azienda regionale per l'edilizia abitativa
azienda regionale pro s'edilitzia abitativa

PIANO PER LA SICUREZZA INFORMATICA

E PER LA TUTELA DEI DATI PERSONALI

SOMMARIO

PREMESSA 3
1. GESTIONE FLUSSI DOCUMENTALI E VALUTAZIONE DEL RISCHIO 3
2. LA COMPONENTE ORGANIZZATIVA DELLA SICUREZZA 5
a) Componente fisica della sicurezza 6
b) Componente logica della sicurezza 8
c) Componente infrastrutturale della sicurezza 9
3. TUTELA DEI DATI PERSONALI 9
a) Modello organizzativo e adempimenti finalizzati all'applicazione del Regolamento (UE) 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 (GDPR Privacy) 9
b) Abilitazioni per l'accesso al sistema di gestione informatica dei documenti 10
c) Formazione dei documenti 11
d) Gestione, trasmissione, interscambio e accesso 12
4. CONSERVAZIONE DIGITALE 15

PREMESSA

Il "Piano per la sicurezza informatica e per la tutela dei dati personali" riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

Le misure di sicurezza adottate da AREA garantiscono che:

- i documenti e le informazioni trattate dall'Azienda Regionale per l'Edilizia Abitativa (di seguito AREA) siano disponibili, integre e riservate;
- i dati personali di qualsiasi tipologia vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Le misure di sicurezza devono formare oggetto di revisione almeno annuale in funzione dell'estensione del sistema, dell'evoluzione tecnologica, della variazione degli obiettivi dell'organizzazione e del manifestarsi di nuovi o mutati rischi per la sicurezza.

1. GESTIONE FLUSSI DOCUMENTALI E VALUTAZIONE DEL RISCHIO

La gestione dei flussi documentali e il sistema di protocollo informatico di AREA sono ispirati alle norme in materia di tutela dei dati personali di cui al Codice in materia di protezione dei dati personali e al GDPR, con particolare riferimento al concetto di responsabilità (accountability) ed alla capacità di adottare un processo efficace per la protezione degli stessi in grado di ridurre al minimo i rischi di una loro possibile violazione.

Si riporta di seguito la valutazione del rischio effettuata con riferimento al complesso della gestione documentale:

I - Definizione e contesto dell'operazione di trattamento, individuazione dei rischi

AREA tratta dati personali e di natura particolare di cittadini e imprese (dati di identificazione, dati patrimoniali e reddituali, dati relativi alla salute, dati giudiziari). Il trattamento avviene nell'ambito dei procedimenti amministrativi di competenza degli uffici e nei processi connessi all'attività dell'Azienda. Il trattamento è solo in parte automatizzato

L'infrastruttura sottesa al sistema di gestione documentale, nella sua componente legata al software applicativo e all'intera infrastruttura di AREA, può essere così descritta per macro aree:

- reti e apparati di rete;
- elaboratori e software di sistema;
- software applicativo;

- supporti informatici di memorizzazione;
- infrastrutture;
- contenitori/archivi cartacei, archivi informatici di Backup.

Il sistema di gestione documentale, garantisce:

1. Riservatezza: in modo che l'informazione sia resa disponibile solamente ai processi che la devono elaborare ed all'utilizzatore che ne è autorizzato all'uso;
2. Integrità: in modo che ogni informazione sia realmente quella originariamente immessa nel sistema informativo, ovvero successivamente legittimamente modificata;
3. Disponibilità: in modo che la reperibilità delle informazioni in funzione delle esigenze di continuità dei processi aziendali ed nel rispetto delle norme, tecniche e giuridiche, che ne impongono la conservazione storica.

I rischi cui è esposto il sistema di gestione documentale suindicato sono di seguito riportati :

- rischio legato all'accesso di soggetti non autorizzati nei locali tecnici;
- rischio di guasti tecnici hardware, software e supporti, possibilità cioè che strumenti fisici e logici si deteriorino o si danneggino, per caso fortuito, incuria o dolo, attraverso attività fisiche e logiche, in modo tale da non consentire la fruizione del sistema di gestione documentale;
- rischio di penetrazione in reti di comunicazione, device e servizi (accesso alla rete telematica senza autorizzazione, attacchi informatici);
- rischio legato ad errori umani cioè la a possibilità che, a causa di incuria o distrazione, il sistema di gestione documentale, o le sue attività, siano messe a rischio sotto il loro profilo logico e fisico (accesso a device e punti rete incustoditi, interruzione prolungata di servizi elettrici, incendio e allagamento dei locali tecnici);
- rischio per possibili eventi distruttivi (danneggiamento/distruzione degli edifici e delle connessioni di rete).

