# Unione dei Comuni Gallura

# GDPR

## PIANO DI SICUREZZA INFORMATICA

# INDICE

# 1. FINALITÀ E SINTESI DELLA NORMATIVA

## 1.1. Premessa

Il presente Piano viene redatto ispirandosi al Documento Programmatico per la Sicurezza (DPS), così come modificato a seguito dell'adozione del D.L. 9 febbraio 2012, n. 5, convertito nella L. 4 aprile 2012, n. 35. Detto DPS costituisce tuttora valido strumento di documentazione delle politiche interne adottate in materia di privacy, nonchè atto propedeutico e di ausilio all'applicazione del "Regolamento Europeo" del 27 aprile 2016 (di seguito definito **GDPR** o **Regolamento**) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Tra le disposizioni normative afferenti la materia relativa alla protezione dei dati personali si rinvengono, inoltre:

- Linee Guida e altra documentazione pubblicata dal Gruppo dei Garanti dell'Unione Europea (cd. "WP29") ex articolo 29 della direttiva 95/46;
- Decreto legislativo 30 giugno 2003, n. 196 - Codice per la protezione dei dati personali, come modificato dal Decreto Legislativo 10 agosto 2018, n. 101 (di seguito definito **Codice);**
- Decreto Legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento Europeo", pubblicato in G.U. il 4 settembre 2018;
- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema, emanate dall'Autorità Garante Privacy il 27 novembre 2008, modificate in base al provvedimento del 25 giugno 2009, ove applicabili.

## 1.2. Finalità e ambito di applicazione della normativa

La normativa sulla protezione dei dati personali ha la finalità di **limitare i rischi per i cittadini europei** permettendo e facilitando **una libera circolazione dei loro dati personali**.

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare (GDPR considerando 75):

- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli

interessi personali, l’affidabilità o il comportamento, l’ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;

- se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

La normativa italiana ed europea 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 ed in particolare:

- al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione;
- al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare;
- al trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
- l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure,
- il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione;
- al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale.

### 1.3. Definizioni sui trattamenti

Ai fini del GDPR s'intende per:

- «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;
- «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;
- «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- «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;
- «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;
- «trattamento transfrontaliero»:
  - a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure,
  - b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.

### 1.4. Il GDPR in sintesi

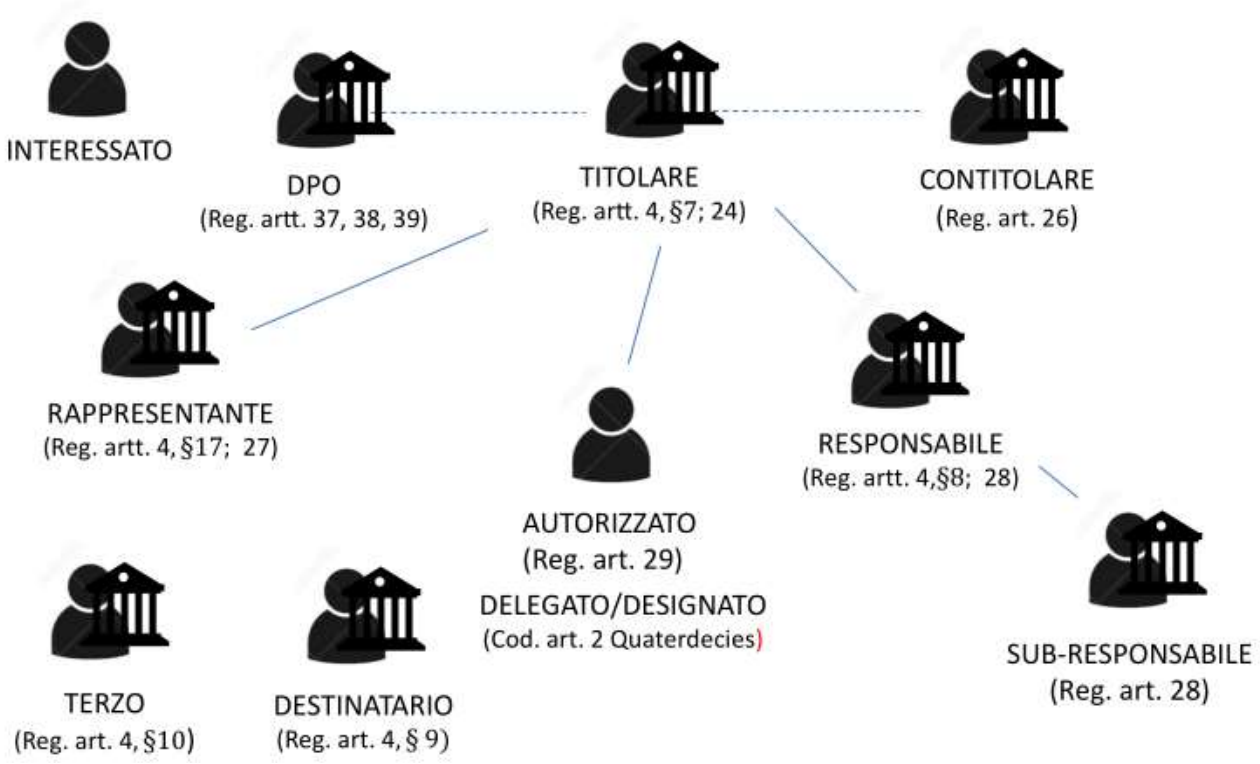
Il GDPR è logicamente molto più semplice di quello che può apparire, esso si fonda principalmente su tre articoli basilari ovvero: artt. 24, 32 e 5 e a livello di astrazione possiamo rappresentarlo con tre perimetri:

1. l’articolo 32 (rischio per gli interessati al trattamento) è il perimetro più interno, cuore della normativa e norma primaria atta alla corretta individuazione del rischio relativo ai processi di trattamento dei dati personali;
2. l’articolo 24 (misure tecniche e organizzative) è localizzato nel perimetro intermedio, la cui norma persegue la finalità di realizzareil contenimento dei rischi per la quale si attuano le appropriate misure tecniche e organizzative in un processo continuativo e migliorativo;
3. l'articolo 5 (“accountability”) è il perimetro più esterno, dove è necessario spiegare e comprovare che tutte le attività derivanti dai rischi individuati, l'organizzazione realizzata e le relative misure tecnologiche/procedurali portino ad una corretta gestione dei processi di trattamento dei dati personali.


### 1.5. Soggetti individuati dalla normativa

All'interno del processo di gestione e protezione dei dati personali, rappresentato nel grafico di cui al precedete paragrafo, operano tutti i soggetti individuati dal Regolamento e dal Codice e di seguito indicati, che prevedono delle **figure** con specifici **ruoli**, **relazioni tra i ruoli** e **responsabilità,** i quali debbono agire nei casi e nei modi prescritti:

- TITOLARE
- RAPPRESENTANTE
- RPD/DPO
- CONTITOLARE
- RESPONSABILE
- SUB-RESPONSABILE
- AUTORIZZATO
- DELEGATO/DESIGNATO
- TERZO
- DESTINATARIO
- INTERESSATO




Il concetto dell'assegnazione di ruoli e reponsabilità viene ulteriormente rimarcato dal considerando 79 del GDPR che enuncia:

La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara ripartizione delle responsabilità ai sensi del presente regolamento, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento.

### 1.6. Principi di base del GDPR

Il GDPR si struttura sui seguenti due principi cardine:

1) "**accountability"** come indicato dal comma 2 dell'articolo 5. Rendere una organizzazione "Accountable" significa assegnare compiti da eseguire e decisioni da assumere e aspettarsi che l'organizzazione risponda del suo operato e delle decisioni prese. In questo senso, l'accountability è l'essere tenuti a rispondere dei compiti assegnati, delle decisioni che ci competono ed essere in grado di dimostrarlo.

Il quadro complessivo di conoscenze sui dati personali e delle relative operazioni di trattamento fornito dal Registro dei trattamenti, è il primo passo verso l'accountability, poiché consente la valutazione del rischio sui diritti e le libertà delle persone e di attuare misure tecniche e organizzative adeguate per garantire un appropiato livello di sicurezza al rischio, in un processo di attività continuativo e migliorativo.

