REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

AGENTZIA REGIONALE PRO S'AMPARU DE S'AMBIENTE DE SARDIGNA
AGENZIA REGIONALE PER LA PROTEZIONE DELL'AMBIENTE DELLA SARDEGNA
ARPAS

Direzione Generale

Determinazione n. 1851/2023 del 13-10-2023

OGGETTO: APPROVAZIONE REGOLAMENTO INFORMATICO DELL'ARPAS

VISTI

- la Legge Regionale n. 6 del 18.05.2006 e ss.mm.ii. della Regione Autonoma della Sardegna, che ha istituito l'Agenzia regionale per la protezione dell'ambiente della Sardegna (ARPAS);
- la Deliberazione n. 50/10 del 08/10/2020 della Giunta Regionale e il successivo Decreto n. 112/2020 del 13.10.2020 del Presidente della Giunta Regionale, recanti la nomina dell'Ing. Alessandro Sanna a Direttore Generale dell'ARPAS per tre anni;
- il Regolamento generale e di organizzazione dell'ARPAS, approvato con Determinazione del Direttore Generale n. 31/2015, successivamente modificato con Determina del Direttore Generale n. 922 del 04.07.2017;
- il DPR nr. 81 del 13.06.2023 che aggiorna il codice di comportamento dei dipendenti pubblici (DPR n. 62 del 16.04.2013), con l'inserimento di norme riguardanti l'utilizzo delle tecnologie informatiche, dei mezzi di informazione e dei social media;
- il Codice di comportamento del personale ARPAS approvato con Determinazione n. 1816/2021 del 16.11.2021;

CONSIDERATO che l'Agenzia, nello svolgimento della sua attività istituzionale è tenuta a prestare la massima attenzione alla sicurezza delle informazioni e a perseguire elevati livelli di sicurezza fisica e logica del proprio sistema informativo e informatico, adottando idonee misure organizzative, tecnologiche ed operative volte a prevenire il rischio di utilizzi impropri e a proteggere le informazioni delle risorse informatiche;

DATO ATTO che si rende necessario procedere all'aggiornamento del Regolamento sull'utilizzo delle risorse e degli strumenti informatici approvato con propria Determinazione n. 968 del 21.07.2020 per adeguarlo alle evoluzioni tecnologiche e normative;

CONSIDERATO che in base al vigente Regolamento Generale e di Organizzazione dell'Agenzia, il Servizio Sistema Informativo e Informatico della Direzione Generale svolge il compito di elaborare e definire le politiche di implementazione dei sistemi informatici e informativi agenziali e, nell'ambito di tale obiettivo generale dell'Agenzia, ha predisposto il nuovo Regolamento Informatico dell'ARPAS;

RITENUTO necessario definire le regole e le condizioni per l'utilizzo delle risorse informatiche di ARPAS da parte dei dipendenti e di tutti coloro che, in virtù di un rapporto di lavoro a qualsiasi titolo o di fornitura di servizi (collaboratori, consulenti, stagisti, fornitori, etc.), utilizzano tali risorse;

VISTO il parere positivo espresso dalla Direttrice Amministrativa dell'ARPAS;
VISTO il parere positivo espresso dal Responsabile per la Transizione al Digitale dell'ARPAS;
Per le motivazioni espresse in premessa che debbono intendersi richiamate:

DETERMINA

1. di adottare il Regolamento informatico dell'ARPAS, e dei relativi allegati A (Normativa di riferimento, definizioni, protezione persone fisiche e trattamento dei dati personali) e B (Buone pratiche di tenuta delle postazioni di lavoro a distanza), allegato alla presente per farne parte integrante e sostanziale, e di disporre la pubblicazione sia nella sezione Disposizioni generali - Atti generali del sito web istituzionale dell'ARPAS sia nel Portale interno dell'ARPAS;
2. di abrogare il Regolamento vigente approvato con propria Determinazione n. 968 del 21.07.2020*;*
3. di abrogare l'istruzione operativa IOP 01 (Gestione dei servizi informatici) approvata con proprio Ordine di Servizio n. 1 del 15.10.2014;
4. che il suddetto Regolamento entra in vigore con la pubblicazione della presente determinazione;

La presente determinazione è soggetta agli obblighi di pubblicazione nell'Albo Pretorio on-line del sito istituzionale.