II – Misure di sicurezza organizzative

Al fine di mitigare i rischi l'Azienda ha adottato una serie di misure di sicurezza organizzative che consistono, principalmente, in:

a) individuazione dei ruoli e delle responsabilità del personale, delle misure tecniche e organizzative adottate per la sicurezza dei dati personali la c.d. componente organizzativa della sicurezza (art. 2)
b) i ruoli e le responsabilità in materia di tutela dei dati sono definiti con atto del Direttore Generale (Determinazione n. 1650 del 09/06/2021) che prevede:

   - la delega delle funzioni del Titolare ai direttori pro tempore dei servizi centrali e territoriali di AREA, secondo le rispettive competenze e responsabilità;

   - la delega al Direttore del SERFIC per l'adozione, la gestione e l'implementazione delle soluzioni tecnico-informatiche atte a prevenire e contrastare in termini uniformi per tutta l'AREA, i rischi connessi alla sicurezza informatica (cd. cyber-security) correlati alla protezione dei dati personali e le competenze di responsabile IT con riferimento ai compiti previsti in relazione ai data breach;

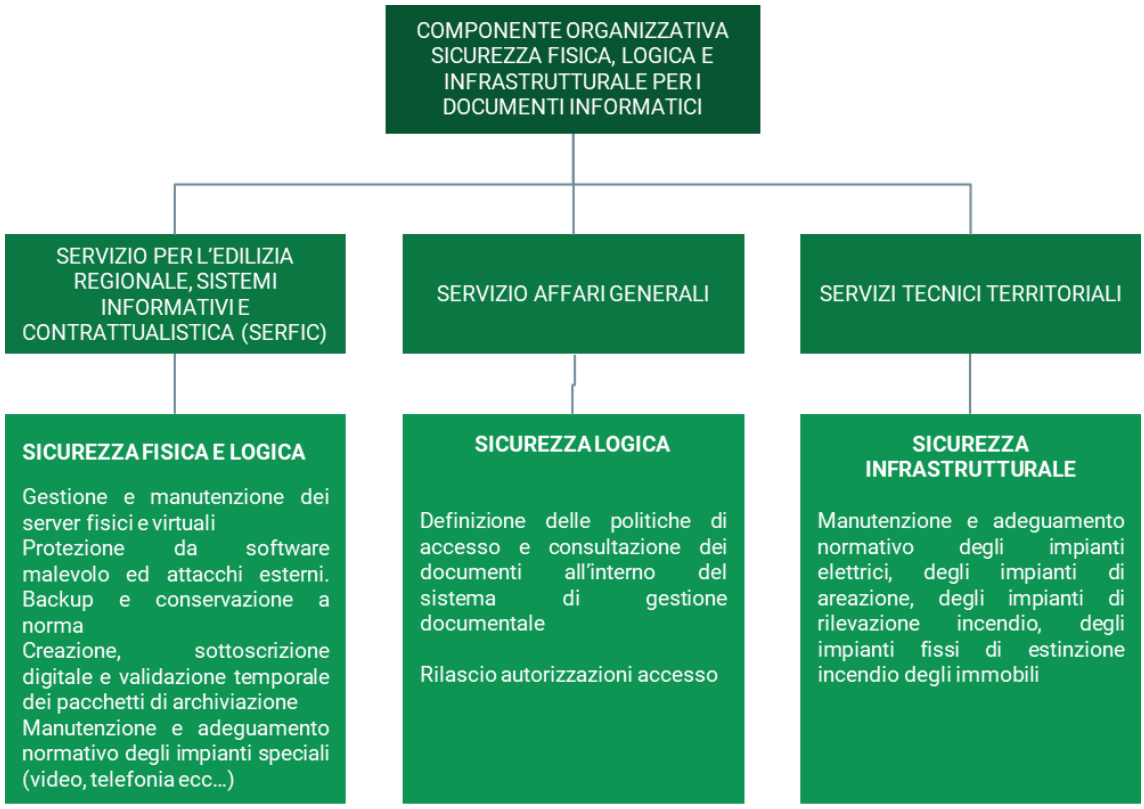
- di mantenere in capo al Direttore Generale pro tempore le funzioni di referente per la gestione del data breach e i compiti e le funzioni di raccordo e coordinamento, coerentemente col proprio ruolo, al fine di garantire un presidio costante per conto del Titolare nelle questioni non riconducibili interamente alle competenze amministrative degli altri delegati del trattamento e, in qualità di vertice gerarchico del Titolare;
- la delega al RPD, oltre ai compiti indicati all'art. 39 del Regolamento, delle funzioni di impulso e proposta degli interventi di adeguamento alla normativa vigente nonché la detenzione del registro del titolare del trattamento;