2) “**privacy by design and by default”**, ovvero la protezione dei dati fin dalla progettazione e protezione per impostazione predefinita come indicato dall’Articolo 25 GDPR :

> Tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, dell’ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all’atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
>
> Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l’accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l’intervento della persona fisica.

Il GDPR nel considerando 78 evidenzia **per la Pubblica Amministrazione** che: *"I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche **nell’ambito degli appalti pubblici**".*

### 1.7. Organizzazione delle attività di conformità e di accountability

Il presente Piano di Sicurezza fa parte di un insieme di documenti ad esso collegati finalizzati a rendere l’organizzazione **conforme** alle citate normative ed **essere in grado d**i **comprovarlo («accountability»),** da cui è necessario realizzare un insieme di attività dove le persone , le policy e i processi possano essere in grado di:

- stabilire gli obiettivi e comunicarli a tutta l’organizzazione;
- assegnare ruoli e responsabilità;
- individuare le competenze necessarie;
- stabilire regole (policy), processi e procedure;
- identificare gli asset (dati, tecnologie, processi aziendali rilevanti per la privacy);
- svolgere le analisi dei rischi con la individuazione/adeguamento delle misure tecniche e organizzative in un processo continuativo di miglioramento.

## 2. ORGANIZZAZIONE E PROFILI DI AUTORIZZAZIONE

In questa sezione viene descritta sinteticamente l’organizzazione delle strutture aziendali, i compiti e le relative responsabilità assegnate, in relazione ai trattamenti effettuati a fronte delle attività svolte dal seguente Ente:

Unione dei Comuni Gallura (di seguito il “Titolare”) ;

Via XX Settembre - 07024 - La Maddalena (SS) ;

P.Iva: 02346160902 ;

Email: info@unionegallura.it ;

PEC: info@pec.unionegallura.it ;

L'ente Unione dei Comuni Gallura è formato dai comuni di Arzachena, La Maddalena, Palau, Sant'Antonio di Gallura, Telti.

Di seguito vengono identificate le strutture organizzative che governano i processi di trattamento dei dati personali con i relativi profili di utenza:

- Organi
- Direttore Generale
- Area Amministrazione Generale

## 2.1. Organi

Oltre ai profili del Presidente, Giunta, Consiglio è presente il Nucleo di Valutazione dell'ente.

COMPETENZE

**Presidente**
**Giunta**
**Consiglio**

| Struttura | Descrizione dei compiti e delle responsabilità della struttura | Profilo |
|---|---|---|
| Presidente | Presidente protempore Ente | PRES_OI |
| Giunta | Membri della giunta | GIUNTA_OI |
| Consiglio | Sindaci dei Comuni | CONS_OI |

## 2.2. Direttore Generale

Il Direttore Generale è il responsabile tecnico-amministrativo dell'Ente e ha in capo anche le funzioni di Segretario Generale.

COMPETENZE GENERALI

**Direzione Generale e Segretario Generale**

In particolare al Direttore Generale compete:

- la direzione dei settori che compongono gli uffici che erogano i servizi interni e associati, secondo i criteri e le norme dettate dallo statuto e dai regolamenti;
- la segreteria generale
- la predisposizione dello schema di programma del bilancio e del conto consuntivo e della proposta del programma degli obiettivi e dei piani esecutivi di gestione;
- la cura l'esecuzione delle deliberazioni assunte dalla Giunta e dall'Assemblea secondo le proprie competenze;
- la responsabilità delle procedure di appalto e di concorso e la stipulazione dei contratti;
- l'emanazione degli atti che impegnano l'ente di gestione verso l'esterno e che la legge e lo statuto non riservano espressamente ad altri organi;
- la responsabilità del servizio di vigilanza ai fini del rispetto dei divieti e delle prescrizioni vigenti all'interno dell'Unione;
- la promozione delle iniziative di informazione e sensibilizzazione dei cittadini all'attività dell'Unione
- la gestione dei servizi di supporto all'attività generale dell'Ente

| Struttura | Descrizione dei compiti e delle responsabilità della struttura | Profilo |
|---|---|---|
| Direttore Generale | Direzione Generale e Segretario Generale | SG_DIRG |
| Nucleo di Valutazione | Membri del nucleo di valutazioni | NUCLEO_DIRG |

## 2.3. Area Amministrazione Generale

A capo dell'Area è preposto il Direttore Generale

COMPETENZE GENERALI

**Segreteria**

In materia di Segreteria e Affari Generali:

- la gestione dell’attività di segreteria di supporto agli Organi di governo: convocazione sedute, redazione dei verbali delle sedute, gestione attività amministrativa
- pubblicazione atti, delibere, decreti e disposizioni di servizio
- Segreteria e corrispondenza degli Organi
- gestione procedimenti legali.

**Ufficio Protocollo e Albo pretorio**

In materia di protocollo:

- gestione del protocollo generale in ingresso per tutto l'ente e in uscita per l'Ente/Area
- gestione degli atti amministrativi
- gestione della pubblicazione nell'albo pretorio.

**Ufficio Anticorruzione e trasparenza**

In materia di Anticorruzione e Trasparenza:

- proposte di piano,
- gestione del medesimo con sollecito e verifica attuazione
- inserimento dati su software di gestione trasparenza.

**Ufficio Bilancio e Ragioneria**

In materia di Bilancio:

- Redazione bilanci,
- Peg,
- Fondo incentivante personale,
- Variazioni di bilancio,
- Rendicontazione regione per servizi associati ,

- Certificati bilanci (BDAP e TBEL)

In materia di finanziario Ragioneria:

- Emissione ordinativi incasso e pagamento ,
- accertamenti,
- impegni,
- istruttoria visti contabili,
- mandati di pagamento per stipendi e F24,
- verifiche di cassa,
- gestione rapporto contrattuale revisore dei conti, autoliquidazione Inail, certificazione crediti.
- Piattaforma certificazione crediti. Fatture elettroniche.
- Rapporti con il Tesoriere.
- Conto annuale del personale

**Privacy e Transizione digitale**

In materia di Responsabile della Protezione Dati (Servizio associato DPO):

- il rapporto con il DPO – Responsabile Protezione dei dati dell'ente unione e dei comuni associati (*i dati personali non sono condivisi tra l'Unione e gli altri enti associati*);
- il coordinamento, la gestione amministrativa ed il monitoraggio in materia di privacy e protezione dei dati personali.

In materia di Transizione digitale

- responsabile della transizione digitale

**Tutela Ambientale e Protezione Civile (SA)**

In materia di Tutela Ambientale e Protezione Civile:

- Gestione piano e proposta di atti deliberativi e determinativi attuativi.
- None
- Atti di liquidazione conseguenti. Adempimenti normativi legati agli appalti banditi.

**Nucleo di Valutazione (SA)**

Gestione Nucleo di Valutazione (SA):

- Coordinamento e formalizzazione attività Nucleo di valutazione associato
- Gestione rapporto contrattuale Nucleo di valutazione.

**Formazione Professionale del Personale non dirigenziale (SA)**

In materia di Formazione Professionale del Personale non dirigenziale (SA):

Il servizio sovra comunale è delegato a gestire la formazione del personale dell'ente Unione e dei comuni degli enti aderenti alla presente convenzione tramite l'organizzazione e gestione dei corsi di formazione in loco o tramite la partecipazione a corsi da altri enti organizzati. I corsi organizzati dall'Unione potranno anche essere aperti a soggetti esterni nel caso in cui si ravvedano ragioni di convenienza ed interesse pubblico.

