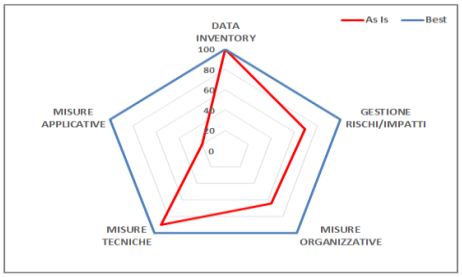
Past Health
Analisi condotta presso il Comune di AIROLA

DATA AVVIO	18/08/2018	CONTATTO	0
DATA AVVIO in PRODUZIONE	In progress		
DATA FINE Progetto	18/06/2019	OWNER	0

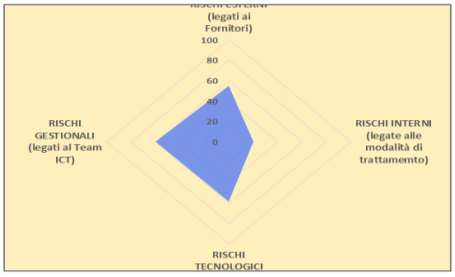
DESCRIZIONE PROGETTO

L'utilizzo del tool consente di valutare la compliance al modello di gestione Aifsis dell'adeguamento al GDPR e la compliance ai requisiti minimi di sicurezza di Agid che sono obbligatori per la Pubblica Amministrazione. In proposito si richiamano i termini di applicazione che sono: il 31.12 2017 per la compliance delle misure minime di sicurezza Agid e il 25.5.2018 per la compliance al GDPR

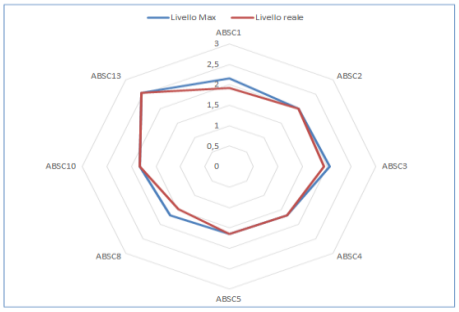
VALUTAZIONE SULLA COMPLIANCE AL NUOVO GDPR



RISCHI/IMPATTI SU PRIVACY E SICUREZZA



VALUTAZIONE SULLA COMPLIANCE AI REQUISITU MINIMI SICUREZZA AGID



©Aisis 2017

In quest'ultimo grafico vengono riportati i risultati ottenuti dalle valutazioni effettuate sulla compliance AISIS e AGID al nuovo regolamento UE GDPR, dove si evince appunto come il livello di sicurezza implementato dall'Ente abbia raggiunto le misure minime necessarie.

Il livello minimo, indicato nella tabella successiva con "M" ("Minimo"), è quello al quale ogni pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme.
Nelle immagini successive si riportano pertanto le misure che l'Ente ha attuato tramite il Centro Servizi Territoriale della Provincia di Benevento, per garantire che il livello di sicurezza del sistema informativo sia conforme a quello minimo necessario in ottemperanza alla circolare AGID 2/2017:

Centro Servizi Territoriale della Provincia di Benevento

Atto di adozione prot. n. _____ **Benevento, _____**

Misure Minime di sicurezza ICT per le PA

Il presente documento è una implementazione da parte di Easyteam.org del documento ufficiale AgID reperibile al seguente indirizzo: http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/cert-pa/misure-minime-sicurezza-ict-pubbliche-amministrazioni

Mantenendo gli stessi contenuti del documento originale, aggiunge alcune tabelle per una più facile comprensione e gestione del piano di sicurezza.

Il presente documento va ad integrarsi ai documenti:

- Manuale di gestione del Protocollo Informatico
- Piano di sicurezza informatica, continuità operativa a e di Disaster Recovery
- Certificazione Misure Minime Dlgs 196/2003 Allegato B con allegato Piano di gestione dei rischi
- Relazione semestrale Amministratore di Sistema

Il presente documento presenta i seguenti allegati:

1. Whitelist degli applicativi informatici consentiti
2. Inventario dei pc (riferirsi alla ABSC 1.1.1)
3. Inventario dei software di ogni singola macchina
4. Inventario di tutti gli account
5. Report sulle vulnerabilità

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

costituisce pieno adempimento a quanto richiesto da:

- Circolare AgID 18/04/2017 n. 2
- Direttiva PCM 01/08/2015

E' importante tenere presente che i documenti citati nell'elenco precedente costituiscono un unico corpus e che solo congiuntamente permettono all'Amministrazione di adempiere completamente a quanto richiesto dalle normative.

Acronimi utilizzati nelle Circolari ufficiali e nel resto del presente documento:

SIGLA	SIGNIFICATO	NOTE
ABSC	AgID Basic Security Control(s)	Controlli di sicurezza previsti dall'AgID
CSC	Critical Security Control(s)	Controlli di sicurezza critici, ritenuti fondamentali
CSSC	CIS - Critical Security Controls for Effective Cyber Defense	Controlli di sicurezza critici per una protezione funzionale dagli attacchi cibernetici

Livelli di sicurezza utilizzati nel presente documento:

Nel documento, per ogni singola implementazione tecnica, è indicato il livello di sicurezza relativo. Le misure previste dal livello minimo devono essere messe in atto quanto prima, poiché ritenute necessarie dall'AgID.

SIGLA	SIGNIFICATO	NOTE
M	Minimo	Livello sotto il quale nessuna amministrazione può scendere: i controlli indicati debbono riguardarsi come obbligatori
S	Standard	Base di riferimento per un livello di sicurezza completo. Rappresenta il primo step a cui tendere per la protezione della propria infrastruttura informatica
A	Alto	Obiettivo finale a cui tendere, al completamento del piano di sicurezza

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

Nel corso del documento sono state evidenziate con diversi colori le singole misure previste, in modo da fornire un veloce colpo d'occhio su quanto sia:

- strettamente necessario: verde -da programmare: arancione -obiettivo finale: rosso

ALLEGATO 1 - Modulo implementazione Misure Minime con suggerimenti

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	**Implementare un inventario delle risorse attive correlato a quello ABSC 1.4**	L'inventario è riportato in allegato al presente documento e conservato presso l'UFFICIO ASSOCIATO PER IL DIGITALE (UAD) istituito presso il CST e/o presso il protocollo del Comune consorziato aderente all'UAD, ed elenca i dispositivi informatici collegati in rete in modo permanente o provvisorio. *Viene inventariato ogni dispositivo: PC, notebook, laptop, server, stampanti, fotocopiatrici in rete, smartphone, telefoni VOIP, switch ed apparati di rete, router, ecc.* *Sono da inventariare anche eventuali risorse che non vengano collegate in rete (ad es. PC isolati).* *Nell'elenco, per ogni dispositivo, sono riportate almeno le seguenti informazioni:* • *codice identificativo univoco assegnato all'apparato (ad es. PC08; oppure l'identificativo del bene assegnato nell'inventario patrimoniale);*

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

					• *descrizione breve del tipo di dispositivo;* • *MAC Address;* • *indirizzo IP (se statico; se invece l'indirizzo IP viene assegnato dinamicamente, indicare tale fatto, attivando la conservazione del log del DHCP server - vedi punti 1.2.1 e 1.2.2);* • *Collocazione e persona alla quale è assegnato.* *L'inventario, su proposta dell'UAD, viene realizzato dal sistema di monitoraggio automatico che prevede delle operazioni preventive da parte dell'amministratore di sistema come: la creazione degli account con privilegi di amministratore su ogni singola macchina o l'utilizzo di un dominio centralizzato.* *Il documento deve riportare la data di ultimo aggiornamento.*
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	*Lo strumento adottato è un software di monitoraggio, installato su un pc/server nella LAN dell'Ente e riportato nella whitelist allegata al presente documento.*
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Il *software di monitoraggio* è configurato con i trigger che azionano allarmi (segnalazione diretta sul pannello generale, segnalazione indiretta alla mailing list di amministrazione) in caso di anomalie.
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Il *software di monitoraggio* è configurato per monitorare il traffico di tutti gli apparati connessi alla rete.
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	La LAN dell'Ente non utilizza il DHCP ma solo indirizzamenti statici.
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	N/A
1	**3**	**1**	**M**	**Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.**	L'elenco di cui alla misura 1.1.1 è aggiornato automaticamente dal *software di monitoraggio*. L'aggiornamento dell'elenco allegato al presente documento è a carico dell'Amministratore di Sistema referente dell'Ente e dell'UAD (di seguito semplicemente REFERENTE) e viene

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

					modificato quando nuovi dispositivi approvati vengono collegati in rete.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	L'inventario è aggiornato automaticamente dal *software di monitoraggio*.
1	4	1	M	**Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.**	Vedi punto 1.1.1.
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	Il *software di monitoraggio* è configurato in modo tale da tener traccia delle informazioni richieste. All'interno dell'Ente non è ammesso l'utilizzo di dispositivi personali. Eventuali dispositivi esterni, ad esempio introdotti da operatori di società di assistenza contrattualizzati dall'Ente devono richiedere espressa autorizzazione al referente che ne traccerà l'utilizzo. Utilizzare le matricole o il nome dell'ufficio associato al posto dei nomi dei dipendenti nella nomenclatura delle macchine; Utilizzare come nome della macchina il nome dell'Ufficio (es. Anagrafe1 – Tributi2);
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	-
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	-
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	-