c) tenuta, in capo al SERFIC, di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete), in caso di riorganizzazioni interne o di cessazione dal servizio o assegnazione del personale ad altro ruolo, si provvede alla revoca dei diritti e dei profili di autorizzazione e al recupero di materiali e mezzi del trattamento;
d) le procedure relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) sono definite e documentate e stabiliscono almeno lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento. Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi. Il responsabile del trattamento deve fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza;
e) le violazione dei dati personali sono immediatamente segnalate al Titolare del trattamento, alle autorità competenti e agli interessati;
f) tutti i dipendenti, lavoratori e persone autorizzate al trattamento, sono formalmente autorizzate al trattamento dei dati e agli stessi sono impartire, dai Direttori dei Servizi, delegati del Titolare, le istruzioni ai sensi dell'articolo 29 del Regolamento (UE) 2016/679 e dell'articolo 2-quaterdecies del d.lgs. 101/2018;
g) formazione iniziale e continua di tutti i dipendenti in materia di protezione dei dati.

2. LA COMPONENTE ORGANIZZATIVA DELLA SICUREZZA

La componente organizzativa della sicurezza legata alla gestione dei flussi documentali si riferisce alle attività svolte per l'erogazione delle funzionalità di gestione documentale, protocollo informatico e della documentazione soggetta a registrazione particolare.

L'Azienda individua nell'ambito della sua organizzazione i Servizi aziendali che si occupano di vari aspetti inerenti la sicurezza fisica, logica e infrastrutturale:



a) Componente fisica della sicurezza

La gestione e manutenzione dei server è affidata al Servizio per l'edilizia regionale, sistemi informativi e contrattualistica (SERFIC) al cui interno è incardinato il Settore Flussi informativi e contrattualistica che svolge, tra l'altro le seguenti funzioni/attività:

1. gestione flussi informativi e documentali e relative infrastrutture;
2. aggiornamento ed implementazione del sito istituzionale;
3. la gestione e lo sviluppo del sistema informatico, dei sistemi di rete per la trasmissione e in generale di tutte le tecnologie e servizi ICT per l'Azienda;
4. la gestione tecnica del sito web, banche dati tributaria e ipo/catastale, linee di telefonia e connessione dati;
5. l'assistenza alle postazioni di lavoro per problemi hardware e software e utilizzo applicativi;
6. la gestione della casella istituzionale di posta elettronica e della PEC (attivazioni, rilascio credenziali ecc…);
7. affidamento e gestione dei contratti per la gestione documentale e la conservazione digitale.

Il controllo degli accessi fisici alle risorse del sistema informativo di AREA è regolato secondo i seguenti principi:

• l'accesso è consentito soltanto al personale di AREA, nonché a dipendenti di aziende o enti esterni, previa autorizzazione dell'Amministratore di sistema ed esclusivamente per motivi di servizio, manutenzione e controllo;

• l'accesso è consentito al Responsabile della protezione dei dati personali esclusivamente per attività di verifica del rispetto dei requisiti di sicurezza (in presenza di personale di AREA autorizzato dall'Amministratore di sistema);

• le chiavi di accesso sono custodite esclusivamente dal personale individuato;

• gli accessi fisici alle sedi di AREA sono registrati e conservati ai fini della imputabilità delle azioni conseguenti ad accessi non autorizzati;

• il personale in servizio presso ciascuna sede ha l'obbligo di utilizzare il badge sia in ingresso che in uscita per rilevare la propria presenza.

Su ogni server e su ogni dispositivo in uso agli utenti è installata un'applicazione di protezione dalle minacce informatiche monitorato a livello centrale dal Settore flussi informativi e contrattualistica che comprende i seguenti elementi:

- antivirus – Network attack defense
- sandbox analyzer
- anti-exploit
- mitigazione dei Ransomware
- machine learning HyperDetect
- analisi rischio da fattore umano

Con riferimento alle "Misure minime di sicurezza ICT per le Pubbliche Amministrazioni" di cui alla Delibera della Presidenza del Consiglio dei Ministri del 1 agosto 2015 e alla Circolare dell'Agenzia per l'Italia Digitale n. 2/2017 del 18 aprile 2017 si fa rifermento alle procedure e ai documenti prodotti in merito dal Servizio competente (SERFIC) di AREA.