L'Unione si impegna a:

- redigere, sulla base delle proposte degli enti, un piano della formazione;
- organizzare i corsi di formazione richiesti dagli enti aderenti provvedendo ad assumere tutti gli atti amministrativi a ciò necessari, coordinandosi con i comuni al fine di venire incontro alle loro esigenze formative e logistiche;
- iscrivere, contestualmente impegnando e poi liquidando la relativa spesa, ai singoli corsi il personale autorizzato dai comuni richiedenti.

| Struttura | Descrizione dei compiti e delle responsabilità della struttura | Profilo |
|---|---|---|
| Area Amministrazione Generale | Responsabile Direttore Generale e Segretario Generale | DGSG_DIRG |
| Finanziario | Referente interno | RI_FIN |
| Finanziario | Addetti interni | AI_FIN |
| Affari Generali | Referente interno | RI_AAGG |
| Affari Generali | Addetti interni | AI_AAGG |
| Servizi Associati | Addetti Interni | AI_SA |
| Distretto Rurale | Referente interno | RI_DR |
| Distretto Turistico | Addetti Interni | AI_DT |

## 3. REGISTRO DEI TRATTAMENTI

L'Ente Unione dei Comuni Gallura a seguito delle funzioni di competenza sopra descritte tratta come Titolare dei dati i seguenti dati personali:

- dati personali comuni degli utenti, dei fornitori o di terzi ricavati o ricavabili da elenchi pubblici, albi professionali o camerali;
- dati personali comuni degli utenti, forniti dagli stessi per l'espletamento delle attività istituzionali del titolare del trattamento;
- dati personali comuni dei dipendenti e di altri soggetti contrattualizzati, necessari al regolare svolgimento del rapporto di lavoro o di collaborazione, nonchè quelli affidati al datore di lavoro per esigenze di natura bancaria.
- dati particolari sensibili del personale dipendente, idonei a rivelare lo stato di salute e l'appartenenza sindacale;
- dati particolari sensibili e biometrici inerenti a soggetti individuati per esempio attraverso eventuali sistemi di videosorveglianza;
- dati particolari giudiziari dei dipendenti, collaboratori, etc., in relazione ad eventuali procedimenti giudiziari;
- dati particolari giudiziari di fornitori e referenti di aziende in relazione a casellario giudiziario/carichi pendenti o eventuali contenziosi.

Di seguito vengono fornite alcune informazioni utili alla corretta gestione dei dati:

La sede legale e operativa dell'Ente Unione dei Comuni Gallura ove sono effettuati dei trattamenti di dati personali sia con strumenti informatizzati che cartacei è la seguente:

- Via XX Settembre , 07024 - La Maddalena (SS)

I dati personali presenti su supporto cartaceo e supporto elettronico, sono distribuiti tra gli uffici delle strutture organizzative dell'Ente, localizzati presso la sopra citata sede e/o presso ulteriori sedi operative in base alla distribuzione logistica del personale.

I dati in formato elettronico risiedono prevalentemente:

- (L) localmente su proprio sistema Client
- (C) centralmente su propri Data Center
- (SC) SaaS/Cloud del fornitore della soluzione applicativa/infrastrutturale

Le sedi dove sono localizzati i data center e gli archivi cartacei centralizzati, sono le seguenti:

- Data Center presso sede Via Vittorio Emanuele 9, Piano 2°, 07024 La Maddalena (SS)
- Backup Data center via TerraLugiana, Piano 1, 07024 La Maddalena (SS)
- Archivio di deposito per documenti oltre i 3 anni presso sede Via Vittorio Emanuele 9, Piano 2°, 07024 La Maddalena (SS)
-
-

Banche di dati personali la cui titolarità è afferente all'Ente possono essere trattati da soggetti esterni, sia su supporto cartaceo e/o informatizzato, anche localizzati

esternamente, che operano come Responsabili dei dati (con eventuali catene di sub-fornitori), a seguito di servizi contrattualizzati, come l'erogazione di servizi applicativi in SaaS/Cloud, servizi ICT di assistenza sulle applicazioni e i sistemi tecnologici presenti nelle proprie sedi ed servizi di consulenza aziendale, fiscale e legale, etc..

Ulteriori banche di dati personali possono essere trattati su supporti cartacei e informatizzati da soggetti contitolari esterni all'ente, per erogazione di servizi in modalità associata.

Il presente Ente può operare esso stesso anche come Responsabile dei dati, al fine di fornire servizi di trattamento di dati personali non afferenti alla sua titolarità, per servizi convenzionati con altri enti locali o nazionali.

In allegato è presente il registro dei processi di trattamento contenente l'elenco dei trattamenti effettuati come Titolare dei dati e come Responsabile dei dati, svolti alla data di redazione, in conformità alla normativa italiana di riferimento e all'articolo 30 del GDPR.

# 4. APPROCCIO BASATO SUL RISCHIO

## 4.1. Descrizione generale

L’approccio basato sul rischio permea l’intera logica applicativa del GDPR e porta il titolare a dover considerare “rischioso” per l’interessato qualsiasi trattamento di dati personali al quale sia applicabile il GDPR.

Per tale ragione, la consapevolezza che chi tratta dati personali in qualità di titolare del trattamento espone l’interessato a potenziali rischi, è il punto di partenza per un corretto recepimento dei principi fondanti del GDPR. Alcuni di tali principi, quali l’accountability e la privacy by design e by default, non fanno altro che guidare i titolari del trattamento verso l’adozione di misure e cautele che consentono di trattare i dati personali limitando il più possibile i rischi per gli interessati.

Mentre il GDPR fornisce, in particolare nel suo considerando 75, orientamenti su ciò che è considerato rischioso o elaborazione ad alto rischio, questa guida logicamente è abbastanza generale e non affronta su come procedere sull'identificazione e sulla valutazione di particolari rischi e danni associati ai trattamenti dei dati.

L’approccio basato sul rischio può tradursi come l’analisi preventiva del contesto del trattamento, del grado di probabilità e di gravità dei potenziali rischi ai quali è esposto l’interessato e, di conseguenza, la predisposizione di piani di azione volti a limitare il verificarsi degli eventi a rischio.

Si tratta di un processo di autovalutazione, all’esito del quale il titolare deve adottare le cautele e le misure che risultino (e che ritiene) più idonee a tutelare e proteggere gli interessati e i relativi dati personali.

L’analisi dei rischi deve essere generalmente compiuta per ogni macro processo o gruppi di macro processi all’interno delle strutture organizzative, avendo attenzione alla tipologia degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali, nonchè all’impatto sui danni e sofferenze del cittadino interessato.

Sono considerate ad alto rischio le aree nelle quali un accadimento, su uno più trattamenti all’interno dei processi, potrebbe produrre danni e sofferenze rilevanti e irreversibili nei confronti di cittadini quali soggetti interessati ed eventuali e conseguenti danni alla società.

L'articolo 24, paragrafo 1 richiede che i Titolari e i Responsabili del trattamento applichino "gli opportuni requisiti tecnici e organizzativi, con misure atte a garantire e dimostrare la conformità con il GDPR tenendo conto della "**Natura, ambito, contesto e finalità del trattamento**" al fine di valutare i rischi di varia natura e la gravità dei danni per i diritti e le libertà delle persone. I Titolari e i Responsabili del trattamento hanno anche l'obbligo di rivedere e aggiornare tali misure "ove necessario"

## 4.2. Rischio, Alto Rischio e DPIA

All’interno del GDPR non si rinviene una precisa nozione di “rischio”. Tale concezione può essere indirettamente ricavata da diverse disposizioni normative contenute all’interno del Regolamento ed in particolare:

## RISCHIO

| | Descrizione |
|---|---|
| **Definizione di rischio (Considerando 75)** | I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale (Considerando 75) |
| **Ulteriori esempi di rischio ( Articolo 32.2)** | • distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. |
| **Fattori da tenere conto quando si determina il livello di rischio (probabilità e gravità del rischio) (Considerando 76)** | • Natura;<br>• Ambito di applicazione;<br>• Contesto; and<br>• Finalità del trattamento. |
| **Rischio o Alto Rischio (Considerando 76)** | • Valutazione oggettiva. |

## ALTO RISCHIO O RISCHIO ELEVATO

| | Descrizione |
|---|---|
| **Quali tipi di trattamento possono risultare ad alto rischio?** | • Ciascuno dei rischi può diventare "ad alto rischio", in base alla "probabilità e gravità" dei rischi determinati in un processo di valutazione del rischio in riferimento alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento;<br>• quelli che comportano l'utilizzo di nuove tecnologie o;<br>• quelli che sono di nuovo tipo e in relazione ai quali il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale; e<br>• in particolare ai trattamenti su larga scala, |

| | |
|---|---|
| | che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati. |

In tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche si rende necessario produrre una Valutazione di impatto sulla protezione dei dati (DPIA), in base all'articolo 5 del GDPR.