Il Direttore Generale *
ALESSANDRO SANNA

** Documento informatico sottoscritto con firma digitale ai sensi del Decreto legislativo 82/2005.*

REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

AGENTZIA REGIONALE PRO S'AMPARU DE S'AMBIENTE DE SARDIGNA
AGENZIA REGIONALE PER LA PROTEZIONE DELL'AMBIENTE DELLA SARDEGNA
ARPAS

Direzione Generale

CERTIFICATO DI PUBBLICAZIONE

Direzione Generale
Determinazione n. 1851/2023 del 13-10-2023

Si certifica che la determinazione 1851/2023 trovasi in corso di pubblicazione nell'Albo pretorio on line dell'ARPAS per 15 giorni dal 13-10-2023 al 28-10-2023.

L'originale informatico dell'Atto è stato predisposto e conservato presso l'ARPAS in conformità alle regole tecniche di cui all'articolo 71 del Decreto legislativo 82/2005. Nella copia analogica la sottoscrizione con firma autografa è sostituita dall'indicazione a stampa del nominativo del soggetto responsabile secondo le disposizioni di cui all'articolo 3 del Decreto legislativo 39/1993.

Il Responsabile *
ALESSANDRO SANNA

** Documento informatico sottoscritto con firma digitale ai sensi del Decreto legislativo 82/2005.*

REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA
AGENTZIA REGIONALE PRO S'AMPARU DE S'AMBIENTE DE SARDIGNA
AGENZIA REGIONALE PER LA PROTEZIONE DELL'AMBIENTE DELLA SARDEGNA
ARPAS

Direzione Generale
Servizio Sistema informativo e informatico

REGOLAMENTO INFORMATICO ARPAS

Ottobre 2023

Sommario

ART. 1 – AMBITO DI APPLICAZIONE

1.1 OGGETTO E FINALITA'

1.1.1 Il presente Regolamento disciplina l'utilizzo delle risorse e strumenti informatici dell'ARPAS, nel rispetto di quanto previsto dal Codice dell'amministrazione, dalle Linee Guida AgID sulla Sicurezza Informatica, dal Piano Triennale per l'informatica, dal Regolamento Europeo n. 679/2016 (GDPR), dal Codice della Privacy, dalla Linee guida del Garante per posta elettronica e internet e dalla Direttiva n. 2/09 sull'utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro, fermo restando il diritto del lavoratore a mantenere una sfera di riservatezza anche nelle relazioni professionali.

1.1.2 Il Regolamento è osservato da tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché da tutti i collaboratori, a prescindere dal rapporto contrattuale intrattenuto (lavoratori somministrati, collaboratori a progetto, tirocinanti, ecc.) che si trovino ad essere assegnatari/utilizzatori di risorse informatiche e di servizi di connettività messi a disposizione dell'Agenzia Regionale per la Protezione dell'Ambiente della Sardegna (di seguito ARPAS o Agenzia), per finalità esclusivamente inerenti al rapporto lavorativo/contrattuale che intercorre tra ciascun utilizzatore e l'Agenzia. In tale contesto, il Regolamento codifica un insieme di regole di comportamento contenenti un quadro preciso di indicazioni per il corretto utilizzo delle suddette risorse e strumenti informatici, al fine di prevenire disservizi, tutelare la sicurezza dei sistemi, dei dati e del patrimonio agenziale, definire ambiti e modalità di utilizzo degli stessi e disciplinare le condizioni ed i limiti per il legittimo utilizzo, diffondendo altresì una cultura della sicurezza che concorra al conseguimento ed al mantenimento dei più alti livelli qualitativi dei servizi resi.