COPIE DI SICUREZZA E FLUSSI CONSERVATIVI

Dispositivo	**PERIODICITA' BACKUP**	
	Risorse locali	**Cloud**
Database	GIORNALIERA	NON PREVISTO
VM Documenti e allegati	GIORNALIERA	NON PREVISTO
SERVIZIO DI CONSERVAZIONE DIGITALE SAAS QUALIFICATO AGID - MAGGIOLI	QUOTIDIANA (2 TENTATIVI AL GIORNO) PER IL FLUSSO DEL REGISTRO GIORNALIERO DI PROTOCOLLO MENSILE GLI ALTRI FLUSSI ATTIVATI, IN BASE ALLA QUANTITÀ DI DATI PRODOTTI (I PACCHETTI SONO GENERATI DAL SISTEMA VERSANTE IN BASE AI DATI CHE VIA VIA DIVENTANO "CONSERVABILI")	-Aggiornamento a delta del DR/backup con RPO di 15 minuti -

b) Componente logica della sicurezza

La componente logica della sicurezza è ciò che garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

Le competenze sono ripartite tra il Servizio per l'edilizia regionale, sistemi informativi e contrattualistica (SERFIC) e il Servizio Affari Generali (SAG).

Il SERFIC gestisce i contratti relativi al sistema di gestione documentale e di conservazione, attiva le credenziali di accesso al sistema sulla base dell'abilitazione rilasciata dal Responsabile della gestione documentale, attiva le caselle PEC/PEO dell'Azienda, all'interno del Settore sono individuati, con provvedimento del Direttore Generale, gli Amministratori di Sistema.

All'interno del SAG è incardinato il Settore affari generali cui sono attribuite, tra l'altro, le funzioni gestione documentale e di protocollazione (ricezione, protocollazione, assegnazione della corrispondenza presso la direzione generale e le strutture territoriali) e la gestione delle mail e PEC aziendali.

Il Direttore del Servizio Affari Generali è Responsabile della gestione documentale.

Tale componente è realizzata attraverso:

a) la tracciabilità delle operazioni di visualizzazione, smistamento, rimozione dei documenti da parte degli utenti abilitati all'utilizzo dell'applicativo di gestione documentale: tutte le attività elencate sono registrate in forma non modificabile. In particolare, laddove le modifiche di taluni indici siano consentite, viene memorizzato il versioning degli stessi in moda da risalire sia all'utente che ha apportato modifiche sia ai valori esistenti prima della modifica;

b) l'identificazione, autenticazione e autorizzazione degli utenti abilitati all'utilizzo dell'applicativo di gestione documentale;

c) la riservatezza dei dati, ottenuta mediante l'attribuzione della visibilità dei documenti esclusivamente ai soggetti e/o ai servizi aziendali competenti;

d) l'integrità dei dati, ottenuta mediante l'impossibilità per gli utenti dei servizi aziendali di apportare modifiche ai documenti protocollati;

e) la disattivazione delle credenziali di accesso degli utenti non più autorizzati alla consultazione degli archivi (per termine del rapporto di lavoro, trasferimento presso altro Ente, cambio di mansioni, etc…);

L'accesso all'applicativo di gestione documentale avviene a seguito di abilitazione da parte del Responsabile della gestione documentale (o del suo vicario) e attivazione delle credenziali di dominio da parte del SERFIC.

Si distinguono;

- l'abilitazione per l'accesso al sistema di gestione documentale per la creazione di documenti informatici;
- l'abilitazione per le funzionalità di registrazione di protocollo;
- l'abilitazione per la visualizzazione dei documenti protocollati.

Le modalità e i termini di rilascio delle abilitazioni sono riportate al successivo art. 3, lett.a).

La disabilitazione delle utenze cessate, l'attribuzione di eventuali diritti operativi particolari è esclusiva competenza del Responsabile della gestione documentale (o del suo vicario) per il tramite del SERFIC.

c) Componente infrastrutturale della sicurezza

La manutenzione e l'adeguamento normativo degli impianti elettrici, di aerazione, di rilevazione incendio e degli impianti fissi di estinzione incendio degli immobili sono di competenza dei Servizi territoriali Tecnici.
La sala server dov'è custodito il complesso principale dell'infrastruttura sistemistica fisica e virtuale è dotata di:

- continuità elettrica;
- impianto di condizionamento;
- estintori a CO2.

Le sedi in cui sono ubicate le sale server sono dotate di sistema di antintrusione collegato ad una centrale operativa di vigilanza.