Al fine di fornire un insieme più concreto di operazioni di trattamento che richiedono un DPIA, a causa del loro elevato rischio intrinseco, tenendo conto degli elementi particolari dell'articolo 35 ( 1) e 35 (3) (a) - (c), l'elenco da adottare a livello nazionale ai sensi dell'articolo 35, paragrafo 4, e considerando 71, 75 e 91, e altri riferimenti GDPR "suscettibili di rischio "operazioni di trattamento, i seguenti criteri dovrebbero essere considerati:

- **Valutazione o punteggio**, compresa la profilazione e la previsione, in particolare da "aspetti riguardanti le prestazioni del soggetto interessato sul luogo di lavoro, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione di movimenti" (punti 71 e 91).
- **Decisione automatizzata con significativo effetto giuridico o analogo**: trattamento che mira a prendere decisioni sugli interessati che producono "effetti giuridici riguardanti la persona fisica" o che "influenza in modo significativo anche la persona fisica" (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti degli individui.
- **Monitoraggio sistematico**: elaborazione utilizzata per osservare, monitorare o controllare le persone interessate, compresi i dati raccolti attraverso le reti o "un monitoraggio sistematico di un'area accessibile al pubblico" (articolo 35, paragrafo 3, lettera c).
- **Dati sensibili o dati di natura altamente personale**: ciò include categorie speciali di dati personali come definiti all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati definiti all'articolo 10.
- **Dati trattati su larga scala**: il GDPR non definisce ciò che costituisce su larga scala, sebbene il considerando 91 fornisca alcune indicazioni. In ogni caso, il WP29 raccomanda che i seguenti fattori, in particolare, siano presi in considerazione per determinare se il trattamento è effettuato su larga scala:
    - il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
    - il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
    - la durata, ovvero la persistenza, dell'attività di trattamento;
    - la portata geografica dell'attività di trattamento.

- **Corrispondenza o combinazione di set di dati**, ad esempio provenienti da due o più operazioni di trattamento eseguite per scopi diversi e / o da diversi responsabili del trattamento dei dati in un modo che eccederebbe le ragionevoli aspettative dell'interessato.
- **Dati personali di persone fisiche vulnerabili** (considerando 75): il trattamento di questo tipo di dati è causa dell'aumento dello squilibrio di potere tra le persone interessate e il titolare del trattamento dei dati, il che significa che le persone potrebbero non essere in grado di acconsentire facilmente o opporsi trattamento dei loro dati, o esercitare i loro diritti (bambini).
- **Uso innovativo o applicazione di nuove soluzioni tecnologiche o organizzative**, come la combinazione dell'uso di impronte digitali e riconoscimento facciale per un migliore controllo dell'accesso fisico, ecc.
- Quando il trattamento in sé "**impedisce agli interessati di esercitare un diritto o di utilizzare un servizio o un contratto**" (articolo 22 e considerando 91).

Nella maggior parte dei casi, un Titolare può considerare che un processo che soddisfa due criteri richiederebbe la realizzazione di una DPIA. In generale, il WP29 ritiene che più criteri sono soddisfatti in relazione al trattamento, maggiore è la probabilità di presentare un alto rischio per i diritti e le libertà degli interessati, e quindi di richiedere una DPIA, indipendentemente dalle misure che il Titolare prevede adottare.

### 4.3. Potenziali minacce

La valutazione del rischio dovrebbe considerare le potenziali minacce di ogni processo di trattamento. Tali minacce includono:

- ingiustificabile o eccessiva raccolta di dati;
- uso o conservazione di dati obsoleti o inesatti;
- uso inappropriato o improprio dei dati, incluso l’uso di dati al di là della ragionevole aspettativa dell’individuo;
- perdita o distruzione di dati;
- alterazione dei dati;
- furto di dati;
- ingiustificabile e non autorizzato accesso, trasferimento, condivisione o pubblicazione di dati;
- indisponibilità dei dati.

### 4.4. Potenziali danni

Le organizzazioni devono valutare la probabilità e gravità di qualsiasi danno che potrebbe risultare dai rischi di trattamento in relazione alle minacce che incombono su di essi. Tali danni possono includere:

a) Danni materiali, tangibili, fisici o economici all’individuo, come:

- danno fisico;
- perdita di libertà personale e di movimento;
- perdita finanziaria e di guadagno;
- altri significanti danni di interesse economico, per esempio causato da furto di identità.

b) Danni immateriali, intangibile sofferenza dell'individuo, come:

- danno derivante dal controllo o dall'esposizione di identità, caratteristiche, attività, associazioni o opinioni;
- limitazione della libertà di parola, associazione, ecc .;
- danno alla reputazione;
- incutere paura personale, familiare, lavorativa o sociale, imbarazzo, apprensione o ansia;
- inaccettabile intrusione nella vita privata;
- illecita discriminazione o stigmatizzazione;
- perdita di autonomia;
- limitazione della capacità personale di scelta;
- furto di identità e privazione del controllo sui dati personali.

### 4.5. Tabelle di Analisi del rischio

In allegato è presente il documento contenente la valutazione del rischio e dei potenziali impatti, generalmente compiuta per ogni macro processo o gruppi di macro processi all'interno delle strutture organizzative, avendo attenzione alla tipologia degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali, nonchè all'impatto sui danni e le sofferenze del cittadino interessato.

# 5. TRATTAMENTI AFFIDATI ALL'ESTERNO

Rendendosi necessario l'affidamento di alcuni servizi all'esterno dell'organizzazione, l'Ente Unione dei Comuni Gallura , in qualità di Titolare del trattamento dei dati procede, in tale sezione del Documento, a descrivere i soggetti nominati "Responsabile dei dati" ai sensi dell'art. 28 GDPR, per il trattamento dei dati personali svolti in nome e per conto dell'Ente.

In particolare, la nomina dei soggetti è avvenuta per iscritto mediante apposita lettera nella quale, oltre che indicare l'attività esternalizzata, sono espressamente indicate le misure che il soggetto esterno si impegna a mettere in atto per garantire la sicurezza dei dati conformemente a quanto previsto nel Regolamento.

Il Titolare ha affidato il servizio a soggetti che forniscano i requisiti di affidabilità previsti nel Regolamento.

Di seguito, per ciascun soggetto responsabile identificato come "*Outsourcer*", vengono riportati:

- descrizione dell'attività;
- la natura dei dati esternalizzati;
- i dati identificativi del fornitore Responsabile dei Dati;
- i dati identificativi dei sub-fornitori.

| Descrizione sintetica dell'attività | Trattamenti di dati interessati | Soggetto esterno (Fornitore) | Soggetto esterno (Elenco Sub-Resp) |
|---|---|---|---|
| Servizio di consulenza legale specialistica per enti | comuni identificativi; particolari; relativi a condanne penali o reati; | Avv. Enrico Pintus Via Stintino, 2 - Sassari | |
| Servizio di consulenza del lavoro e/o elaborazione paghe per enti | comuni identificativi; di appartenenza a sindacato; relativi alla salute della persona; | Solutive S.r.l. Via Mazzini, 1 - 23811 Ballabio (LC) | |
| Servizio di amministratore di sistema su server/applicazioni/backup/restore per enti | comuni identificativi; particolari; relativi a condanne penali o reati; | Halley Sardegna S.r.l. Via Ticino, 7 - 09032 Assemini (CA) | |
| Servizio di amministratore di sistema su server/applicazioni/backup/restore per enti | comuni identificativi; particolari; relativi a condanne penali o reati; | Comune di La Maddalena P.zza Garibaldi, 13 - 07024 La Maddalena (SS) | |
| Servizio di posta elettronica certificata per enti | comuni identificativi; particolari; relativi a condanne penali o reati; | Aruba S.p.A. Via San Clemente, 53 - 24036 Ponte San Pietro (BG) | |
| Servizio di posta elettronica per enti | comuni identificativi; particolari; relativi a condanne penali o reati; | Aruba S.p.A. Via San Clemente, 53 - 24036 Ponte San Pietro (BG) | |
| Servizio di conservazione | comuni identificativi; | Halley Sardegna S.r.l. | |