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	**Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.**	L'elenco è redatto dal Responsabile per la Transizione Digitale e riportato in allegato al presente documento/conservato presso l'UFFICIO ASSOCIATO PER IL DIGITALE (UAD) istituito c/o CST o presso il protocollo del Comune consorziato aderente all'UAD. Sono state date direttive al personale ed agli amministratori di sistema di non installare alcun software diverso. In caso di necessità, questa viene evidenziata agli Amministratori di Sistema, che ne verificano la reale esigenza, verifichino l'esistenza di soluzioni Open Source equipollenti, ed eventualmente provvedono affinché sia installato, come pure che venga aggiornato l'elenco. Le abilitazioni all'installazione del software sono state concesse soltanto agli amministratori di sistema (vedi 5.1.1) *Nell'elenco, per ciascun software inventariato vanno riportati almeno i seguenti dati:* *- tipologia dispositivo* *- nome del software* *- fornitore e/o marca* *- versione* *- soggetto autorizzante* *- eventuale data di scadenza dell'autorizzazione* *- .....* *Si suggerisce di riportare anche le informazioni sulla licenza di utilizzo (ad es. numero e data fattura, periodo di validità della licenza, ecc.)*

					Per la costruzione dell'elenco si può partire dall'analisi del software realmente presente sui computer del Comune. Da tale operazione potrebbero emergere software ad uso personale o software impiegato, ma obsoleto (versioni non più mantenute dal produttore). *Nel caso in cui il fornitore di un software fornisca o sia comunque responsabile anche dell'hardware o macchina virtuale sul quale tale software è installato, va nominato Amministratore di Sistema (ai sensi del Codice della privacy) per quel server con la disposizione di fornire l'elenco del software installato e degli aggiornamenti.*
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	L'elenco delle applicazioni autorizzate è presente nella "whitelist" riportata in allegato al presente documento depositato presso l'UFFICIO ASSOCIATO PER IL DIGITALE (UAD) istituito presso il CST o presso il protocollo del Comune consorziato aderente all'UAD.
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	La whitelist per l'Ente è unica perché le funzioni assolte dalle singole macchine dell'amministrazione sono assimilabili. Il caso citato del software personalizzato non è presente nell'Ente.
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	-
2	**3**	**1**	**M**	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Gli Amministratori di Sistema eseguono periodicamente la verifica del software installato su ciascun dispositivo e comparano il risultato con l'elenco di cui al punto 2.1.1. Verosimilmente i due elenchi saranno sempre analoghi perché le installazioni sono consentite al solo amministratore di sistema. *Si suggerisce una cadenza della scansione semestrale.*

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	*L'inventario avviene automaticamente tramite il software di monitoraggio.*
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	-
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	-

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	**Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.**	Gli Amministratori di Sistema hanno definito e documentato le configurazioni sicure standard per ciascun sistema operativo utilizzato. *Questo può essere raggiunto definendo e documentando le scelte che occorre operare durante la procedura di installazione e per la configurazione, incluse le scelte relative alla configurazione del firewall, antivirus, ecc.; oppure utilizzando sistemi di clonazione e di copie d'immagine (vedi* 3.3.1 e 3.3.2). Tale documentazione è conservata presso l'UFFICIO ASSOCIATO PER IL DIGITALE (UAD) istituito c/o CST o presso il protocollo del Comune consorziato aderente all'UAD.
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente:	**La configurazione dei sistemi spetta all'amministratore che ha provveduto alla rimozione di tutti gli account inutili lasciando solo il proprio e quello all'operatore dell'Ufficio pertinente.**

				eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	**L'amministratore ha posto tutti i servizi inutili nella modalità disabilitata mentre i servizi utili e necessari sono stati posti in modalità di avvio automatico. Per i servizi inutili che è stato possibile disinstallare l'amministratore li ha rimossi dal sistema aumentandone la sicurezza.**
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	-
3	2	1	M	***Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.***	Vedi 3.1.1.
3	2	2	M	***Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.***	L'amministratore utilizzerà l'immagine creata e salvata in precedenza del sistema corrotto per ripristinare in tempi rapidi la messa in esercizio. In alternativa reinstallerà la configurazione standard utilizzando gli applicativi licenziati e quelli della whitelist.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	L'amministratore di sistema aggiorna l'immagine salvata ogni qualvolta cambia la sua configurazione. Questa operazione garantisce il ripristino all'ultima configurazione utilizzata dall'operatore.
3	3	1	M	**Le immagini d'installazione devono essere memorizzate offline.**	Sono state date disposizioni all'amministratore di sistema di salvare le immagini d'installazione sul supporto HD esterno rimovibile. Quindi l'Ente per consentire lo storage delle immagini, dovrà dotarsi di Dischi rimovibili o NAS di adeguata capienza. Sarà cura dell'amministratore eseguire la disconnessione dalla rete locale dell'unità esterna di salvataggio a seguito di backup e restore delle immagini. L'unità verrà riposta in luogo sicuro a lui solo accessibile.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	*Vedi 3.3.1*

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

3	4	1	M	**Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).**	Per attività di gestione effettuate da reti esterne alla rete comunale vengono utilizzate connessioni VPN o comunque criptate. Anche gli applicativi utilizzati dalla teleassistenza utilizzano algoritmi di cifratura nella comunicazione.
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	L'amministratore dovrà accertarsi che tali sistemi siano presenti nei sistemi operativi installati. Infatti tale condizione è verificata automaticamente dai moderni e supportati sistemi operativi ed antivirus. Sarà compito dell'Ente garantire la copertura della spesa per attuare tali prescrizioni.
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	-
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	-
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	-
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	-
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	-

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	**Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con**	Ad ogni modifica delle configurazioni vengono eseguite scansioni delle vulnerabilità tramite lo strumento di analisi delle

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

				strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	vulnerabilità presente in whitelist.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Sono state date disposizioni agli Amministratori di Sistema di effettuare almeno semestralmente una scansione su tutta la rete tramite lo strumento di analisi delle vulnerabilità in dicato anche in whitelist.
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common ConfigurationEnumeration Project).	-
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	La misura 4.2.1 verrà attuata a seguito della 4.1.1. In seguito alla 4.1.1.il tracciamento delle attività avverrà tramite un'analisi approfondita dei log di sistema, per cui bisogna essere sicuri che i log siano validi e non siano stati modificati in alcun modo. La correlazione avverrà a mano nelle more di trovare una soluzione automatizzata.
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	**Utilizzare software che monitorano le entry nei file di log di sistema e che possano essere configurati per eseguire date operazioni in presenza di determinate righe di log.** **La verifica nelle more della soluzione automatizzata verrà fatta a mano dall'amministratore di sistema.**
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	**Riferirsi alla misura 4.2.2**
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	**Le scansioni delle vulnerabilità avverranno dal solo account con privilegi di amministratore. Verrà disabilitata la possibilità agli altri account di accedere al sistema delle scansioni.**
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale	**Tutte le macchine della LAN hanno un solo account con privilegi di amministratore ed utilizzando IP statici è possibile eseguire**

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

				autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	**con solo tali privilegi la scansione delle vulnerabilità da tutte le macchine.**
4	4	1	M	**Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.**	Sono state date disposizioni agli Amministratori di Sistema di verificare che il software di scansione prima di ciascun utilizzo sia aggiornato rispetto alle vulnerabilità.
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	Riferirsi alla misura 4.1.1
4	5	1	M	**Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.**	L'applicazione delle patch di vulnerabilità è schedulata dagli Amministratori di Sistema e dovrà essere eseguita contestualmente alla scoperta della vulnerabilità. Nell'impossibilità di applicazione immediata della patch la macchina dovrà essere sconnessa dalla rete. L'amministratore dovrà abilitare la modalità di aggiornamento automatico per tutti gli applicativi che abbiano la funzionalità, per gli altri dove non esiste la possibilità di un automatismo le patch verranno installate manualmente. Per non appesantire il download complessivo della LAN si consiglia all'amministratore di sistema di configurare un proxy server.
4	5	2	M	**Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.**	Sono state date disposizioni agli Amministratori di Sistema di controllare ed aggiornare manualmente periodicamente i sistemi non raggiungibili via rete. Sono state date disposizioni ai possessori di smartphone, tablet o notebook di proprietà dell'ente di accettare gli aggiornamenti proposti automaticamente dal sistema.
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	Sono state date disposizioni agli Amministratori di Sistema in merito.
4	7	1	M	**Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando**	Sono state date disposizioni agli Amministratori di Sistema di verificare la risoluzione delle vulnerabilità. Nel caso non siano state trovate o applicate le patch necessarie, gli Amministratori di

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

				un ragionevole rischio.	Sistema documentano il caso, le eventuali contromisure o la motivazione della mancata risoluzioni su apposito registro/rapportino conservato presso l'ente.
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	Attività di VulnerabilityAssessment devono essere effettuate sui sistemi e le reti più rilevanti in termini di operatività comunale. Le Vulnerabilità identificate devono essere risolte. Gli aggiornamenti dei sistemi e dei software spesso infatti migliorano e risolvono falle delle versioni precedenti.
4	8	1	M	**Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).**	*L'amministratore di sistema utilizza lo strumento di analisi delle vulnerabilità e da questo si* analizzano le azioni suggerite dal report prodotto dallo strumento di scansione, agendo in base alle priorità ivi indicate.
4	8	2	M	**Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.**	Vedi 4.8.1 Sono state date disposizioni agli Amministratori di Sistema di ordinare secondo la priorità il report prodotto.
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	L'amministratore di sistema deve, in caso di vulnerabilità grave, isolare la macchina dalla rete laddove l'assenza di patch potrebbe provocare danni alle altre macchine della rete. Inoltre se la stessa macchina, seppur isolata dalla rete, può presentare rischi, l'amministratore in assenza di patch deve spegnerla definitivamente e schedulare le azioni risolutive di ripristino.
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	Le patch installabili dall'amministratore di sistema sono tutte quelle consigliate dalle società erogatrici dei software e quindi tale misura non è applicabile.