1.1.3 Le disposizioni del presente Regolamento sono improntate ai principi di diligenza, informazione e correttezza e perseguono altresì la finalità di prevenire eventuali comportamenti illeciti nell'ambito dei rapporti di lavoro da parte del personale dipendente, pur nel rispetto dei diritti ad essi riconosciuti dall'ordinamento giuridico italiano e dei provvedimenti appositamente emanati dall'Autorità Garante.

1.1.4 Non rientra tra gli scopi del presente Regolamento ed è peraltro strettamente vietato il controllo a distanza e/o in forma occulta sulle opinioni, abitudini e/o attività del personale dipendente;

1.1.5 Eventuali modifiche al presente Regolamento sono elaborate in accordo o su indicazione della Direzione Generale, sulla base dell'evoluzione tecnologica nel settore o comunque ogniqualvolta si riscontrino evidenti e documentabili esigenze tecniche o funzionali.

1.2 TITOLARE DELLE RISORSE E DEGLI STRUMENTI INFORMATICI

1.2.1 Titolare dei beni e delle risorse informatiche, dei servizi ICT e delle reti informative è l'ARPAS, legalmente rappresentata dal/la proprio Direttore/Direttrice Generale, i cui ambiti di responsabilità e competenza sono definiti dalla Legge istitutiva dell'ARPAS e dal suo Regolamento generale e di organizzazione.

1.2.2 L'utilizzo dei beni e delle risorse informatiche è consentito esclusivamente per l'espletamento delle mansioni lavorative affidate a ciascun utente ovvero per scopi professionali afferenti all'attività svolta per l'ARPAS e, in ogni caso, per l'esclusivo perseguimento degli obiettivi dell'ARPAS.

1.3 RESPONSABILE PER LA TRANSIZIONE AL DIGITALE

1.3.1 Il Responsabile per la transizione al digitale (RTD) è una figura dirigenziale, introdotta con i decreti legislativi n. 179 del 26 agosto 2016 e n. 217 del 13 dicembre 2017 di modifica al dell'Amministrazione Digitale (di seguito CAD), dotata di adeguate competenze informatiche e manageriali, nominata dal vertice politico o amministrativo, interna a tutte le pubbliche amministrazioni.

1.3.2 Il RTD è nominato con provvedimento del Direttore Generale e nello svolgimento dei suoi compiti, **risponde direttamente all'organo di vertice politico (art. 17 comma 1-ter CAD) o in assenza di questo, al vertice amministrativo dell'ente (art. 17 comma 1-sexies CAD)**. Come riportato sul sito di AgID (https://www.agid.gov.it/en/node/100373) "*il RTD ha un ruolo gerarchicamente superiore a ogni altro dirigente nell'attuazione di tutte le iniziative dell'amministrazione legate al digitale, anche per quanto riguarda pareri e verifiche. Ha poteri di impulso e coordinamento nei confronti di tutti gli altri dirigenti nella realizzazione degli atti preparatori e di attuazione delle pianificazioni e programmazioni previste dal Piano Triennale dell'Informatica. Questa figura deve essere trasversale a tutta l'organizzazione in modo da poter agire su tutti gli uffici e aree dell'ente.*"

1.3.3 L'articolo 17 del CAD definisce le caratteristiche dell'Ufficio per la transizione alla modalità operativa digitale, elencandone le funzioni e inquadrando la figura del suo responsabile. In particolare, sono attribuiti i compiti relativi a:

a) coordinamento strategico dello sviluppo dei sistemi informativi di telecomunicazione e fonia;
b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni sia esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività;
d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità;
e) analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
f) cooperazione alla revisione della riorganizzazione dell'amministrazione;
g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;

i) promozione delle iniziative attinenti all'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione;
k) pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione, al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale.

1.4 AMMINISTRATORE DI SISTEMA

1.4.1 L'ARPAS designa come Amministratore di Sistema (di seguito "AdS") uno o più soggetti, sia interni che esterni all'Agenzia, dotati di comprovate competenze specialistiche nell'ambito della tecnologia IT, incaricandoli della gestione e manutenzione degli impianti di elaborazione - compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza - con cui vengono effettuati trattamenti di dati personali.