| | | | |
|---|---|---|---|
| sostitutiva per enti | particolari; relativi a condanne penali o reati; | Via Ticino, 7 - 09032 Assemini (CA) | |
| Servizio di Responsabile della Protezione dei Dati (RPD/DPO) per enti | comuni identificativi; particolari; relativi a condanne penali o reati; | Extra Informatica S.r.l. Z.I. Predda Niedda Strada 30 snc - Sassari | |
| Servizio di Revisione dei conti per enti | comuni identificativi; particolari; relativi a condanne penali o reati; | Dott.ssa Clementina Di Pellegrini Via S.Antonio n.6 - Calangianus (SS), | |
| Servizio di amministratore di sistema su sistemi di videosorveglianza per enti | comuni identificativi; di origine razziale o etnica; su opinioni politiche o affilazioni; su convinzioni religiose o filosofiche; di appartenenza a sindacato; relativi alla salute della persona; relativi all'orientamento o la vita sessuale; biometrici biologici; particolari su minori di 14 anni; relativi a condanne penali o reati; | Tecnit Srl Via P.L. Nervi 22/24 - 09067 Z.I. (CA) | |
| Servizio applicativo di gestionali/contabili per enti | comuni identificativi; | Halley Sardegna S.r.l. Via Ticino, 7 - 09032 Assemini (CA) | |
| Servizio di redazione Piano urbano di sostenibilità | comuni identificativi; particolari; relativi a condanne penali o reati; per un periodo di tempo non superiore al conseguimento delle finalità, o in base alle scadenze previste dalla norma di legge; | Dottor Agronomo Giovanni Pizzadili Via Vincenzo Piro 20 07026 Olbia | |
| Servizio di componente del Nucleo o Organismo interno di valutazione per enti | comuni identificativi; particolari; relativi a condanne penali o reati; durata come indicata al contratto ex art. 28 GDPR in essere con il soggetto titolare, o con il responsabile del trattamento in contesti di sub-fornitura; | Dasein Srl Lungo Dora Colletta 81 - Torino (TO) | |

## 6. MISURE TECNICHE E ORGANIZZATIVE

Per misura si intende:

a) lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia;
b) le attività di verifica e controllo effettuate nel medio e lungo periodo, essenziali per assicurarne l'efficacia, che possono essere così sintetizzate:
   - la pseudonimizzazione e la crittografia dei dati personali;
   - la capacità di garantire la riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di elaborazione;
   - la possibilità di ripristinare la disponibilità e l'accesso ai dati personali in modo tempestivo in caso di incidente fisico o tecnico;
   - un processo per testare, analizzare e valutare regolarmente l'efficacia di misure tecniche e organizzative per garantire la sicurezza dell'attività.

Nei paragrafi che seguono vengono analizzate nel dettaglio le misure tecniche e organizzative connesse alla corretta gestione del rischio.

In allegato è presente il documento contenente in forma sintetica, le architetture tecnologiche e organizzative in essere al fine di meglio individuare le azioni da adottare per contrastare i rischi informatici, anche per rendersi conformi alle misure minime e alle attribuzioni delle funzioni di amministratore di sistema, nonchè le attività per l'assegnazione di ruoli in relazione ai soggetti individuati dalla normativa.

## 6.1. Identificazione e Autenticazione degli utenti

Tale misura deve essere diretta a garantire che un utente acceda solo ai sistemi di cui ha bisogno, ogni utente deve quindi seguire un processo di identificazione e autenticazione prima di qualsiasi accesso ai dati personali.

I fattori di autenticazione sono raggruppati in tre famiglie in base a:

- una informazione che l'utente conosce, ad esempio una password;
- un dispositivo che l'utente ha, ad esempio una smart card;
- una azione che l'utente fa, come apporre la propria impronta digitale o una firma scritta a mano.

L'autenticazione di un utente è considerata forte quando richiede una combinazione di almeno due di questi fattori.

PRECAUZIONI DI BASE

- Definire un identificativo univoco per utente e vietare account condivisi tra più utenti. Nel caso in cui l'utilizzo di identificatori generici o condivisi è inevitabile, richiede una conferma esplicita da parte della direzione e attuare le misure per registrare le loro attività;
- Rispettare le raccomandazioni di base quando le password sono utilizzate per l'autenticazione, in particolare memorizzando il file password in modo sicuro e applicando a loro i seguenti requisiti di complessità:
    - avere una lunghezza di almeno 8 caratteri, compresi 3 tipi di caratteri su 4 (maiuscole, minuscole, numeri, caratteri speciali);
- Se l'autenticazione include una misura che limita l'accesso all'account come:
    - la password può essere di soli 4 caratteri se l'autenticazione si basa sull'apparecchiatura posseduta dall'individuo e se la password viene utilizzata solo per sbloccare il dispositivo fisico detenuto dall'individuo stesso (ad esempio una smart card o un telefono cellulare) e che il dispositivo sia bloccato al 3 ° tentativo fallito.
    - avere più di 5 caratteri se l'autenticazione richiede alcune informazioni riservate aggiuntive. Per le informazioni aggiuntive, utilizzare un identificatore riservato di almeno 7 caratteri e bloccare l'account al 5 ° tentativo fallito;
    - avere 12 caratteri minimi e 4 tipi di carattere se l'autenticazione si basa solo su una password;
    - il blocco dell'account dopo 10 tentativi falliti;
    - un eventuale "Captcha",
    - blocco temporaneo dell'account dopo diversi tentativi falliti,

COSA SI DEVE EVITARE

- Comunicare la propria password a chiunque;
- Memorizzazione di password in un file non crittografato
- Salvataggio delle password nel browser senza utilizzare una password principale;
- Utilizzo di password con un collegamento a informazioni personali (nome
- Utilizzo della stessa password per accedere a diversi account;
- Mantenere la password predefinita;
- Invio di password personali tramite e-mail.

## 6.2. Gestione delle Autorizzazioni di accesso

Tale misura deve essere diretta a consentire l’accesso ai dati di cui l’utente ha realmente bisogno.

PRECAUZIONI DI BASE

- Definire i profili di autorizzazione nei sistemi separando le attività e l'area di responsabilità
- Ritirare i diritti di accesso degli utenti non appena non sono più autorizzati ad accedere a una stanza o a una risorsa IT
- Effettuare una revisione annuale dei diritti di accesso al fine di identificare e rimuovere account non utilizzati e riallineare i diritti e il ruolo di ciascun utente.

COSA SI DEVE EVITARE

- Creazione o utilizzo di account condivisi per più utenti;
- Concessione dei diritti di amministratore agli utenti che non ne hanno bisogno;
- Concedere a un utente più privilegi del necessario;
- Dimenticare di rimuovere le autorizzazioni temporanee concesse a un utente (per una sostituzione
- Dimenticare di cancellare gli account utente delle persone che hanno lasciato l'organizzazione o cambiato ruolo.

## 6.3. Tracciamento degli accessi e gestione degli incidenti

**Registrare l'accesso ai sistemi e organizzare le procedure di gestione degli incidenti in caso di violazione sui dati** (violazione di riservatezza, integrità o disponibilità), al fine di poter identificare l'accesso fraudolento o l'uso abusivo di dati personali, o per determinare l'origine di un incidente sui sistemi IT. Devono quindi essere presenti dei sistemi di tracciamento con la registrazione dell'evento e il piano contenente le procedure di gestione degli incidenti sui dati.