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	**Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di**	I privilegi di amministratore sono riservati unicamente agli amministratori di sistema espressamente nominato/i da parte

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

				modificare la configurazione dei sistemi.	dell'ente. I privilegi di amministrazione per smartphone e tablet sono assegnati al soggetto al quale l'apparato è dato in dotazione dato che devono avere la possibilità di accettare in autonomia gli aggiornamenti di sicurezza. Tutti gli altri utenti sono operatori senza privilegi di amministrazione. Eventuali permessi particolari a specifici applicativi sono a discrezione dell'amministratore di sistema e saranno da lui stesso valutati necessari e verranno documentati su apposito registro/rapportino conservato presso l'ente.
5	1	2	M	**Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.**	L'amministratore di sistema deve attivare il log di sistema per registrare gli accessi come amministratore su PC, server, apparati di rete.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Le utenze non amministrative devono essere configurate in modo che abbiano privilegi relativi al solo sistema relativo alle attività previste.
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	N/A
5	2	1	M	**Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.**	L'amministratore di sistema è unico all'interno della rete e le sue credenziali sono conservate in modalità protetta.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	N/A
5	3	1	M	**Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.**	Agli amministratori di sistema sono tenuti ad applicare tale misura.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	N/A vedi la 5.2.1
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	N/A vedi la 5.2.1
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di	N/A vedi la 5.2.1

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

				un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	L'amministratore di sistema è tenuto ad abilitare nei log il tracciamento dei tentativi di autenticazione falliti.
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	N/A
5	7	1	M	**Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).**	L'amministratore di sistema genera per tutti gli utenti password di autenticazioni "forti" del tipo *"almeno 8 caratteri di cui uno speciale + 1 numero + una maiuscola". Gli stessi forniscono agli operatori indicazioni dettagliate sulla conservazione sicura di tutte le password di rete e web utilizzate per la funzione svolta nell'Ente.*
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	N/A vedi 5.7.1
5	7	3	M	**Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging)**	Il sistema di autenticazione è configurato per obbligare tutti gli utenti al cambio password ogni 6 mesi.
5	7	4	M	**Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).**	Il sistema di autenticazione è configurato per impedire il riutilizzo delle ultime 6 password per tutti gli utenti.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	**Verifica periodica da parte dell'Amministrazione di sistema.**
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	**Verifica periodica da parte dell'Amministrazione di sistema.**
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	**I sistemi sono configurati per l'accesso come operatore. L'utente amministratore per eseguire operazioni di livello più alto deve comunque utilizzare l'account di operatore ed eseguire i comandi con accesso privilegiato mediante la propria password. Eventuali accessi diretti con l'account privilegiato saranno da lui stesso valutati necessari e verranno documentati su apposito registro/rapportino conservato presso l'ente.**
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori	**N/A**

				debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	10	1	M	**Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.**	Vedi 5.1.1
5	10	2	M	**Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.**	Vedi 5.1.1
5	10	3	M	**Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.**	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo. Vedi 5.1.1
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
5	11	1	M	**Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.**	Le credenziali amministrative non personali sono elencate su un documento conservato presso l'Ente in modo sicuro e protetto ad esclusivo accesso (Allegato).
5	11	2	M	**Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.**	Non si utilizzano certificati digitali per l'autenticazione delle utenze amministrative.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	**Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.**	Su tutti i PC, portatili e server è installato un antivirus con aggiornamento automatico.
8	1	2	M	**Installare su tutti i dispositivi firewall ed IPS personali.**	Su tutti i PC, portatili e server Windows è attivato il firewall di Windows. Sui server Linux è installato ... *(ad es. Shorewall per*

					Iptables, ...)
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	**Il software di monitoraggio rileva tutti gli eventi sulle macchine e ne fa dei report, che vanno poi salvati in un archivio centralizzato ad accesso esclusivo dell'amministratore di sistema.**
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	**Gli amministratori di sistema, migrano tali strumenti a scadenza verso configurazioni centralizzate e ne hanno accesso esclusivo in configurazione.**
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	**L'amministratore, ove ritiene opportuno, può forzare manualmente l'aggiornamento dei sistemi anti-malware dalla macchina centralizzata. L'evento è automaticamente verificato e riportato al server (8.1.3).**
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	-
8	**3**	**1**	**M**	**Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.**	All'interno della rete non è consentito l'utilizzo di dispositivi esterni non autorizzati preventivamente dall'amministratore di sistema istruito sui necessari trattamenti.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	-
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data ExecutionPrevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	**L'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR.**
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	-
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	**L'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR.**
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	-
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	**L'amministratore di sistema deve configurare il Firewall per inserire gli indirizzi sospetti in blacklist e bloccarne l'accesso. Qualora l'Ente utilizzi service esterni deve fornire al provider la blacklist da bloccare.**

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

8	7	1	M	**Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	7	2	M	**Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	7	3	M	**Disattivare l'apertura automatica dei messaggi di posta elettronica.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	7	4	M	**Disattivare l'anteprima automatica dei contenuti dei file.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	8	1	M	**Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	9	1	M	**Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.**	L'Ente utilizza un servizio di posta elettronica esterno, che include il filtraggio richiesto.
8	9	2	M	**Filtrare il contenuto del traffico web.**	*Spesso l'antivirus include funzioni di filtraggio (contentfiltering). Altrimenti cambiare antivirus.* Sono state date disposizioni agli amministratori di sistema di configurare il software antivirus delle postazioni di lavoro in tal senso. *E' anche possibile utilizzare una soluzione centralizzata (proxy server: ad es. squid + DansGuardian)*
8	9	3	M	**Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).**	Sono state date disposizioni agli amministratori di sistema di configurare il software antivirus delle postazioni di lavoro in tal senso.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	**L'amministratore ha provveduto ad installare un sistema di antivirus che rileva le firme ma anche anomalie di comportamento.**
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	**L'antivirus adottato dall'amministratore invierà automaticamente degli alert al provider della sicurezza, che da remoto verificherà.**

ABSC 10 (CSC 10): COPIE DI SICUREZZA

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	**1**	**1**	**M**	**Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.**	*L'amministratore di sistema effettua copie di sicurezza che consentano il completo ripristino dei sistemi e le tiene aggiornate on change.*
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	-
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	-
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	**L'amministratore provvederà a verificare periodicamente l'utilizzabilità delle copie facendo dei ripristini di prova.**
10	**3**	**1**	**M**	**Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso il sistema di backup conservando le copie *in un luogo sicuro ad accesso controllato.*
10	**4**	**1**	**M**	**Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso il sistema di backup. *Una copia deve essere offline rispetto al sistema di backup.*

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	**1**	**1**	**M**	**Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica**	L'analisi dei livelli particolari di riservatezza è implementata attraverso la compartimentazione dei dati in cartelle il cui accesso è regolato da specifici criteri di accesso (ACL). L'Ente ha rilevato gli ambiti di riservatezza che richiedono crittografia dei dati che è stata realizzata crittografando il volume che contiene le relative cartelle:
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	**L'amministratore ha provveduto a configurare sistemi di cifratura per tutti i dispositivi che contengono informazioni rilevanti.**

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

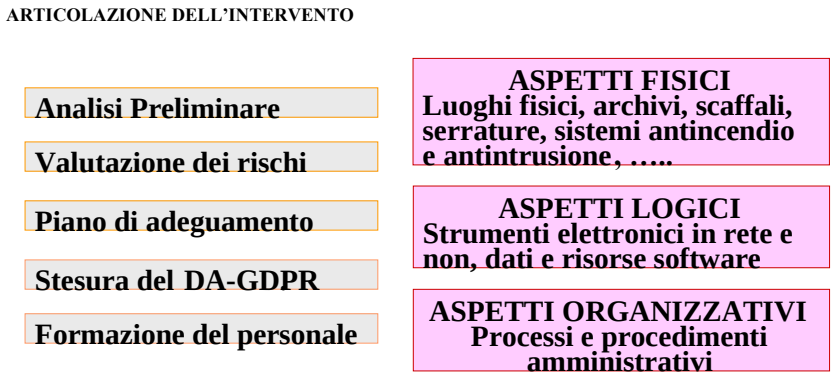
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	-
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	-
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	-
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	-
13	6	1	A	Implementare strumenti DLP (Data LossPrevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	-
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	-
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	-
13	**8**	**1**	**M**	**Bloccare il traffico da e verso url presenti in una blacklist.**	Vedi misura 8.9.2
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	

Consorzio Sannio.it
Viale degli Atlantici c/o ex Caserma Guidoni - 82100 Benevento
Tel. 0824 312780 fax 0824 351993 - info@cstsannio.it