3. TUTELA DEI DATI PERSONALI

I criteri utilizzati per la tutela dei dati personali delle persone fisiche assicurano che tali dati siano protetti in tutto il ciclo di vita del documento (sia analogico sia informatico).
A ogni documento, all'atto della registrazione nel sistema di protocollo informatico, è associata una Access Control List (ACL) che consente di stabilire quali utenti o gruppi di utenti hanno accesso ad esso.
All'atto della protocollazione l'UOP assegna al documento il livello di riservatezza distinguento l'accesso a uno o più utenti o all'interno ufficio (Servizio e/o settore). L'accesso ai protocolli riservati è consentito esclusivamente all'utente o all'ufficio cui il documento è indirizzato.

a) Modello organizzativo e adempimenti finalizzati all'applicazione del Regolamento (UE) 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 (GDPR Privacy)

Con la Determinazione n. 1650 del 09/06/2021 - Nuovo modello organizzativo e adempimenti finalizzati all'applicazione del Regolamento (UE) 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 (GDPR Privacy) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati – di dospone la delega, ai direttori pro tempore dei servizi centrali e territoriali di AREA, secondo le rispettive competenze e responsabilità, delle seguenti funzioni:

- verificare la liceità e la proporzionalità dei trattamenti di dati personali effettuati dalla struttura di riferimento, procedendo alla ricognizione dei trattamenti di dati personali, giudiziari e di natura particolare svolti nella struttura organizzativa di propria competenza, l'analisi dei flussi informativi e del rischio per i diritti e le libertà degli interessati;
- compilare e tenere costantemente aggiornato, per i trattamenti di competenza, il registro delle attività di trattamento del Titolare;
- individuare i soggetti autorizzati a compiere operazioni di trattamento fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite, ivi compreso il richiamo espresso alle presenti misure e alle policy regionali adottate dal Titolare;
- designare gli amministratori di sistema in aderenza alle norme vigenti in materia;
- garantire agli interessati l'esercizio dei diritti previsti dagli articoli 15 e seguenti del Regolamento e provvedere a dare riscontro alle istanze degli interessati;

- predisporre le informative relative al trattamento dei dati personali di competenza nel rispetto degli articoli 13 - 14 del Regolamento;
- effettuare gli adempimenti correlati, per quanto di competenza, all'attuazione degli articoli 26 e 28 del Regolamento, concernenti, rispettivamente, gli obblighi correlati alla situazione di contitolarità del trattamento e disciplina del responsabile esterno del trattamento;
- rilevare i casi nei quali effettuare la valutazione d'impatto sulla protezione dei dati personali e condurre o presidiare lo svolgimento della stessa valutazione di impatto secondo le direttive e previa consultazione del DPO, provvedendo, ove necessario anche alla consultazione preventiva del Garante per la protezione dei dati personali ai sensi dell'articolo 36 del Regolamento;
- collaborare, per quanto di competenza, con il responsabile della protezione dei dati della Regione Sardegna, nell'esecuzione dei compiti ad esso attribuiti;
- adottare le misure tecniche e organizzative adeguate ad attuare in modo efficace e fin dalla progettazione i principi di protezione dei dati personali e integrare nel trattamento le garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati (privacy by design) e adottare le misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari in relazione a ciascuna specifica finalità del trattamento (privacy by default).
- attuare, per quanto di competenza, le prescrizioni contenute nei provvedimenti imposti dall'Autorità Garante per la protezione dei dati personali;
- gestire le violazioni di dati personali (*data breach*), con particolare riferimento alla decisione di notifica, fermo restando quanto disposto dall'articolo 8 delle Direttive e dalla specifica procedura data breach. Detta funzione non è ulteriormente delegabile;
- adottare e ove necessario riesaminare e aggiornare le misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al Regolamento; fatte salve eventuali misure particolari correlate alle specificità delle finalità del trattamento, della categoria di interessati o dei dati trattati, le predette misure possono consistere in interventi conformi a linee guida e policy da applicare secondo standard comuni a tutti gli uffici dell'Amministrazione.

b) Abilitazioni per l'accesso al sistema di gestione informatica dei documenti

L'abilitazione per l'accesso al sistema di gestione documentale per la creazione di documenti informatici e per le funzionalità di registrazione di protocollo, di cui all'allegato 4, deve essere richiesto dal Direttore del Servizio cui afferisce l'utente al Responsabile della gestione documentale che, se autorizzato, inoltrerà la richiesta al Responsabile dei Servizi Informativi (SERFIC).

L'accesso ai documenti protocollati è consentito previa autorizzazione del Responsabile per la gestione documentale, ai sensi dell'art. 61, comma 3, lett. a) del DPR 445/2000, che definisce, sulla base delle richieste dei Direttore dei Servizi in cui i dipendenti sono incardinati e delle autorizzazioni al trattamento dei dati rese dai medesimi Direttori, il livello di autorizzazione per l'accesso alle funzioni del sistema di protocollo informatico distinguendo tra autorizzazioni riferite:

- alla sola attività assegnata al dipendente (tramite smistamento sul sistema gestionale);

- alle attività assegnate al settore di appartenenza;
- alle attività assegnate al Servizio di appartenenza.