PRECAUZIONI DI BASE

- Configurare i tracciamenti (ovvero memorizza gli eventi in "file di registro/log") per registrare le attività degli utenti
    - questi registri devono salvare eventi su un periodo che non può superare i sei mesi (tranne nel caso di un obbligo legale
    - gli accessi devono essere al minimo registrati con il loro identificatore utente, la data e l'ora della loro connessione, nonché la data e l'ora della loro disconnessione;
    - in alcuni casi, valutare se conservare anche le informazioni sulle azioni intraprese dall'utente, come la tipologia di dati consultati e / o modificati e il riferimento dei dati interessati.
- Comunicare agli utenti la presenza di un sistema di tracciamento, dopo aver informato e consultato il personale coinvolto;
- Proteggere i sistemi di tracciamento e le informazioni registrate da accessi non autorizzati, in particolare rendendole inaccessibili agli individui la cui attività è stata soggetta al tracciamento;
- Attivare procedure che effettuano il monitoraggio dei log e procedere periodicamente ad un monitoraggio per rilevare possibili anomalie;
- Aggiornare periodicamente i responsabili della gestione dei sistemi di tracciamento, affinchè comunichino al titolare dei dati, il prima possibile, di qualsiasi anomalia o incidente di sicurezza;
- Notificare le violazioni dei dati personali all'autorità di controllo competente per la protezione dei dati e, ad eccezione di indicazioni fornite dal GDPR , effettuare la notificazione anche alle persone interessate nel caso si presenti un alto rischio nei loro confronti, in modo da limitare gli impatti causati dalla violazione.

COSA SI DEVE EVITARE

- Usare le informazioni provenienti dai log per scopi impropri, come ad esempio usare i registri per conteggiare le ore lavorate dagli utenti.

## 6.4. Sicurezza delle postazioni di lavoro

Tale misura deve essere diretta a prevenire l'accesso fraudolento alle postazioni di lavoro. Evitare i rischi di intrusione nei sistemi informatici *client,* le *workstation* e i *notebook* costituisce uno dei punti principali di ingresso per gli attacchi alle infrastrutture *server.*

PRECAUZIONI DI BASE

- Implementare una procedura di disconnessione per bloccare qualsiasi workstation non utilizzata per un oltre un determinato periodo di tempo;
- Installare un firewall e limitare le porte di comunicazione autorizzate a quelle strettamente necessarie per il corretto funzionamento delle applicazioni installate sulle workstation;
- Utilizzare software antivirus regolarmente aggiornati e definire una politica che impone aggiornamenti regolari dei software;
- Configurare i software in modo che gli aggiornamenti di sicurezza vengano eseguiti automaticamente quando possibile;
- Favorire la memorizzazione dei dati degli utenti su un supporto di memorizzazione regolarmente sottoposto a backup e accessibile tramite la rete dell'organizzazione piuttosto che sulle workstation stesse. Nel caso in cui i dati siano memorizzati localmente, fornire delle procedure di sincronizzazione o misure di backup per gli utenti e addestrarli nel loro uso;
- Limitare la connessione di supporti mobili (chiavette USB, dischi rigidi esterni, ecc.) all'essenziale;
- Disabilitare l'esecuzione automatica per i supporti rimovibili;
- Fornire delle credenziali temporanee prima di qualsiasi intervento di assistenza temporanea sulle workstations e i Personal Computer, se questo non svolto da amministratori di sistema preventivamente autorizzati.

COSA SI DEVE EVITARE

- Utilizzo di sistemi operativi obsoleti
- Concessione dei diritti di amministratore agli utenti che non hanno competenze nella sicurezza IT.
- L'esecuzione di applicazioni scaricate non provenienti da fonti sicure;
- L'uso di applicazioni che richiedono diritti di amministratore.

## 6.5. Sicurezza dei dispositivi mobili

Tale misura deve essere diretta a evitare la violazione dei dati in seguito al furto o alla perdita di un'apparecchiatura mobile. L'uso crescente di *laptop,* chiavette *USB e smartphone* rende necessaria la preparazione di misure per limitare la violazione dei dati, riducendo le probabilità di furto o la perdita di tali apparecchiature o l'accesso ai dati presenti.

PRECAUZIONI DI BASE

- Rendere consapevoli gli utenti sui rischi specifici associati all'uso di strumenti mobili (ad es. furto di attrezzature) e sulle procedure pianificate per ridurre questi rischi;
- Implementare misure di backup o sincronizzazione periodica per le workstation mobili, al fine di proteggersi contro la perdita dei dati memorizzati;
- Fornire misure di crittografia per proteggere le workstation mobili e dei supporti di archiviazione mobile (laptop, penne USB, dischi rigidi esterni, CD-ROM, DVD-RW, ecc.), ad esempio:
    - creazione di contenitori crittografati (un file contenente altri file e cartelle).
    - crittografia del disco rigido nella sua interezza quando il sistema operativo offre tale funzionalità;
- Per quanto riguarda gli smartphone, oltre al codice PIN per la carta SIM, attivare il blocco automatico del terminale con la richiesta di informazioni confidenziali per sbloccarlo (password, schema, ecc.).

COSA SI DEVE EVITARE

- Utilizzo dei servizi cloud per il backup installati per impostazione predefinita, o effettuare la sincronizzazione senza eseguire un analisi approfondita delle loro condizioni d'uso e delle loro garanzie di sicurezza. Tali servizi non sono generalmente in grado di rispettare le misure fornite nella scheda da allegare/inserire al contratto della gestione dei subfornitori in subappalto.

## 6.6. Sicurezza dei server

Tale misura deve essere diretta a rafforzare le misure di sicurezza applicate ai *server.*

PRECAUZIONI DI BASE

- Consenti solo alle persone qualificate di accedere agli strumenti e alle interfacce di amministrazione, per assistenza temporanea sui server attraverso strumenti di amministrazione remota, si devono eventualmente fornire delle credenziali temporanee prima di qualsiasi intervento se questo non svolto da amministratori di sistema preventivamente autorizzati;
- Utilizzare account con minori privilegi per operazioni comuni;
- Adottare una politica password specifica per gli amministratori. Cambiare le password almeno ogni tre mesi, per ogni sistema in gestione ad ogni singolo amministratore, centralizzando il sistema di identificazione;
- Installa gli aggiornamenti critici senza ritardi sia per i sistemi operativi che per le applicazioni, pianificando una verifica automatizzata settimanale;
- In termini di amministrazione del database:
    - implementare misure contro gli attacchi di SQL injection, script, ecc.
    - utilizzare identificativi di account personalizzati per accedere ai database e creare account specifici per ciascuna applicazione;
- Eseguire i backup e controllarli regolarmente;
- Implementare il protocollo TLS (in sostituzione di SSL 1 ) o altro protocollo che garantisca un adeguato livello di sicurezza per la crottografazione e l'autenticazione.

COSA SI DEVE EVITARE

- Utilizzo di servizi non protetti (autenticazione cleartext, flusso in chiaro, ecc.);
- Utilizzo di server che ospitano database per altre funzioni;
- Localizzazione di database su un server in una rete direttamente accessibile da Internet;
- Utilizzo di account utente generici (in altre parole condivisi tra più utenti).

## 6.7. Sicurezza dei siti Web

Tale misura deve essere diretta a garantire che vengano applicate ai siti *web* le basilari "*best practices*" di sicurezza. Ogni sito *web* deve garantire l'integrità e la riservatezza delle informazioni che invia o raccoglie.

PRECAUZIONI DI BASE

- Implementare il protocollo TLS (che sostituisce SSL 23 ) su tutti i siti Web, utilizzando solo la versione più recente e controllare la sua corretta implementazione;
- Rendere obbligatorio l'uso di TLS per tutte le pagine, compresi i moduli che raccolgono dati personali o che autorizzano l'utente e quelli sui quali vengono visualizzati o trasmessi I dati personali non pubblici;
- Limitare le porte di comunicazione a quelle strettamente necessarie per il corretto funzionamento delle applicazioni installate.
- Consentire solo alle persone qualificate di accedere agli strumenti e alle interfacce di amministrazione. In particolare, limitare e profilare l'uso di account di amministratore agli amministratori di sistema solo per le azioni amministrative che lo richiedono;
- Se vengono utilizzati cookie non richiesti dal servizio, raccogliere il consenso dell'utente Internet dopo averlo informato e prima che il cookie sia depositato;
- Eseguire il monitoraggio del servizio WEB mantenere aggiornate il software di base e i framework utilizzati.