5 PIANO DI SVILUPPO DELL'INTERVENTO DI ADEGUAMENTO AL GDPR 679/2016

5.1 ARTICOLAZIONE DELL'INTERVENTO

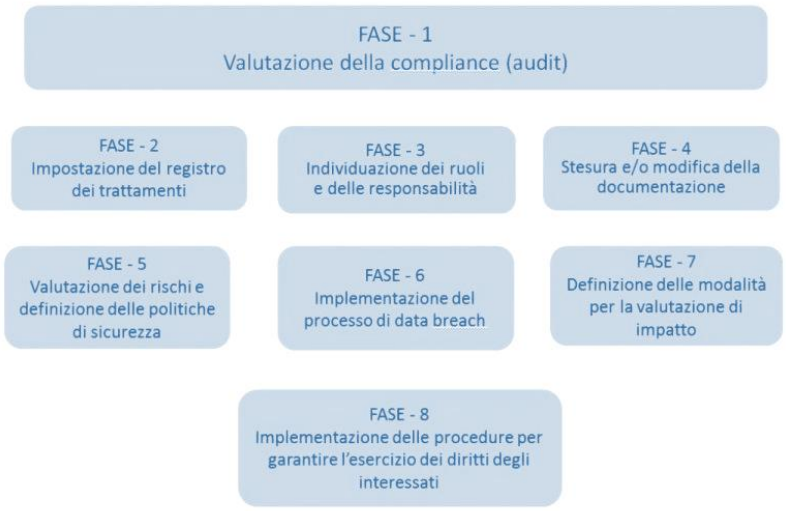
L'intervento è stato realizzato mediante una serie di attività che hanno interessato tutti i settori dell'Ente nella sua interezza. Nella figura seguente vengono schematizzate le fasi in cui si è articolato l'intervento:



Nel dettaglio, le attività svolte dal CST Consorzio Sannio.it nell'ambito dell'incarico di prestazione del servizio RPD conferito dall'Ente, sono le seguenti:

- designazione del CST Consorzio Sannio.it nella qualità di RPD per il periodo di almeno due anni con referente nella persona dell'ing. Carmine Basco;
- supporto e assistenza alla mappatura dei processi, per individuare quelli collegati al trattamento dei dati personali;
- individuazione, tra i processi risultanti dalla mappatura, di quelli che presentano rischi, con una prima valutazione degli stessi i termini di maggiore o minore gravità
- supporto e assistenza alla mappatura degli incarichi dei soggetti coinvolti nel trattamento e dei livelli di responsabilità, ed eventuale aggiornamento
- elaborazione del piano di adeguamento complessivo, contenente le proposte di miglioramento del livello di sicurezza per i processi che presentano rischi, con stima dei costi (se necessario) e dei tempi previsti, nonché delle attività di monitoraggio;
- interventi formativi del personale
- predisposizione del registro dei trattamenti di dati personali e del registro delle categorie di attività
- proposta di adeguamento della modulistica e contrattualistica in uso agli uffici, qualora non conforme alle nuove disposizioni
- eventuale valutazione di impatto sulla protezione dei dati nei casi previsti dalla normativa.

Tutte le attività descritte possono essere raggruppate per macro-fasi e rappresentate graficamente nel diagramma sotto riportato:



5.2 CONTENUTI E TEMPISTICA

5.2.1 NOMINA DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)

La nomina a RPD presso il Comune di Airola avrà decorrenza dalla data di conferimento dell'incarico e durata biennale.
Nell'ambito dell'incarico ricevuto di Responsabile della Protezione dei Dati, saranno svolti i seguenti compiti:

- informare e fornire consulenza al Titolare ed al Responsabile nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. Ai fini del presente compito il RPD indicherà al Titolare e/o al Responsabile i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
- sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento. Faranno parte di questi compiti: la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;
- sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;
- fornire parere in merito alla eventuale valutazione di impatto sulla protezione dei dati (DPIA),
- fornire gli opportuni suggerimenti per lo svolgimento delle attività nel modo più sicuro e meno impattante, sorvegliarne lo svolgimento;
- cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità;
- provvedere alla tenuta dei registri del Titolare e del/dei Responsabili sul trattamento.
- supportare il Titolare e i Responsabili del trattamento nell'individuare processi organizzativi idonei a contemperare le esigenze della gestione delle attività di competenza e le esigenze di tutela dei dati.

5.2.2 MAPPATURA DEI PROCESSI, INDIVIDUAZIONE DEI RISCHI E MAPPATURA DEGLI INCARICHI

L'attività di mappatura dei processi, degli incaricati e l'individuazione del livello di protezione o di rischio saranno il passo iniziale per definire la situazione di partenza e la strada da percorrere per raggiungere gli obiettivi previsti dal legislatore europeo.
Previa acquisizione e consultazione della documentazione adottata dall'Ente in adempimento al previgente D.Lgs 196/2003 "*Codice Privacy*", l'indagine sarà svolta in maniera accurata, settore per settore, sulla base di check list predisposte dal RPD incaricato; i dirigenti ed i responsabili dei singoli servizi, nonché gli addetti al Sistema Informativo Comunale, forniranno il supporto necessario, fornendo tutte le informazioni richieste, acquisendole a loro volta dai fornitori esterni, qualora non siano a disposizione dell'ente.
Le attività previste in questo paragrafo saranno concluse presumibilmente entro 30 giorni naturali e consecutivi dal conferimento dell'incarico.

5.2.3 ELABORAZIONE DEL PIANO DI ADEGUAMENTO

Il piano di adeguamento conterrà le proposte di miglioramento del livello di sicurezza per i processi che presentano rischi, con stima dei costi (se necessario) e dei tempi previsti, nonché delle attività di monitoraggio e le tempistiche.
Le misure tecniche ed organizzative di sicurezza che verranno messe all'attenzione del Titolare e che dovranno essere attivate per ridurre i rischi del trattamento ricomprenderanno: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
Costituiranno altresì misure tecniche ed organizzative i sistemi di autenticazione; i sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro); le misure antincendio; i sistemi di rilevazione di intrusione; i sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.
L'attività prevista nel presente paragrafo sarà presentata al responsabile del procedimento entro 30 giorni naturali e consecutivi dalla scadenza del termine di cui al punto precedente; entro i successivi 30 giorni naturali e consecutivi dovranno essere apportate, a cura dei Responsabili o dei Fornitori esterni, le eventuali modifiche ed integrazioni concordate, e consegnata la relazione definitiva.

5.2.4 INTERVENTI FORMATIVI DEL PERSONALE

Gli interventi formativi del personale prevedranno una formazione di base, da impartire a tutti i dipendenti, e una formazione specialistica per i dipendenti che svolgono attività classificate a rischio più elevato (ad es. personale addetto al Piano Sociale di Zona). Il piano di formazione sarà presentato in contemporanea al piano di adeguamento di cui al punto 2.3 e sarà programmato in modo da fare fronte alle carenze riscontrate nell'ambito della mappatura. Il calendario e le modalità di articolazione della formazione saranno concordati con il Titolare del trattamento o suo delegato, e/o, in caso di formazione riguardante specifici settori, con il dirigente competente.

5.2.5 PREDISPOSIZIONE E TENUTA DEL REGISTRO UNICO DEI TRATTAMENTI DI DATI PERSONALI

Il Registro unico delle attività di trattamento prevedrà almeno le seguenti informazioni:
- il nome ed i dati di contatto del Comune, eventualmente del Contitolare del trattamento, del RPD;
- le finalità del trattamento;
- le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione;
- la sintetica descrizione delle categorie di interessati (cittadini, residenti, utenti, dipendenti, amministratori, parti, altro), nonché le categorie di dati personali (dati identificativi, dati genetici, dati biometrici, dati relativi alla salute);
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati: persona fisica o giuridica; autorità pubblica; altro organismo destinatario;
- l'eventuale trasferimento di dati personali verso un paese terzo od organizzazione internazionale;
- ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

La predisposizione del registro sarà curata dal RPD non appena conclusa la fase di mappatura prevista al punto 7.2.2.

La tenuta e l'aggiornamento del registro sarà curata dal RPD che provvederà tempestivamente in tal senso con cadenza, se del caso, almeno semestrale. Il registro sarà sottoposto al controllo ed alla vidimazione del titolare del trattamento o suo delegato e dei dirigenti dei servizi competenti.

5.2.6 PROPOSTA DI ADEGUAMENTO DELLA MODULISTICA E DELLA CONTRATTUALISTICA IN USO AGLI UFFICI, QUALORA NON CONFORME ALLE NUOVE DISPOSIZIONI

La proposta di adeguamento della modulistica e contrattualistica in uso agli uffici, se non conforme alle nuove disposizioni, sarà completata entro tre mesi dalla data di scadenza dei termini per la mappatura di cui al punto 7.2.2.