Il Direttore generale e il suo sostituto, il Responsabile della gestione documentale e il vicario, gli amministratori di sistema, nominativamente individuati con disposizione del Direttore generale, hanno accesso a tutto il protocollo informatico.

Il Direttore generale può richiede, con riferimento alle proprie attività e competenze, motivato accesso a documenti registrati o una parte del protocollo informatico per ulteriori dipendenti, previa autorizzazione al trattamento dei dati.

I dipendenti del Settore in cui è incardinata l'attività di protocollazione hanno accesso a tutti i documenti protocollati e da protocollare ricevuti tramite il sistema di gestione documentale, tramite le PEC e le mail aziendali e in cartaceo.

La ricerca e la riassegnazione di specifici documenti inerenti o connessi comunque a uno specifico affare o procedimento di competenza del richiedente dipendente di AREA, sempre che non si tratti di documenti riservati o ad accesso riservato, può essere richiesta all'Unità Organizzativa di Protocollo (UOP).

I documenti assegnati al Settore risorse umane sono sempre considerati documenti ad accesso riservato al solo personale assegnato al medesimo Settore a cui deve essere presentata la richiesta di accesso.

Eventuali ulteriori autorizzazioni all'accesso motivato per la visualizzazione di documenti assegnati alla competenza di Servizi differenti da quello di appartenenza devono essere richieste al Responsabile della gestione documentale.

I documenti sono assegnati tenendo conto delle competenze e delle attività degli Organi istituzionali e della struttura organizzativa (Servizi) così come definiti negli atti di organizzazione http://www.area.sardegna.it/index.php?xsl=2398&s=43&v=9&c=13439&na=1&n=10&tb=13175.

Il Direttore del Servizio cui afferisce l'utente potrà autorizzare direttamente l'utente:

- all'accesso alla consultazione dell'eventuale casella PEC assegnata al servizio o all'area funzionale;
- all'invio di messaggi di posta elettronica certificata dalla casella PEC eventualmente assegnata al servizio o all'area funzionale.

c) Formazione dei documenti

Le risorse strumentali e le procedure utilizzate dai Servizi per la formazione e trasmissione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti Linee Guida dell'Agenzia per l'Italia Digitale;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- la conservazione sostitutiva digitale;
- l'interscambiabilità dei documenti all'interno dell'AOO.

I documenti redatti dai Servizi aziendali sono prodotti con l'ausilio di applicativi di videoscrittura e possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. I formati dei documenti prodotti all'interno dell'AOO, nonché gli allegati ad essi, rispondono alle raccomandazioni dell'Agid (Formati di file e riversamento Allegato 2 alle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici") e sono:

- Documenti impaginati — PDF, Microsoft® OOXML (.docx) e Word (.doc), OpenDocument Text (.odt), Rich-Text Format (.rtf);
- Ipertesti — XML, dialetti e schemi XML (.xsd, .xsl), HTML (.html, .htm), fogli di stile per XML/HTML (.xsl, .xslt, .css);
- Posta elettronica— .eml;
- Fogli di calcolo— Microsoft® OOXML (.xlsx) e Excel (.xls), OpenDocument Spreadsheet (.ods);
- Presentazioni multimediali — Microsoft® OOXML (.pptx) e PowerPoint (.ppt), OpenDocument Presentation (.odp);
- Immagini raster — JPEG (.jpg, .jpeg), TIFF (.tif, .tiff), PNG, GIF;
- Immagini vettoriali e modellazione digitale — SVG, Adobe® Illustrator® (.ai);
- Modelli digitali — StereoLithography (.stl); Autodesk® DWG™, DXF™, DWF™, FBX™;
- Video — formati video delle famiglie MPEG2 e MPEG4;
- Contenitori multimediali — MP4, MPEG2, AVI RIFF (.avi);
- Archivi compressi —ZIP, RAR, TAR compresso (.tgz, .t7z, …), ISO9660 (.iso);
- Documenti amministrativi — fattura elettronica, response SAML SPID, segnatura di protocollo;
- Applicazioni crittografiche — certificati elettronici (.cer, .crt, .pem), chiavi crittografiche (.pkix, .pem), marcature temporali elettroniche (.tsr, .tsd, .tst), impronte crittografiche (.sha1, .sha2, .md5, …); per le firme e i sigilli elettronici avanzati: buste crittografiche XAdES (.xml), CAdES (.p7m, .p7s), PAdES (.pdf), contenitori ASiC (.zip); KDM (.kdm.xml).