1.4.2 L'**AdS interno** è autorizzato con atto adottato dall'ARPAS allo svolgimento delle mansioni e dei compiti assegnati, da elencarsi in maniera analitica. L'AdS interno deve autenticarsi nella propria Postazione di Lavoro (di seguito PdL) mediante le credenziali di utente standard ed utilizzare le credenziali di Amministratore solo ogni qualvolta venga richiesto dall'attività svolta.

1.4.3 L' **AdS esterno** assolve i suoi compiti in base ad un contratto di servizi. In tal caso è necessaria la stipula di un atto giuridico con cui il fornitore del servizio è nominato **responsabile del trattamento (art. 28 GDPR)**, con l'assegnazione delle specifiche funzioni affidate e l'elencazione analitica di tutte le attività che dovranno essere svolte.

1.4.4 L'AdS, sia esso interno o esterno, svolge funzioni (anche qualora non siano preposte a operazioni che implicano una comprensione del dominio applicativo) che comportano la concreta capacità di accedere, in modo privilegiato, alle risorse del sistema informativo e informatico e a dati personali e nella misura in cui sono, nelle loro consuete attività tecniche, responsabili di fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati. A mero titolo esemplificativo e non esaustivo, tali attività sono: salvataggio dei dati (backup/recovery), organizzazione dei flussi di rete, gestione dei supporti di memorizzazione, custodia delle credenziali di autenticazione e di autorizzazione, gestione dei sistemi di autenticazione e di autorizzazione.

1.4.5 I compiti dell'AdS interno, declinati nella nomina formale dello stesso in funzione dell'incarico ricoperto, possono riguardare una o più delle seguenti attività:

a) gestire l'hardware e il software di tutto il patrimonio informatico con riferimento alle risorse di cui all'art. 2.1.1;
b) gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete con riferimento alle risorse di cui all'art. 2.1.1;

c) la gestione dei privilegi di accesso sia alle risorse condivise che ai software applicativi, previamente assegnati agli utenti con riferimento alle risorse di cui all'art. 2.1.1;
d) monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, limitatamente alle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
e) gestire i log di accesso ai sistemi;
f) creare, modificare, rimuovere o utilizzare qualunque account o privilegio limitatamente alle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati con riferimento alle risorse di cui all'art. 2.1.1;
g) rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, limitatamente alle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati con riferimento alle risorse di cui all'art. 2.1.1
h) utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di prolungata assenza, non rintracciabilità o impedimento dello stesso. Tale ultima attività, tuttavia, deve essere autorizzata dal diretto Responsabile di Struttura dell'utente interessato ed essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto. L'utente deve essere informato, appena possibile, dell'evento e delle sue motivazioni.

1.5 DIRETTORI/DIRETTRICI DI STRUTTURA

1.5.1 La/Il Direttrice/Direttore di ciascuna struttura dell'ARPAS (di seguito responsabile) assicura che il personale assegnatole/gli rispetti le disposizioni del presente Regolamento in merito all'uso consentito delle risorse del sistema informativo e informatico agenziale.

1.5.2 A tal riguardo, il D.P.R. del 13 giugno 2023, n. 81, pubblicato nella Gazzetta Ufficiale n. 150 del 29 giugno 2023 ed in vigore dal 14 luglio 2023, ha modificato il "**Codice di comportamento dei dipendenti pubblici (D.P.R. n. 62/2013)**". Le modifiche sono volte a promuovere un'etica del lavoro più equa e responsabile, in conformità con i principi cardine del Codice quali i doveri fondamentali di diligenza, lealtà, imparzialità e buona condotta che gli impiegati devono osservare sia in servizio sia fuori servizio. Tali modifiche costituiscono uno specchio del crescente fenomeno di digitalizzazione del lavoro e sono state rese necessarie dall'articolo 4, comma 2, del decreto-legge 30 aprile 2022, n. 36, convertito, con modificazioni, dalla legge 29 giugno 2022, n. 79, recante «Ulteriori misure urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR)», il quale ha disciplinato l'introduzione nel Codice di misure in materia di utilizzo delle tecnologie informatiche e dei mezzi di informazione e social media. In particolare, l'articolo 11 bis del D.P.R. 62/2013 prevede che l'Amministrazione potrà, attraverso i propri responsabili di struttura, svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati. Le modalità di svolgimento di tali accertamenti sono stabilite mediante linee guida adottate dall'Agenzia per l'Italia Digitale, sentito il Garante per la protezione dei dati personali.