Con la stessa tempistica saranno altresì effettuate le seguenti attività di supporto:
- per l'elaborazione della modulistica interna ed esterna (informative e consenso);
- per l'elaborazione nuovo regolamento per la protezione dei dati personali (in riferimento alla bozza proposta dall'ANCI);
- per l'elaborazione dei documenti di nomina dei soggetti delegati interni;
- per l'elaborazione dei documenti di nomina dei soggetti autorizzati al trattamento;
- per la revisione delle clausole contrattuali con i responsabili esterni del trattamento;
- per l'elaborazione del modello di esercizio dei diritti dell'interessato;

5.2.7 ISTITUZIONE DEL REGISTRO DELLE VIOLAZIONI DELLA SICUREZZA (DATA BREACH) E PRESA IN CARICO DELLE EVENTUALI RELATIVE NOTIFICAZIONI/COMUNICAZIONI (GARANTE/INTERESSATI)

Presso l'Ente è stato istituito il registro delle violazioni della sicurezza (data breach) e della presa in carico delle eventuali relative notificazioni sia verso il garante sia verso l'interessato. Il modello di registro adottato viene riportato nella figura sottostante:

Evento				Conseguenze	Provvedimenti adottati	Notifica all'autorità di		Comunicazione all'interessato	
Codice4	Irrilevante	Falso Positivo	Rilevante			SI/NO	Data	SI/NO	Data

Di seguito si riporta il modello della scheda evento adottato dall'Ente:

SCHEDA EVENTO	
CODICE	
Data evento e ora della violazione anche solo presunta (specificando se è presunta);	
Data e ora in cui si è avuto conoscenza della violazione;	
Fonte di segnalazione	
Tipologia evento anomalo	
Descrizione evento anomalo	
Numero interessati coinvolti	
Numerosità dei dati personali di cui si presume la violazione	
Data, anche presunta, della violazione e del momento in cui se ne è avuta conoscenza	
Luogo in cui è avvenuta la violazione dei dati (specificare se è avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)	

Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	

Di seguito si riporta il modello della scheda violazione dati adottato dall'Ente:

SCHEDA VIOLAZIONE DATI		
CODICE EVENTO[1]	**CLASSIFICAZIONE[2]**	**RISCHIO[3]**

[1] Inserire il CODICE della scheda evento

[2] Classificazione dell'evento tra i seguenti casi:

- distruzione di dati illecita,
- perdita di dati illecita,
- modifica di dati illecita,
- distruzione di dati accidentale,
- perdita di dati accidentale,
- modifica di dati accidentale,
- divulgazione non autorizzata
- accesso ai dati personali illecito.

[3] Valutazione del rischio secondo i seguenti livelli di rischio:

- NULLO
- BASSO
- MEDIO
- ALTO

DEFINIZIONE DI VIOLAZIONE DI DATI PERSONALI (DATA BREACH) E DEI DANNI CONSEGUENTI

Ai sensi dell'art. 4, comma 12, del Regolamento UE n. 679/2016 (di seguito: "Regolamento") per violazione di dati personali (*data breach*) si intende "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso di dati personali trasmessi, conservati o comunque trattati". Ai sensi del considerando 85 del Regolamento una violazione di dati personali può "provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo di dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata".

IPOTESI DI DATA BREACH PREVISTE DAL REGOLAMENTO

Il Regolamento 679/2016 si occupa di *data breach* in due specifiche ipotesi di carattere generale:

- la notifica all'autorità di controllo ai sensi dell'art. 33; e
- la comunicazione all'interessato ai sensi dell'art. 34.

SOGGETTO OBBLIGATO E RELATIVI COMPITI PER GARANTIRE LA SICUREZZA DEI DATI

L'obbligo della notifica/comunicazione di un *data breach* incombe esclusivamente sul titolare (artt. 33 e 34 del Regolamento), che sarà tenuto a valutare i rischi inerenti il trattamento ed attuare le misure di sicurezza tecniche ed organizzative adeguate per evitare (o ridurre al minimo) il rischio di violazione dei dati, quali ad es. la cifratura e la pseudonimizzazione (considerando 83 e art. 32 del Regolamento). Il livello di sicurezza è, pertanto, adeguato quando è in grado di contrastare i rischi (accidentali o illeciti) di distruzione, perdita, modifica, divulgazione o accesso a dati personali.

CONOSCENZA DELLA VIOLAZIONE

Presupposto per procedere alla notifica ex art. 33 è la conoscenza da parte del titolare della violazione. Potrebbe essere a conoscenza della violazione il responsabile (anziché direttamente il titolare), che informerà il titolare di conseguenza.

AUTORITÀ DI CONTROLLO COMPETENTE

Per individuare il Garante competente a cui vada effettuata la notifica occorre fare riferimento allo Stato membro in cui si trovi lo stabilimento del titolare interessato dalla violazione o i cui interessati siano riguardati dalla violazione (ai sensi del combinato disposto degli artt. 5 e 55 del Regolamento e del considerando 122) e non all'autorità capofila ai sensi dell'art. 56, norma quest'ultima che non è richiamata, a differenza dell'art. 55, dalla disposizione dell'art. 33. Osservazioni: verificare con il Garante se si è di fronte, come pare, ad un caso di inapplicabilità della regola dello sportello unico (autorità capofila).

TERMINI E MODALITÀ PER LA NOTIFICA/COMUNICAZIONE

Il titolare effettua la notifica al Garante competente "senza giustificato ritardo" e, ove possibile, entro 72 ore dal momento in cui è venuto a conoscenza della violazione. Superate le 72 ore, il titolare deve motivare il ritardo (cfr. art. 33 del Regolamento). Il responsabile deve informare del *data breach* il titolare "senza ingiustificato ritardo" (art. 33, par. 2, del Regolamento). Quanto alla comunicazione all'interessato, la norma di cui all'art. 34 non specifica un termine in quanto stabilisce che il titolare comunichi "senza ingiustificato ritardo".
Non sono previste formalità e modalità per la notificazione/comunicazione.

OBBLIGHI DI DOCUMENTAZIONE

Ai sensi dell'art. 33, par. 5, del Regolamento il titolare è obbligato a documentare qualsiasi violazione dei dati, le circostanze, le conseguenze e i provvedimenti adottati per rimediarvi. Tale documentazione è messa a disposizione del Garante e consente di verificare il rispetto delle norme regolamentari.

CONTENUTO OBBLIGATORIO DELLA NOTIFICA

La notifica al Garante della violazione ex art. 33 del Regolamento deve contenere almeno le seguenti informazioni:

a) la descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati in questione;
b) la comunicazione del nome e dei dati di contatto del RPD o di altro punto di contatto presso cui ottenere più informazioni;
c) la descrizione delle probabili conseguenze della violazione;
d) la descrizione delle misure adottate o da adottarsi per rimediare alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

CONTENUTO OBBLIGATORIO DELLA COMUNICAZIONE

La comunicazione all'interessato ex art. 34 del Regolamento deve contenere almeno le informazioni di cui alle precedenti lettere b), c) e d), deve descrivere "con un linguaggio semplice e chiaro" la natura della violazione dei dati e formulare raccomandazioni agli interessati per attenuare gli effetti negativi della violazione (considerando 86 del Regolamento).

CASI DI ESONERO DALLA NOTIFICA

Il primo paragrafo dell'art. 33 del Regolamento prevede che il titolare notifichi la violazione al Garante competente: "senza giustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le liberà delle persone fisiche". Non è chiaro se la deroga summenzionata (improbabilità di rischi per i

diritti/libertà personali) si applichi in via generale, comportando un'esclusione dall'obbligo di notifica tout court; oppure, se si tratti di ipotesi che esoneri il titolare esclusivamente dall'effettuare una notifica tempestiva entro le 72 ore.

CASI DI ESONERO DALLA COMUNICAZIONE

Non è richiesta la comunicazione all'interessato ex art. 34 del Regolamento se è soddisfatta una delle seguenti condizioni:

a) il titolare ha messo in atto le misure tecniche ed organizzative adeguate di protezione e tali misure sono state applicate ai dati violati (ad es.: la cifratura);
b) il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c) la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede ad una comunicazione pubblica o ad una misura similare per informare gli interessati.

DATA BREACH GIÀ PREVISTI DALL'ORDINAMENTO ITALIANO

Già prima del Regolamento, nel nostro ordinamento sono state disciplinate alcune ipotesi specifiche di obbligo di notifica al Garante di data breach, utilizzando dei modelli predisposti da quest'ultimo. I provvedimenti relativi emanati dal Garante riguardano, in particolare, le società telefoniche e gli Internet provider, la biometria, il dossier sanitario elettronico e le amministrazioni pubbliche.

SANZIONI

La violazione degli obblighi di cui agli artt. 33 e 34 del Regolamento è punita con la sanzione amministrativa pecuniaria fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (cfr. art. 83, paragrafo 4, lettera a), del Regolamento).

5.2.8 VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, su segnalazione del Responsabile del trattamento, prima di effettuare il trattamento, dovrà effettuare una valutazione dell'impatto del medesimo trattamento ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.
Il Titolare si avvarrà della consulenza tecnica del RPD, il quale fornirà i seguenti elementi, entro 15 giorni dalla richiesta:

- descrizione del trattamento, valutazione della necessità e proporzionalità, individuazione delle migliori modalità di gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali che permettano di realizzare e dimostrare la conformità alle norme del trattamento di che trattasi.

5.3 ANALISI PRELIMINARE

Dato il forte impatto trasversale che hanno gli adempimenti previsti dal GDPR, si è ritenuto indispensabile procedere ad una azione di rilevazione e monitoraggio delle attività di trattamento svolte in ogni settore, al fine di avere un quadro generale e di verificare la compatibilità della situazione reale con le previsioni normative.

In questa fase è stata svolta l'analisi dell'organizzazione della struttura dell'Ente attraverso la rilevazione dettagliata dei luoghi fisici, dell'infrastruttura telematica, delle postazioni di lavoro, delle applicazioni software e delle banche dati utilizzate.

La fase è stata esplicata nelle seguenti attività:

- rilevazione dei luoghi fisici afferenti all'Ente dove avvengono i trattamenti e dove vengono conservati gli archivi cartacei correnti e storici;
- rilevazione dell'infrastruttura Hw, Sw di base e di telecomunicazione;
- rilevazione delle applicazioni Sw utilizzate per il trattamento dei dati personali;
- rilevazione della struttura organizzativa;
- censimento dei trattamenti di dati personali.