Fermo restando la possibilità di utilizzare, per determinati contesti, ulteriori tipologie di file avendo cura di seguire le indicazioni contenute nell'Allegato 2 "Formati di file e riversamento" delle Linee Guida sopra citate.

Per attribuire in modo certo la titolarità del documento e la sua integrità il documento informatico è sottoscritto con firma digitale.

d) Gestione, trasmissione, interscambio e accesso

Il sistema operativo delle risorse elaborative destinate ad erogare il servizio di protocollo informatico è conforme alle specifiche previste dalla normativa vigente.

Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in maniera tale che:

1. gli utenti non possano mai accedere ai documenti al di fuori del sistema di gestione informatica dei documenti;
2. avvenga la registrazione delle attività rilevanti ai fini della sicurezza nonché quelle necessarie per la manutenzione svolte sul server di cui sopra dagli utenti abilitati o dai fornitori di servizi di assistenza

informatica opportunamente nominati Responsabili esterni del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679 in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate;

3. venga effettuato periodicamente un backup su risorse interne dei volumi contenenti i documenti presenti nel sistema di gestione documentale e relativi allegati.

Il sistema di gestione informatica dei documenti, intendendo per esso l'applicazione utilizzata per la creazione, protocollazione e archiviazione dei documenti:

a) garantisce la disponibilità, la riservatezza e l'integrità dei documenti;
b) consente la produzione giornaliera del registro di protocollo che viene trasmesso entro la giornata successiva al sistema di conservazione;
c) consente la produzione del registro di protocollo annuale;
d) assicura la corretta e puntuale registrazione di protocollo dei documenti;
e) fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto da AREA e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
f) consente il reperimento delle informazioni riguardanti i documenti registrati;
g) consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte degli utenti dei Servizi aziendali interessati;
h) garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

L'accesso al programma di gestione dei flussi documentali (sicr@web) è riconosciuto agli Organi istituzionali e a tutti i dipendenti dell'Azienda secondo le seguenti disposizioni:

1. la visualizzazione all'interno del programma di gestione dei flussi documentali, dei documenti contenenti dati personali è sempre limitata agli utenti la cui funzione è strettamente connessa al procedimento collegato alle tipologie documentarie ad essi smistate. La visibilità dei documenti, in generale, è sempre la più limitata possibile;

2. l'abilitazione all'utilizzo delle funzionalità specifiche del programma di gestione dei flussi documentali (produzione e protocollazione dei documenti) è riservato agli utenti **appositamente abilitati** dal Responsabile della gestione documentale o dal suo vicario e previa attivazione delle credenziali di dominio da parte del Responsabile dei Servizi Informativi (SERFIC);

3. tutti gli utenti interni che accedono al programma di gestione dei flussi documentali devono essere preventivamente "autorizzati al trattamento dei dati personali" ai sensi di quanto previsto dal Regolamento UE 2016/679 e i nominativi devono essere riportati, a cura del Dirigente del Servizio di appartenenza, nel Registro delle attività di trattamento, previsto dall'art.30 del GDPR[1]. Ad essi, con particolare riferimento al trattamento dei dati personali nell'ambito della gestione dei flussi documentali, sono impartite le seguenti istruzioni:

[1] Il Registro, accessibile dal link **https://rpd.regione.sardegna.it/registrotrattamento/auth.php?id=2138&otp=Z21pOf6!KSfjP!gkmIljGBGdCPqkgSGWLfGZ8GQgeM9_RKkptm,** deve essere compilato con attenzione e mantenuto aggiornato nel corso del tempo e in caso di variazione dei trattamenti.

I. trattare i dati personali in modo lecito e secondo correttezza;
II. raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;
III. verificare che tali dati siano esatti e, se necessario, aggiornarli;
IV. comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati a riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti;
V. astenersi dal comunicare a terzi, al di fuori dell'ambito lavorativo, qualsivoglia dato personale;
VI. informare tempestivamente il Titolare del trattamento di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;
VII. informare tempestivamente il Titolare del trattamento qualora si verificasse la necessità di porre in essere operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle risultanti dalle istruzioni riportate nell'atto di nomina, nonché di ogni istanza di accesso ai dati personali da parte di soggetti interessati e di ogni circostanza che esuli dalle istruzioni impartite;
VIII. accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
IX. accertarsi dell'identità degli interessati e della loro autorizzazione al trattamento e dell'eventuale autorizzazione scritta a terzi, al momento del ritiro di documentazione in uscita;
X. non fornire telefonicamente, a mezzo fax o attraverso strumenti telematici, dati e informazioni relativi a terzi, senza una specifica autorizzazione del Titolare;
XI. non fornire telefonicamente, a mezzo fax o attraverso strumenti telematici, dati e informazioni ai diretti interessati, senza aver prima accertato la loro identità;
XII. dovrà essere autorizzato all'invio di messaggi di posta elettronica tradizionale (dal proprio account istituzionale)
XIII. utilizzo di password di accesso "robuste" e modifica delle stesse almento ogni tre mesi.