COSA SI DEVE EVITARE

- Trasferimento di dati personali tramite una URL come ID o password;
- Utilizzo di servizi non protetti (autenticazione cleartext, flusso in chiaro, ecc.).;
- Utilizzo di server che ospitano database o server come workstation, in particolare con client per la navigazione di siti Web, accesso elettronico messaggistica, ecc.;
- Localizzazione di database su un server direttamente accessibile da Internet;
- Utilizzo di account utente generici (in altre parole condivisi tra più utenti).

## 6.8. Protezione delle reti interne

Tale misura deve essere diretta ad autorizzare solo le funzioni di rete necessarie per l'elaborazione dei trattamenti dei dati.

PRECAUZIONI DI BASE

- Limitare l'accesso a Internet bloccando i servizi non essenziali (VoIP, peer to peer, ecc.);
- Gestire le reti Wi-Fi. Devono utilizzare la crittografia avanzata (WPA2 o WPA2-PSK con password complesse) e le reti aperte agli ospiti devono essere separate dalla rete interna;
- Richiede una VPN per l'accesso remoto, nonché, se possibile, una autenticazione forte dell'utente (smart card, dispositivo di generazione password one-time “OTP”, ecc.);
- Assicurarsi che nessuna interfaccia di amministrazione sia direttamente accessibile da Internet. L’attività di manutenzione da remoto deve essere effettuata tramite una VPN;
- Limitare e filtrare il traffico di rete verso gli indirizzi IP e le porte TCP/UDP/ICMP/.. essenziali , filtrando il traffico in entrata e in uscita sull'apparecchiatura (firewall, proxy, server, ecc.). Ad esempio, se un server web utilizza HTTPS, autorizzare solo il traffico in entrata questa macchina tramite la porta 443 e bloccare tutte le altre porte.

COSA SI DEVE EVITARE

- Utilizzo del protocollo telnet per la connessione remota alle apparecchiature di rete attive (firewall, router e switch). Invece, è consigliabile utilizzare SSH o un accesso fisico diretto all'apparecchiatura;
- Fornire agli utenti un accesso a Internet non filtrato;
- Configurazione di una rete Wi-Fi utilizzando una crittografia WEP.

## 6.9. Continuità del servizio

Tale misura deve essere diretta ad effettuare regolarmente i *backup* per evitare la perdita di dati e mantenere la loro integrità e definire un documente contenente il piano di ripristino dei dati (*contingency plan*) o un piano di continuità operativa (*disaster recovery*).

PRECAUZIONI DI BASE

- Riguardo al backup dei dati:
    - Quando i backup vengono inviati tramite la rete, è consigliabile crittografare il loro canale di trasmissione se il trasporto non è svolto tra reti perimetrate all'interno della rete dell'organizzazione.
    - Proteggere i dati di backup con lo stesso livello di sicurezza dei dati memorizzati sui server in produzione (ad esempio, crittografando i backup, organizzando l'archiviazione in un luogo sicuro o regolando contrattualmente un servizio di backup in outsourcing);
    - Conservare i backup su un sito esterno, o se possibile in casseforti impermeabili e antincendio;
    - Eseguire backup periodici e frequenti dei dati, siano essi in formato cartaceo o elettronico. Potrebbe essere appropriato eseguire backup incrementali su base giornaliera e backup completi a intervalli regolarisu periodo più lungo;
- Per quanto riguarda la gestione della continuità operativa:
    - Assicurarsi che utenti, fornitori di servizi e subappaltatori sappiano chi avvisare in caso di incidente;
    - Testare periodicamente il ripristino dei backup e l'applicazione del piano di gestione della continuità operativa.
    - Creare un piano di gestione della continuità operativa dei servizi IT, anche se breve, includendo l'elenco delle persone coinvolte;
- Per quanto riguarda l'attrezzatura:
    - inserire la ridondanza dell'unità di memoria, ad esempio utilizzando una tecnologia RAID .
    - utilizzare un gruppo di continuità per proteggere l’utilizzo della infrstruttura più critica;

COSA SI DEVE EVITARE

- Mantenere i backup nello stesso luogo dei computer che ospitano i dati. Un grave incidente che si verificherebbe in questo luogo determinerebbe una perdita definitiva dei dati.

## 6.10. Sicurezza fisica

Tale misura deve essere diretta a rafforzare la sicurezza dei locali che ospitano le infrastrutture IT e le apparecchiature di rete. L'accesso ai locali deve essere controllato per evitare o rallentare l'accesso non autorizzato, sia di materiale cartaceo, *file* o apparecchiature IT, in particolare per i *server.*

PRECAUZIONI DI BASE

- Installare sistemi di allarmi anti-intrusione e controllarli periodicamente;
- Installare rilevatori di fumo e strumenti antincendio e ispezionarli ogni anno;
- Garantire la sicurezza delle chiavi e dei codici di allarme che concedono l'accesso ai locali;
- Separare le aree dell'edificio in base ai rischi (ad esempio utilizzando un controllo di accesso dedicato per la sala computer);
- Tenere un elenco aggiornato delle persone o delle categorie di individui autorizzati a entrare in ciascuna area;
- Stabilire le regole e i metodi per controllare l'accesso dei visitatori, come minimo avere visitatori accompagnati, al di fuori delle aree di ricevimento pubbliche da una persona della tua organizzazione;
- Proteggere fisicamente le apparecchiature IT tramite metodi specifici (sistema di prevenzione incendi dedicato, attrezzatura di sollevamento contro possibili alluvioni, alimentazione elettrica e / o ridondanza del condizionamento d'aria, ecc.).

COSA SI DEVE EVITARE

- Trascurare la manutenzione delle sale computer (climatizzazione, UPS, ecc.), un guasto di questi sistemi spesso si traduce in macchine che si fermano o l'apertura di accesso alle camere (circolazione aria) che contribuiscono alla sicurezza fisica dei locali.

## 6.11. Sicurezza degli archivi storici

Tale misura deve essere diretta ad assicurare l’archiviazione dei dati che non vengono più utilizzati su base giornaliera, ma che non hanno ancora raggiunto la fine del periodo di trattamento. Gli archivi devono essere protetti, soprattutto se i dati archiviati sono dati sensibili o dati che potrebbero avere gravi conseguenze di impatto sugli interessati.

PRECAUZIONI DI BASE

- Definire una procedura di gestione degli archivi: quali dati devono essere archiviati, come e dove sono archiviati, come sono gestiti
- Implementare metodi di accesso specifici ai dati archiviati, poiché l'uso di un archivio è realizzato in modo specifico ed eventualmente in modalità eccezionale;
- Per quanto riguarda la distruzione degli archivi, selezionare una procedura che garantisca che l'archivio sia stato distrutto nella sua interezza.

COSA SI DEVE EVITARE

- Utilizzo di supporti che non hanno una garanzia sufficiente in termini di longevità. Ad esempio, la longevità di CD e DVD riscrivibili raramente superano i quattro o cinque anni.
- Mantenere i dati in un database attivo semplicemente monitorando lo stato del servizio di dataserver o file server. I dati archiviati devono essere accessibili a un profilo specifico di incaricato .

## 6.12. Gestione del software e privacy by design and default

Tale misura deve essere diretta ad integrare quanto prima la sicurezza durante le fasi di progettazione e di installazione e configurazione. La *privacy* deve essere integrata nello sviluppo o modifiche dei servizi che coinvolgono modifiche o nuovi trattamenti di dati personali sin dalle fasi di progettazione, al fine di offrire ai soggetti interessati un migliore controllo sui propri dati e una limitazione di errori, perdite, modifiche non autorizzate o uso illecito di dati personali nelle applicazioni e le infrastrutture tecnologiche coinvolte.