Ci sono tre ordini di benefici, che scaturiscono da questa attività di rilevazione e monitoraggio iniziale:

- la possibilità di avere sempre sotto controllo, nei limiti del possibile, il processo di trattamento, potendo sempre dare risposte adeguate, a seconda dei casi, all'interessato, che eserciti i diritti che la legge gli riconosce, e al Garante, che disponga controlli e ispezioni, esercitando i poteri che la legge gli assegna;
- cogliere il valore aggiunto della legge in termini di organizzazione e di verifica dei flussi informativi interni all'ente e da questo verso l'esterno: può essere l'occasione per verificare eventuali colli di bottiglia, ridondanze, ecc;
- infine, ma non per importanza, questa attività, coinvolgente tutta la struttura, serve a dare consapevolezza e a far nascere e consolidare una cultura della sicurezza in senso generale e del rispetto della riservatezza degli interessati e quindi a perseguire un miglioramento dei rapporti con la propria utenza.

Nei paragrafi successivi vengono descritte le attività svolte in ogni fase.

5.3.1 RILEVAZIONE DEI LUOGHI FISICI AFFERENTI ALL'ENTE

In questa fase sono stati rilevati tutti gli ambienti relativi alle sedi del Comune di Airola. Sono stati rilevati gli strumenti elettronici in esse presenti ed eventuali dispositivi per la messa in comunicazione della rete dati.

5.3.2 RILEVAZIONE DELL'INFRASTRUTTURA HW, SW DI BASE E DI TELECOMUNICAZIONE

E' stato effettuato il censimento delle risorse hardware (workstation client e server) presenti nell'edificio che ospita le applicazioni software e le banche dati fruite dai diversi settori dell'Ente.

La rilevazione ha riguardato tutte quelle caratteristiche e quegli aspetti che potessero evidenziare il livello di sicurezza già attuato dal Comune di Airola e scoprire misure non adottate per contrastare eventuali tentativi di intrusione o danneggiamento dei sistemi.

5.3.3 RILEVAZIONE DELLE APPLICAZIONI SW UTILIZZATE PER IL TRATTAMENTO DEI DATI PERSONALI

Attraverso le interviste con i responsabili di settore/servizio è stato possibile rilevare il disegno logico delle applicazioni software distribuite sull'intera infrastruttura di comunicazione e per ciascuna di esse è stata effettuata una attenta rilevazione delle caratteristiche logiche ed architetturali; ambiente di sviluppo, data base, modalità di comunicazione, sistema di autenticazione e di autorizzazione, criteri di back up adottati. In sintesi, è stata verificata, per ciascuna applicazione, la rispondenza delle funzionalità in essere rispetto ai requisiti previsti dal codice della privacy.

5.3.4 RILEVAZIONE DELLA STRUTTURA ORGANIZZATIVA

Sono state rilevate tutte le informazioni inerenti l'organizzazione dell'Ente, nominativi e mansioni degli incaricati al trattamento dati.

5.4 VALUTAZIONE DEI RISCHI

A partire dalla definizione di una serie di eventi potenzialmente dannosi è stata redatta l'analisi dei rischi incombenti sui dati, evidenziando la loro gravità in funzione del contesto riscontrato: fisico, logico, organizzativo.

L'analisi condotta ha evidenziato all'interno dell'Ente, le seguenti criticità:

- presenza sul territorio comunale di un sistema di videosorveglianza costituito da 32 telecamere in fase di ultimazione e test;
- i cartelli contenenti le informative non sono al momento conformi al provvedimento del Garante anno 2010 in materia di videosorveglianza, ma si prevede in tempi brevi una loro sostituzione;
- la regolamentazione del servizio di videosorveglianza e individuazione dei responsabili dello stesso è in fase di implementazione;
- la centrale per la visualizzazione e memorizzazione delle immagini di ripresa è allocata al piano terra in una stanza adibita ad ufficio dei Vigili Urbani e consente la visualizzazione su un monitor delle immagini in tempo reale;
- utilizzo di tre personal computer dotati di sistema operativo obsoleto (WinXp) non più supportato dal produttore in termini di aggiornamento della patch di sicurezza;

5.5 FORMAZIONE DEL PERSONALE

In questa fase vengono tenute attività specifiche di formazione ed informazione per i responsabili e per gli incaricati del trattamento dei dati.

In data 12/06/2018, presso la sede della Casa Comunale, si è provveduto a tenere una sessione formativa/informativa finalizzata ad istruire il personale dell'Ente sui diversi aspetti introdotti dal nuovo regolamento sulla privacy. Il corso formativo è stato erogato dal RPD. Si riporta di seguito il registro delle presenze:

Comune di Airola

12 Giugno 2018

Incontro informativo/formativocon il Responsabile della Protezione dei Dati dell'Ente - Istruzioni ai dipendenti

Regolamento Europeo in materia di protezione dei datipersonali 679/2016

	COGNOME E NOME	UFFICIO	RUOLO	FIRMA
1	ARAGOSA Pasquale	LL.PP.-PATRIMONIO	Responsabile	
2	SCHETTINI-VINCENZO	EDILIZIA - ECOLOGIA AMBIENTE E SICUREZZA	RESPONSABILE	
3	Mosca Carlo	Segretario Comunale		
4	Maiella Pietro	Sindaco	Vice Sindaco delegato	
5	DI SILVESTRO ANNA MARIA	SS - AA	RESPONSABILE	
6	IADEVAIA GIUSEPPE	SEGRETERIA - AA GENERALI - P.ISTRUZIONE - FINANZE BIL. CONTABILITA'	RESPONSABILE	
7	Esposito Pietro	MANUTENZIONE - PROTEZIONE CIVILE	ISTRUTTORE TECNICO	
8	Talentano Anna	MANUTENZIONE PROTEZIONE CIVILE	ISTRUTTRICE AMM.	
9	CAROLINA DE CARLO	UFFICIO S.G. /URP	ISTRUTTORE AMM	
10	Carmela Alessandra Merola	Ecologia	ISTRUTT. AMM.	
11	AFFINITO PASQUALINA	TRIBUTI	ISTRUTTORA AMM.	

La prima fase dell'attività formativa svolta presso l'Ente ha interessato i seguenti aspetti connessi al nuovo regolamento GDPR volti sostanzialmente a sensibilizzare il personale tutto sui temi di maggiore interesse della nuova normativa europea:

- Presentazione della nuova normativa europea n°679/2016;
- Protezione dei dati e diritti degli interessati;
- Il principio di responsabilità (accountability);
- Il Garante della privacy;
- Sanzioni;
- Formazione;
- Applicabilità del GDPR nel settore pubblico;
- Azioni prioritarie per la PA;
- Il Responsabile della protezione dei dati (RPD);
- Il registro delle attività di trattamento;
- La valutazione di impatto privacy (DPIA);
- Case study su incidenti informatici;

- Violazione dei dati personali;
- Il “Data breach”: rilevazione, valutazione, notifica al Garante e al Cert-PA;
- Trasparenza, pubblicità legale, diritto di accesso
- Il CAD e il Piano triennale per l’informatica nella PA
- Buone pratiche ed esempi di applicazione.

Sono previste eventuali ulteriori sessioni formative sulla base della valutazione di particolari esigenze manifestate dal Titolare e/o dal personale dell’Ente in relazione all’implementazione/monitoraggio delle misure di sicurezza e/o variazioni/ integrazioni della vigente normativa in materia di protezione dei dati personali.

A sostegno e supporto delle attività di formazione e informazione, il RPD ha reso disponibile:

- il manuale *“Disposizioni per il trattamento dei dati personali – Istruzioni e misure organizzative e tecniche”* avente l’obiettivo di informare, in ordine all’ambito di applicazione, le modalità e le norme sul trattamento dei dati personali da parte dei dipendenti dell’Ente ed in generale dei soggetti preposti, al fine di tutelare i beni dell’ente stesso ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre il Comune a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi;
- un’area accessibile dalla rete locale all’indirizzo:
  192.168.0.252\GDPR
  contenente documenti, informative, pubblicazioni, modelli, regolamenti, ecc. inerenti i vari ambiti applicativi in materia di protezione dei dati personali e della sicurezza ICT. Tali materiali, in continuo aggiornamento da parte del RPD, si intendono a supporto ed integrazione dell’attività formativa ed informativa del personale.

6 LA SEDE DEL COMUNE DI Airola

Il Comune di Airola è dislocato in una unica sede ubicata in Via Municipio, 1.

La sede del Comune impegna la totalità dell’edificio collocato al centro del paese lungo la strada principale.

Tutti gli uffici comunali sono collocati sia al piano terra che al primo piano e al piano. Al piano terra sono dislocati gli uffici della Polizia Municipale del Messo e la Sala Consiliare. E mediante un corridoi interno si accede alla sala server del sistema di videosorveglianza.

Al primo piano si accede tramite un’ampia scala che smonta al primo piano su un pianerottolo. Da questo si accede ad un corridoio che percorre quasi tutto il perimetro interno dell’edificio. Su questo corridoio sono situati gli accessi agli uffici. Percorrendo il corridoio verso dx vi sono: l’ufficio tributi, l’ufficio ecologia, l’ufficio protocollo, l’ufficio manutenzione, l’ufficio anagrafe, l’ufficio elettorale edilizia privata e proseguendo sulla dx troviamo la stanza del Sindaco, l’ufficio del Segretario generale , l’ufficio amministrativo, l’ufficio affari generali. Mentre proseguente verso sx troviamo i due uffici del servizio Ragioneria, l’ufficio urp e la sala giunta.