1.5.3 Nel caso in cui il responsabile di struttura venga a conoscenza di una violazione di sicurezza che, accidentalmente o in modo illecito, possa avere causato la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (*data breach*), provvede tempestivamente a darne comunicazione in forma scritta, adoperando i canali di comunicazione in uso in ARPAS, alla/al Direttrice/Direttore del Servizio Sistema Informativo e Informatico (di seguito SSII), per i provvedimenti consequenziali.

1.5.4 Nell'eventualità in cui all'interno della propria struttura vi siano persone con disabilità, ne dà opportuna segnalazione al servizio SSII ed al RTD, al fine di definire congiuntamente alla Direzione Generale ed a tutti i servizi coinvolti le procedure per la progettazione e l'acquisto di strumentazione hardware, software e tecnologia assistiva da mettere a disposizione.

1.6 UTENTI (DIPENDENTI E NON)

1.6.1 Gli utenti assegnatari delle risorse informatiche affidate dall'ARPAS sono personalmente responsabili del loro corretto utilizzo e della loro custodia, nonché responsabili dei relativi dati trattati per le finalità inerenti all'Agenzia. A tal fine ciascun utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'Agenzia, è tenuto a tutelare, per quanto di propria competenza, il patrimonio agenziale da:

a) utilizzi impropri e non autorizzati;
b) danni o abusi anche derivanti da negligenza, imprudenza o imperizia, segnalando tempestivamente al SSII, mediante i canali di comunicazione in uso in ARPAS;
c) eventuali attività non autorizzate;
d) situazioni anomale;
e) guasti e/o difetti di funzionamento dei dispositivi messi a loro disposizione.

1.6.2 Gli utenti, in relazione al proprio ruolo e alle mansioni in concreto svolte, operano a tutela della sicurezza informatica dell'Agenzia, riportando, tempestivamente, al loro responsabile di struttura e al SSII eventuali rischi di cui sono venuti a conoscenza ovvero violazioni del presente Regolamento.

1.6.3 I dipendenti dell'Agenzia partecipano alle iniziative di formazione e aggiornamento professionale erogate dalla Direzione Generale, con il supporto del SSII e degli altri servizi interessati, finalizzate alla conoscenza ed all'uso delle tecnologie dell'informazione e della comunicazione, nell'ottica del processo di digitalizzazione di ARPAS come, ad esempio, il Syllabus (**Direttiva del Ministro per la pubblica amministrazione 23 marzo 2023** https://www.funzionepubblica.gov.it/sites/funzionepubblica.gov.it/files/documenti/Ministro%20PA/Zangrillo/2023_marzo/Direttiva_formazione.pdf) o gli approfondimenti in materia di cybersecurity.

1.6.4 L'utente viene informato, nel rispetto del Regolamento (UE) n. 2016/679 e del successivo Decreto legislativo 101/2018, che il suo operato sulle attrezzature assegnate e il suo traffico in rete possono essere monitorati, registrati e resi disponibili all'autorità competente.

1.7 RAPPORTI TRA AMMINISTRATORI DI SISTEMA E UTENTI

1.7.1 Al fine di ottimizzare l'attività degli AdS, le richieste di intervento vanno inoltrate esclusivamente mediante il portale di helpdesk interno indicato nella intranet agenziale, ad eccezione delle segnalazioni di eventi che comportino pericolo oggettivo per persone e cose.

1.7.2 La richiesta di intervento deve essere formulata in modo chiaro e deve riportare tutti gli elementi che consentano l'esatta identificazione della problematica evidenziata.