Inoltre, in base alla tipologia di strumento utilizzato per il trattamento sono fornite le seguenti ulteriori prescrizioni.

<u>Trattamenti con strumenti elettronici</u>

- non salvare documenti contenenti dati personali sulle risorse locali (hard disk della postazione pc o del notebook o comunque di qualsiasi dispositivo aziendale) o su dispositivi di memorizzazione esterni (hard disk esterni, chiavette usb) o ancora su dvd/cd-rom;
- a fine turno di lavoro, cancellare dalle risorse locali (e svuotare il cestino) eventuali file contenenti dati personali (dopo averli salvati – se necessario – come sopra riportato): con particolare attenzione alla cartella "Download" o comunque alla/e cartella/e dove vengono scaricati i file dal browser. Cancellarne il contenuto e svuotare il cestino;
- non dare evidenza delle credenziali di accesso al proprio pc, alla webmail, agli applicativi (come ad esempio, scrivendo su post-it login+password) o a servizi on line;
- le credenziali di accesso sono strettamente personali e non vanno comunicate ad altri soggetti;
- al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari, o si lavori con collegamento da remoto, in questi casi assicurarsi di attivare un salvaschermo (screen-saver) protetto dalle credenziali di autenticazione;

- in caso di assenza momentanea dalla propria postazione accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. A tal fine è necessario chiudere la sessione di lavoro sul PC attraverso la disconnessione (logout) oppure, in alternativa, attivare un salvaschermo (screen-saver) protetto dalle credenziali di autenticazione. Relativamente allo screen-saver occorre osservare le seguenti prescrizioni:
    - non deve mai essere disattivato;
    - il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
    - deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito.
- quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare che soggetti non abilitati al trattamento ne prendano visione.

Trattamenti senza strumenti elettronici

- per quanto riguarda l'eventuale documentazione cartacea, gli atti e i documenti contenenti dati personali devono essere conservati, dagli autorizzati al trattamento, per la durata di esso e successivamente riposti in archivi ad accesso controllato, al fine di escludere l'accesso agli stessi da parte di persone non incaricate al trattamento. Ciò vale in generale per tutte le pratiche giornalmente trattate che non devono essere lasciate incustodite al termine del turno di lavoro;
- nel caso di trattamento di dati sensibili o di dati giudiziari, la documentazione deve essere conservata in contenitori muniti di serratura, al fine di escludere l'acquisizione o la presa visione degli stessi, da parte di persone non incaricate al trattamento;
- qualora sia necessario distruggere i documenti contenenti dati personali, è buona norma utilizzare gli appositi apparecchi "distruggi documenti"; in assenza di tali strumenti, i documenti devono essere sminuzzati in modo da non essere più ricomponibili;
- gli autorizzati al trattamento sono tenuti a segnalare le eventuali necessità di dotazioni e arredi, in modo da poter adempiere a quanto prescritto;
- analogamente, per quanto riguarda i flussi di documenti cartacei all'interno degli uffici o fra le sedi territoriali di AREA, devono essere adottate idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in buste chiuse).

Inoltre, ai sensi di quanto previsto dall'art. 46 del CAD, recante "Dati particolari contenuti nei documenti trasmessi", al fine di garantire la riservatezza dei dati sensibili o giudiziari di cui all'articolo 4, comma 1, lettere d) ed e), del 10 Codice della privacy, i documenti informatici trasmessi ad altre pubbliche amministrazioni per via digitale possono contenere soltanto i dati sensibili e giudiziari consentiti dalla legge o da regolamenti, indispensabili per il perseguimento delle finalità per le quali sono acquisiti.

Per le misure specifiche inerenti alla protocollazione e gestione delle registrazioni di protocollo riservate, delle PEC/PEO e della corrispondenza personale e riservata si rinvia al Manuale di gestione documentale.

4. CONSERVAZIONE DIGITALE

Si rimanda al Manuale della conservazione digitale di AREA per le specifiche inerenti il processo di conservazione degli archivi secondo quanto previsto dalle vigenti Linee Guida.