Al piano rialzato si accede mediante una scala che si trova alla sx del corridoio e della sala giunta. Al piano rialzato si trovano l’ufficio lavori pubblici e l’ufficio assetto del territorio.

L’ufficio situato in fondo al corridoio di fronte all’ufficio del Segretario Comunale si trova la sala server con un armadio rack chiuso a chiave contenente le apparecchiature attive di rete dati e comunicazione, il firewall fisico, due server e l’apparecchiatura UPS.

L’archivio storico comunale al primo pianerottolo della scala che porta al piano rialzato in posizione centrale dietro al vano scala.

Tutte le aree sono ben delimitate e l’accesso alle stesse è ben organizzato anche da una regolamentazione oraria per l’accesso del pubblico agli uffici. Vi è un’unica apparecchiatura fax l’Ufficio Amministrativo. Le fotocopiatrici e stampanti sono situati nei vari uffici ad accesso esclusivo del personale comunale.

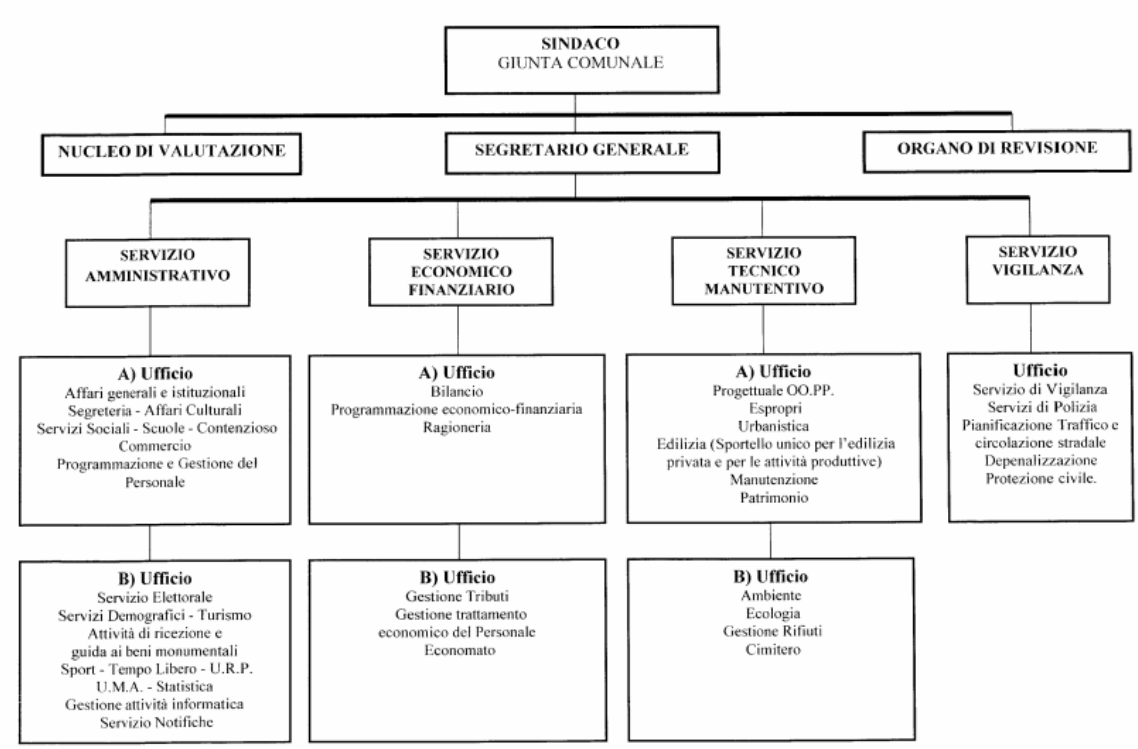
Le chiavi dell’archivio sono affidate al servizio amministrativo.

Tutti gli infissi interni sono dotati di idonea serratura di sicurezza a cilindro europeo. Tutti gli infissi esterni sono dotati di ordinaria protezione. Gli elementi di arredo sono dotati per la maggior parte di serrature funzionanti.

7 DISTRIBUZIONE DI COMPITI E RESPONSABILITA’

Si riporta nella tabella seguente l’organigramma di tutti i soggetti dell’Ente che nell’ambito organizzativo provvedono al trattamento dei dati stessi, con una descrizione di ruoli, mansioni e responsabilità.

Titolare del trattamento: Comune di Airola – Provincia di Benevento
Legale Rappresentante p. t.: ***Sindaco MICHELE NAPOLETANO***
Segretario Comunale: ***Dott.ssa. CARLA MOSCATO***



8 ELENCO DEI TRATTAMENTI DEI DATI PERSONALI

Il censimento dei Processi e delle macro attività e delle relative attività di trattamento sono elencati nell'allegato Registro Unico, redatto ai sensi del regolamento comunale e dell'art. 30, c.1 e 2 del GPRD. Il Registro delle attività di trattamento viene sottoposto a revisione periodica (trimestrale) e tempestivamente qualora dovesse verificarsi una variazione ad un trattamento già censito.