1.7.3 La richiesta di intervento viene gestita all'interno del sistema di helpdesk che tiene traccia degli sviluppi della stessa sino alla sua chiusura.

1.7.4 Le richieste di intervento vengono gestite dagli AdS in funzione del carico di lavoro, dell'eventuale grado di rischio rappresentato dalla segnalazione e della valutazione di impatto della problematica sull'attività lavorativa dell'utente.

1.7.5 Le richieste di intervento che non rientrano tra le attività gestite dagli AdS o che necessitano una richiesta formale da effettuarsi al di fuori del sistema di helpdesk (ad es. particolari autorizzazioni da richiedersi mediante nota protocollata) non verranno gestite. In tali circostanze, gli utenti riceveranno istruzioni per la riformulazione delle richieste.

1.7.6 All'occorrenza gli AdS possono interagire con gli utenti collegandosi con la sessione di lavoro dell'utente interessato previa autorizzazione da parte dello stesso.

1.7.7 Gli AdS sono autorizzati a contattare direttamente gli utenti al proprio numero telefonico interno in casi di particolare urgenza, in casi di rischi per la sicurezza informatica, di compromissione dei dati, in caso di attività di ottimizzazione e gestione pianificate e/o quando la richiesta di intervento necessiti dell'interazione con l'utente.

1.7.8 In caso di assenza improvvisa o prolungata del lavoratore e per improrogabili necessità legate all'attività lavorativa, per le esigenze produttive agenziali o per la sicurezza ed operatività delle risorse informatiche dell'ARPAS, l'Agenzia si riserva la facoltà di accedere, redigendone verbale, a qualsiasi dotazione e/o apparato assegnato in uso all'utente per mezzo dell'intervento degli AdS (*Linee guida del Garante per posta elettronica e internet dell'1 marzo 2007*[1]), che informerà l'utente in questione alla prima occasione utile.

ART. 2 - MISURE ORGANIZZATIVE

2.1 RISORSE INFORMATICHE

2.1.1 Per Risorse e Strumenti Informatici si intendono tutte i beni informatici sia hardware che software. A titolo informativo sono risorse informatiche i server, le PdL complete di software di base ed applicativi, le apparecchiature multifunzione, le stampanti e dispositivi informatici di ogni natura (ivi compresi tablet e supporti rimovibili assegnati in dotazione). Inoltre, sono risorse informatiche i dispositivi di rete e impiantistica (cablaggi e armadi) dislocate presso tutte le

[1] in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell´attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1387522)

strutture agenziali (strutture centrali, dipartimenti territoriali e dipartimenti specialistici) nonché tutte le precedenti risorse dislocate su cloud, ivi compresi spazi di cloud storage, strumenti di videoconferenza e collaboration, database, risorse di calcolo ed applicativi specifici (ad es. software per il GIS).

2.1.2 Tali risorse costituiscono beni agenziali rientranti nel patrimonio dell'ARPAS e sono da considerarsi di esclusiva proprietà della stessa. Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle attività lavorative affidate ad ogni utente in base al rapporto in essere (ovvero per scopi professionali afferenti all'attività svolta per l'ARPAS), e comunque per l'esclusivo perseguimento degli obiettivi agenziali. Ai sensi dell'art. 11-bis (introdotto dall'art. 1, comma 1, lettera a), del d.P.R. n. 81 del 13.06.2023) comma 4 del DPR 16 aprile 2013 n. 62, *al dipendente è consentito l'utilizzo degli strumenti informatici forniti dall'amministrazione per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio*, ***purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali***.

2.1.3 Non è consentito utilizzare supporti rimovibili personali, se non preventivamente autorizzati dal SSII.

2.1.4 È onere dell'utente custodire supporti informatici contenenti dati sensibili e giudiziari in armadi o cassetti sottochiave, onde evitare che il loro contenuto possa essere trafugato, alterato e/o distrutto.