PRECAUZIONI DI BASE

- Integrare la privacy, compresi i requisiti di sicurezza, dalla progettazione di applicazioni o servizi. Questi requisiti possono influenzare le scelte di architettura (decentralizzata o centralizzata), caratteristiche (anonimazzazione, minimizzazione del dato), tecnologie (crittografia), ecc.;
- Per qualsiasi sviluppo che comporta trattmento di dati personali, esaminare i parametri relativi alla privacy, e in particolare la loro configurazione di default;
- Effettuare lo sviluppo del software e test in un ambiente informatico separato dalla produzione (per esempio, su diversi computer o macchine virtuali) e utilizzare dati fittizi o resi anonimi.

COSA SI DEVE EVITARE

- Utilizzo di dati personali degli interessati nelle fasi di sviluppo e test, è quindi indicato realizzare degli archivi con dati fittizzi durante le fasi suddette;
- Sviluppo di applicazioni o servizi senza tenere conto della sicurezza sui dati personali.

## 6.13. Crittografazione e autenticazione del dato

Tale misura deve essere diretta a garantire l'integrità, la riservatezza e l'autenticità del dato. Implementare funzioni di *hashing* per assicurare l'integrità dei dati, firme digitali, che oltre a garantirne l'integrità, sono in grado di verificare l'origine dell'autore delle informazioni e delle eventuali successive modifiche. Infine, implementare sistemi di crittografia per garantire la riservatezza di un messaggio duranti le fasi di conservazione e trasmissione.

PRECAUZIONI DI BASE

- Utilizzare un algoritmo riconosciuto e sicuro, ad esempio, i seguenti algoritmi:
    - per le firme, RSA-SSA-PSS come specificato in PKCS # 1 v2.1.
    - SHA-256, SHA-512 o SHA-3 come funzione hash;
    - HMAC che utilizza SHA-256, bcrypt, scrypt o PBKDF2 per memorizzare le password;
    - AES o AES-CBC per la crittografia simmetrica;
    - RSA-OAEP come definito in PKCS # 1 v2.1 per la crittografia asimmetrica;
- Utilizzare le dimensioni appropriate della chiave, per AES è consigliabile utilizzare chiavi di 128 bit e, per algoritmi basati su RSA, moduli ed esponenti segreti di almeno 2048 bit o 3072 bit, con esponenti pubblici, per la crittografia, maggiore di 65536;
- Proteggere le chiavi segrete, almeno con diritti di accesso restrittivi e una password sicura;
- Creare una procedura che descriva come gestire chiavi e certificati tenendo conto del caso di password dimenticate.

COSA SI DEVE EVITARE

- Utilizzo di algoritmi obsoleti, come DES e 3DES per la crittografia o MD5 e SHA1 come funzioni hash.

## 6.14. Gestione delle manutenzioni e distruzione dei dati

Tale misura deve essere diretta ad garantire la sicurezza dei dati in ogni momento del loro ciclo di vita. Le operazioni di manutenzione devono essere supervisionate per controllare l'accesso ai dati da parte dei fornitori di servizi. i dati devono essere distrutti prima di smaltire l'*hardware*.

PRECAUZIONI DI BASE

- Registrare la manutenzione e I rapportini di lavoro;
- Includere una clausola di sicurezza nei contratti di manutenzione stipulati dai fornitori di servizI;
- Assegnare a una persona la responsabilità dell'organizzazione di supervisionare il lavoro delle terze parti;
- Scrivere e implementare una procedura di cancellazione sicura dei dati;
- Cancellare in modo sicuro i dati dall'hardware prima che vengano smaltiti, inviati per la riparazione da una terza parte o alla fine di un contratto di noleggio.

COSA SI DEVE EVITARE

- Installazione di applicazioni per la manutenzione remota con vulnerabilità note;
- Riutilizzo, rivendita o smaltimento di supporti contenenti dati personali cancellati.

## 6.15. Sicurezza nella comunicazione dei dati tra organizzazioni

Tale misura deve essere diretta ad rafforzare la sicurezza in ogni trasmissione di dati personali. I servizi di comunicazione elettronica non sono un mezzo di comunicazione sicuro per trasmettere dati personali, senza misure aggiuntive. Un semplice errore di gestione può comportare la divulgazione di dati personali a soggetti non autorizzati destinatari e quindi interferire con il diritto alla *privacy* delle persone.

PRECAUZIONI DI BASE

- Criptare i dati prima di inviarli su un supporto fisico (DVD, chiavetta USB, disco rigido portatile) ad una terza parte;
- Quando si inviano dati attraverso la rete:
    - Garantire la riservatezza di informazioni riservate (chiavi di crittografia, password, ecc.) inviandoli tramite un canale separato (ad esempio, l'invio di un file crittografato tramite e-mail e la comunicazione della password per telefono o SMS);
    - utilizzare un protocollo che garantisca la riservatezza e l'autenticazione del server destinatario per i trasferimenti di file, ad esempio SFTP o HTTPS, utilizzando la versione più recente dei protocolli.
    - crittografare i documenti sensibili prima di inviarli;
- Se è necessario utilizzare un fax, impostare le seguenti misure:
    - pre-registrare i potenziali destinatari nella rubrica della macchina del fax (quando questa funzione è disponibile).
    - duplicare la trasmissione fax inviando anche i documenti originali al destinatario per posta;
    - visualizzare l'identità della macchina ricevente durante l'invio di messaggi;
    - installare il fax in un luogo accessibile solo al personale autorizzato con controllo degli accesso fisici;

## 6.16. Piano di Formazione

Tale misura deve essere diretta ad rendere ciascun utente all'interno della propria organizzazione consapevole della necessità di mantenere la *privacy* e la sicurezza delle informazioni.

PRECAUZIONI DI BASE

- Informare gli utenti delle misure attuate dalla loro organizzazione al fine di affrontare i rischi e le loro potenziali conseguenze.
- Documentare le procedure operative, tenerle aggiornate e renderle disponibili a tutti gli utenti interessati. In termini concreti, qualsiasi azione sui dati personali, sia che si tratti di operazioni legate all'amministrazione o di un semplice utilizzo di un'applicazione, deve essere spiegata in un linguaggio chiaro adattato a ciascuna categoria di utenti, in documenti a cui gli utenti possono fare riferimento.
- Spiegare agli utenti dei diversi profili di accesso alle applicazioni il mansionario delle istruzioni IT. Questo mansionario dovrebbe almeno includere un promemoria delle regole di protezione dei dati e delle sanzioni applicate in caso di inosservanza di queste regole, nonchè l'ambito di applicazione delle istruzioni indicate, che dovrebbe includere in particolare:
    - apparecchiature mobili (specialmente nel contesto del telelavoro);
    - spazi di archiviazione individuali;
    - reti locali; dispositivi personali (in particolare le condizioni per utilizzare tali dispositivi);
    - metodi di intervento dei team responsabili della gestione delle risorse IT per l'organizzazione;
    - mezzi di autenticazione utilizzati dall'organizzazione;
    - regole di sicurezza a cui gli utenti devono conformarsi, tra cui:
    - obbligo di informare il dipartimento IT interno di qualsiasi sospetta violazione dei dati o tentare di violare il proprio account utente IT e in generale qualsiasi disfunzione;
    - divieto di comunicare a terzi il proprio identificativo e password;
    - divieto di installare, copiare, modificare o distruggere software senza autorizzazione;
    - obbligo di bloccare i computer non appena gli utenti lasciano la postazione di lavoro;
    - non svolgere attività sui dati personali al di fuori del proprio profilo autorizzativo, in riferimento alle attività di propria competenza ;

- attenersi al rispetto delle procedure operative  finalizzate al trasferimento dei dati sui media mobili, previa autorizzazione da parte del supervisore e rispettando le norme di sicurezza.
- attenersi al rispetto delle procedure operative di gestione degli incidenti in caso di violazione sui dati personali e/o sulle infrastrutture tecnologiche di supporto.
- Le procedure per l'utilizzo delle risorse informatiche e delle risorse di telecomunicazione disponibili per l'utente quali:
- postazioni di lavoro;
- la rete;
- messaggistica elettronica;
- telefonia
- Le condizioni per la gestione delle attività di amministrazione del sistema e, se necessario, l'esistenza di sistemi di filtraggio automatico e sistemi di registrazione automatica;
- Indicare le sanzioni applicate in caso di inosservanza delle istruzioni contenute nel mansionario.