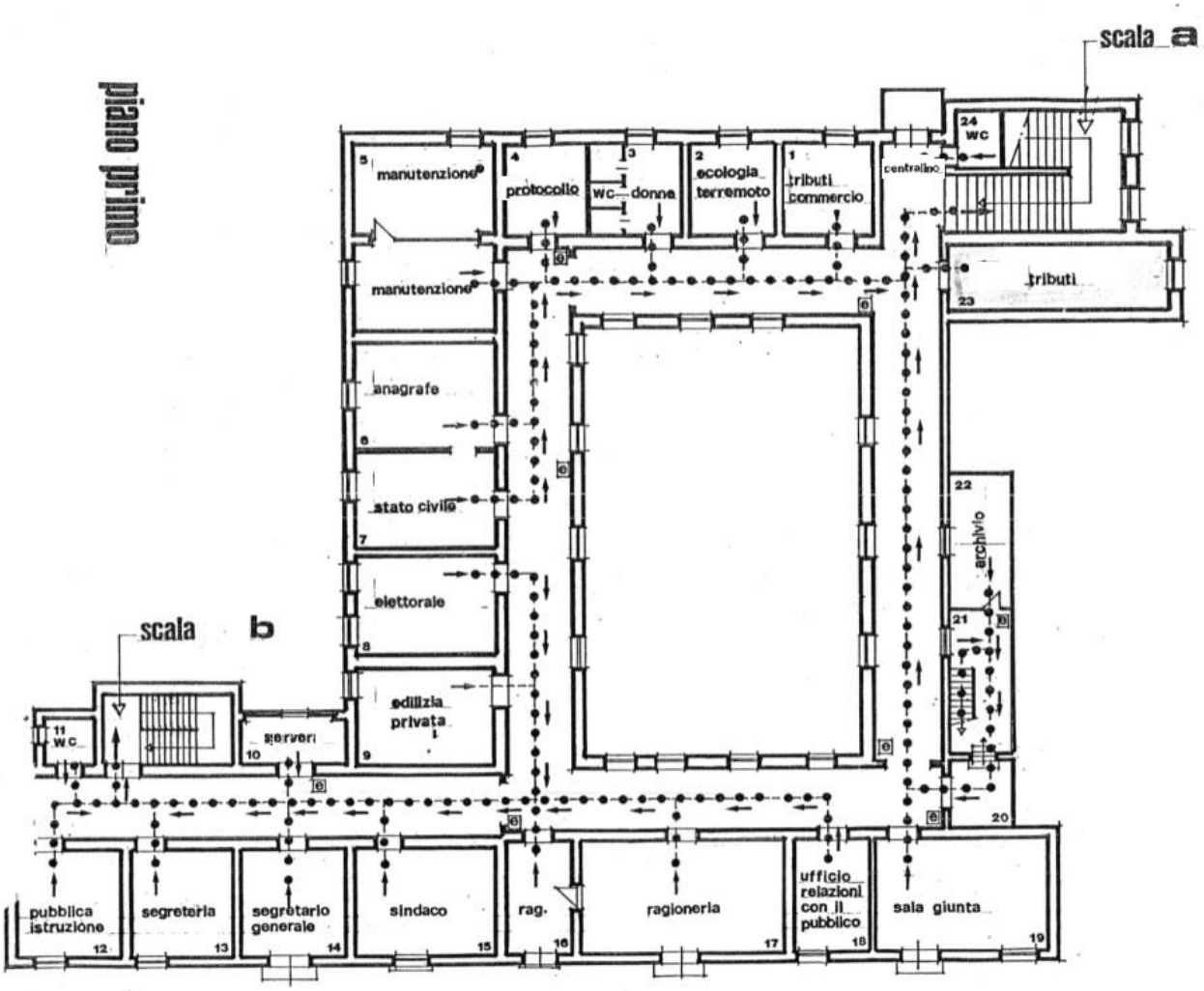
9 IL SISTEMA INFORMATIVO E L'INFRASTRUTTURA DI TELECOMUNICAZIONE

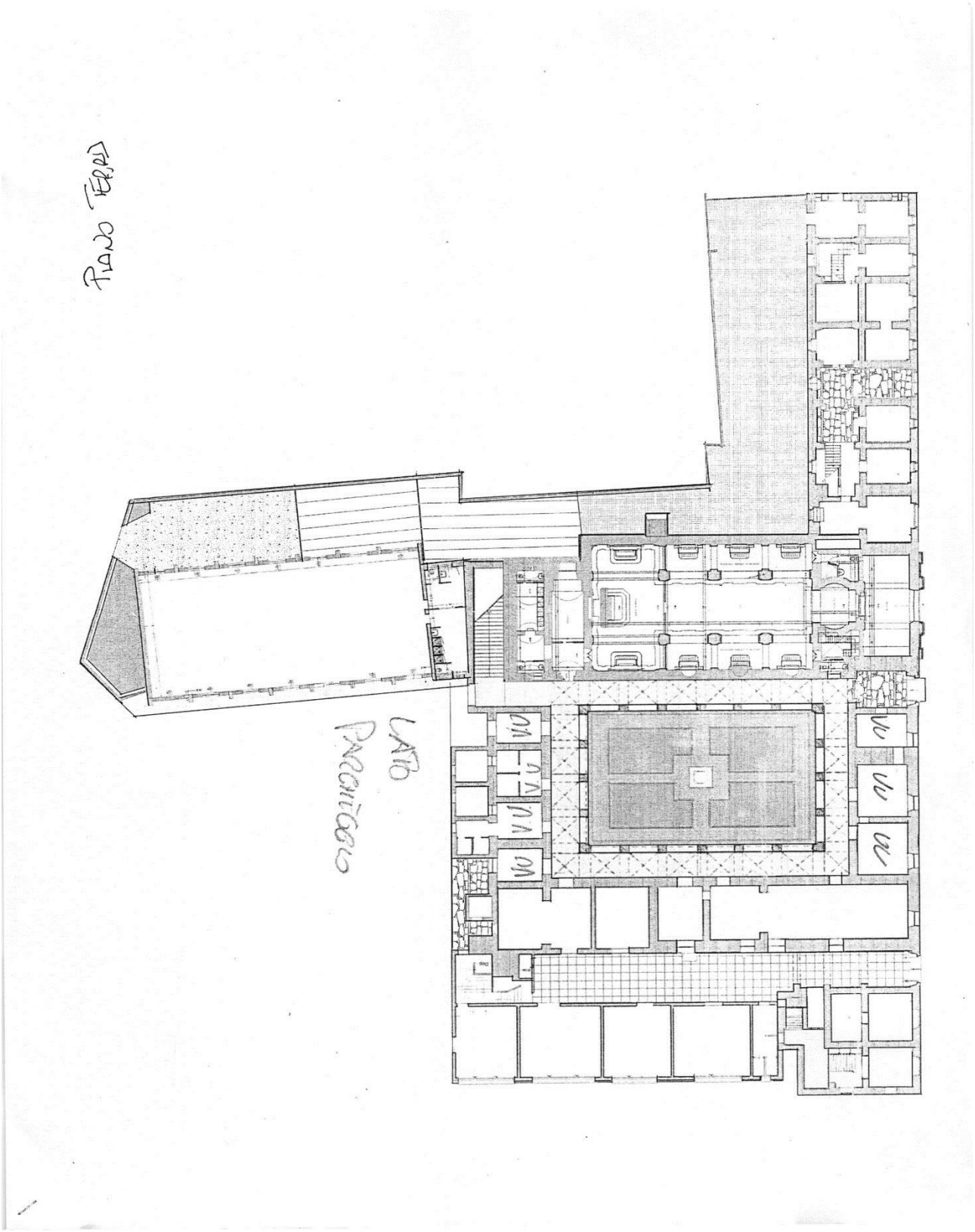
Il sistema informativo è composto da una sala server da cui parte tutto il cablaggio sia della rete LAN che della rete Telefonica ed è così suddivisa:

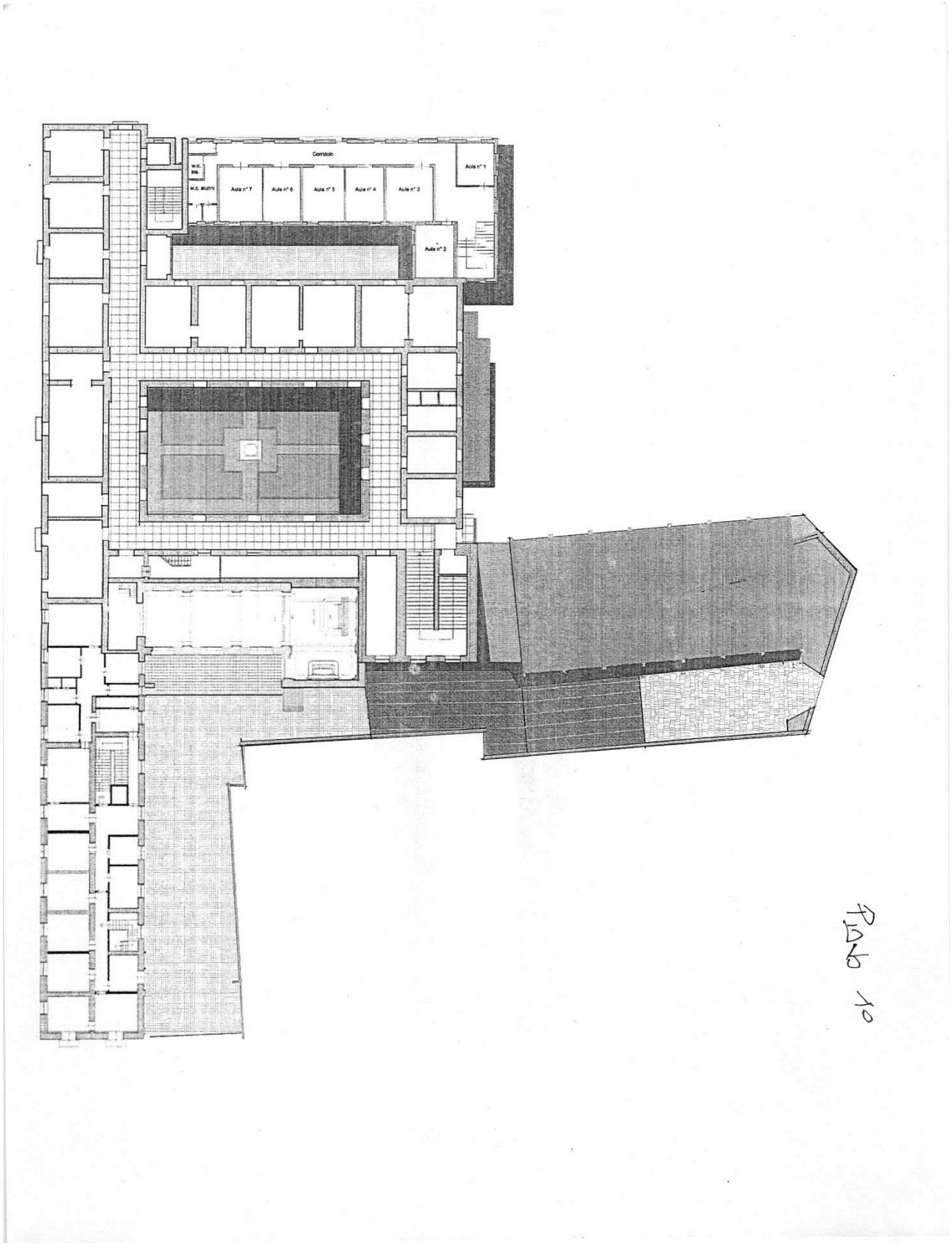
- Ufficio Tributi: 5 punti rete lan e 3 punti telefonici;
- Ufficio Tributi e commercio: 3 punti rete lan e 2 punti telefonici;
- Ufficio Ecologia: 2 punti rete lan e 2 punti telefonici;
- Ufficio Protocollo: 2 punti rete lan e 2 punti telefonici;
- Ufficio Manutenzione: 5 punti rete lan e 4 punti telefonici;
- Ufficio Anagrafe: 7 punti rete lan e 3 punti telefonici;
- Ufficio Elettorale: 2 punti rete lan e 2 punti telefonici;
- Ufficio Edilizia Privata: 5 punti rete lan e 3 punti telefonici;
- Ufficio Pubblica Istruzione: 2 punti rete lan e 2 punti telefonici;
- Ufficio Segreteria: 3 punti rete lan e 3 punti telefonici;
- Ufficio Segretario Generale: 1 punti rete lan e 2 punti telefonici;
- Ufficio Sindaco: 1 punto rete lan e 2 punti telefonici;
- Ufficio Ragioneria: 7 punti rete lan e 5 punti telefonici;
- Ufficio Urp e Assistente Sociale: 2 punti rete lan e 2 punti telefonici;
- Sala Giunta: 1 punto rete

- Ufficio Lavori Pubblici: 4 punti rete lan e 3 punti telefonici;
- Ufficio Assetto del Territorio: 1 punto rete lan e 1 punto telefonico;
- Ufficio Messo: 2 punti rete lan e 2 punti telefonici;
- Ufficio Polizia Municipale: 5 punti rete lan e 3 punti telefonici;
- Sala Consiliare: 1 punto rete e 1 punto telefonico

10 PLANIMETRIE DEI LOCALI




Piano Terra
LABO
Radiologico


Corridoio
Aula n° 1
Aula n° 2
Aula n° 3
Aula n° 4
Aula n° 5
Aula n° 6
Aula n° 7