2.1.5 L'utilizzo di stampanti e/o dispositivi multifunzione (cd. fotocopiatori) deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati. È richiesta una particolare attenzione quando si inviano documenti aventi ad oggetto dati personali o informazioni riservate su una stampante condivisa; in tal caso, è opportuno evitare di lasciare le stampe incustodite: è necessario ritirare immediatamente le copie non appena prodotte dalla stampante, ciò al fine di evitare che le informazioni riportate in tali documenti possano essere visualizzate da persone non autorizzate.

2.2 CREDENZIALI DI ACCESSO

2.2.1 Per l'accesso alle risorse di cui al punto 2.1.1, l'ARPAS adotta sistemi di controllo degli accessi idonei a prevenire l'eventualità che soggetti non autorizzati possano accedere ai programmi agenziali e causare la manomissione, il furto e/o la distruzione di dati e informazioni.

2.2.2 Ove l'accesso al sistema avvenga tramite autenticazione mediante credenziali (nome utente e password), l'utente, dopo la prima comunicazione delle credenziali di autenticazione da parte degli AdS, ha l'onere di modificare, al suo primo utilizzo, la propria password. Nell'accesso ad alcuni sistemi, specialmente quelli esposti su cloud pubblico, l'utente è tenuto ad impostare un metodo di autenticazione a più fattori utilizzando la propria mail o un applicativo installato presso la postazione di lavoro; in alternativa è facoltà dell'utente utilizzare un'apposita applicazione installata sul proprio smartphone (personale o di servizio) per la ricezione di un codice mediante SMS oppure per la generazione di un codice OTP (One Time Password).

2.2.3 L'utente, nel definire il valore della password, rispetta, ove possibile, le seguenti regole:

a) utilizzare almeno dieci caratteri alfanumerici, inclusi i caratteri speciali (#, %, etc.), di cui almeno uno numerico;
b) utilizzare una combinazione che contenga almeno un carattere maiuscolo, un carattere minuscolo, un numero e un carattere non alfanumerico tipo "@#§£$%...";
c) evitare di includere nomi propri di persona, parti del nome, cognome e/o comunque elementi a lui agevolmente riconducibili;
d) evitare l'utilizzo di *password* comuni e/o prevedibili;
e) rispettare il criterio di cronologia ossia non utilizzare *password* già usate negli ultimi sei mesi;
f) proteggere con la massima cura la riservatezza della *password* ed utilizzarla entro i limiti di autorizzazione concessi.

2.2.4 Costituisce violazione del presente Regolamento, nonché condotta contraria alla legge, cedere le proprie credenziali a colleghi o collaboratori così come scrivere la password su post-it o altri supporti che espongano chiaramente le credenziali. In ogni caso resta inteso che l'utente è responsabile delle conseguenze derivanti dalla compromissione, furto o dalla perdita della propria password.

2.2.5 Nell'ipotesi di risoluzione del rapporto di lavoro/collaborazione tra l'utente e l'ARPAS, gli AdS provvedono a disabilitare le credenziali, entro un periodo massimo di 30 giorni dalla cessazione del rapporto di lavoro/collaborazione. Se l'utente è in assegnazione temporanea presso altro ente oppure è collocato in malattia o aspettativa, le sue credenziali vengono temporaneamente sospese.

2.2.6 L'utente che sospetti che le proprie credenziali di autenticazione siano state identificate da qualcuno, o sospetti di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, è tenuto a modificare immediatamente la password e a segnalare la violazione agli AdS. Nel caso in cui la violazione comporti un possibile rischio legato al trattamento dei dati personali, questa dovrà essere segnalata, entro 24 ore anche nei giorni non lavorativi, al dirigente responsabile per la gestione dei *data breach*; in ogni caso, entro il medesimo termine, il dipendente o collaboratore avvisa anche il proprio responsabile di struttura.

2.3 POSTAZIONI DI LAVORO

2.3.1 Ai sensi del presente Regolamento, per Postazione di Lavoro (PdL) si intende il complesso unitario di n.1 personal computer (di seguito, PC), n.1 monitor, n. 1 tastiera e n.1 mouse.

2.3.2 L'assegnazione delle PdL avviene a cura del SSII, con criteri legati alle necessità operative individuali ed alle disponibilità di PdL. Su specifica richiesta del Direttore generale o del responsabile di struttura, in accordo con il SSII che valuterà caso per caso, possono essere concordati criteri e priorità di assegnazione differenti da quelli generalmente applicati.

2.3.3 La PdL viene assegnata dal SSII direttamente all'utente a titolo definitivo, salvo che cause di forza maggiore ne determinino una sostituzione (ad esempio evidenti anomalie hardware non sanabili, cessazione del rapporto di lavoro, eccessiva obsolescenza, sostituzione programmata etc.); ciò

comporta che l'utente che, per ragioni di servizio, venga trasferito in altra sede, mantenga la propria dotazione di cui al punto 2.3.1 per svolgere le attività d'ufficio.

2.3.4 È onere della struttura nella quale è incardinato l'utente:

a) procedere al ritiro, presso la sede del servizio SSII, della PdL di nuova assegnazione;
b) procedere alla consegna, presso la sede del servizio SSII, della PdL in caso di manutenzione e/o sostituzione ed al successivo ritiro della stessa;
c) procedere alla riconsegna dei beni al servizio SSII in caso di cessazione del rapporto di lavoro o di comando presso altra pubblica amministrazione di un utente.

2.3.5 In caso di trasferimento di sede lavorativa sarà onere dell'utente assegnatario procedere allo spostamento della PdL, accordandosi con il SSII per le attività di riconfigurazione software e di rete connesse.

2.3.6 In caso di cessazione del rapporto di lavoro o di comando presso altra pubblica amministrazione di un utente, la PdL in disponibilità al SSII, secondo quanto indicato al punto 2.3.4, verrà ripristinata alle condizioni di fabbrica cancellando i dati presenti.

2.3.7 L'utente deve custodire la PdL con cura evitando ogni possibile forma di danneggiamento ed a conservarla nella configurazione assegnata. Pertanto, non è consentito:

a) rimuovere/aggiungere/cambiare componenti hardware e software: il SSII si riserva la facoltà di rimuovere qualsiasi elemento hardware e software la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata;
b) cambiare l'ubicazione delle apparecchiature, senza la preventiva autorizzazione del SSII;
c) cedere in uso, anche temporaneo, le attrezzature e i beni informatici agenziali a soggetti terzi;
d) disconnettere alcun elemento hardware del sistema (PC, workstation, server, stampanti, etc.) dalla rete dati senza l'autorizzazione preventiva del SSII se non in presenza di un pericolo oggettivo per le persone o le cose;
e) alterare lo stato della workstation impostata dal SSII (modifica del BIOS), resettando eventuali password o impostandone di nuove;
f) avviare la PdL con sistemi operativi diversi da quello installato dal SSII.

2.3.8 L'utente segnala con la massima tempestività agli AdS eventuali guasti, problematiche tecniche o il cattivo funzionamento delle apparecchiature.

2.3.9 LA PdL ed eventuali altri dispositivi in dotazione all'utente devono essere utilizzati con hardware e software autorizzati dall'ARPAS, in ottemperanza alle Misure minime di sicurezza ICT per le pubbliche amministrazioni (allegate alla Circolare AgID n. 1/2017 del 17 marzo 2017 - https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict)

2.3.10 Per utilizzare software o applicativi non presenti nella dotazione di base fornita, è necessaria espressa richiesta scritta dell'utente indirizzata al proprio responsabile di struttura ed al SSII; quest'ultimo, anche alla luce del quadro complessivo dell'infrastruttura informatica dell'ARPAS, ne valuterà i requisiti tecnici e l'aderenza alle policy interne prima di autorizzarne l'installazione e inserirlo nei software consentiti in Agenzia.

2.3.11 Non è consentita l'installazione o l'utilizzo di software di telecontrollo delle postazioni (a titolo esemplificativo TeamViewer, AnyDesk, etc.): ogni accesso dall'esterno della rete Agenziale deve essere autorizzato dal SSII ed avvenire tramite VPN come descritto nel punto 3.3.

2.3.12 Le PdL non devono essere lasciate incustodite con le sessioni utenti attive; pertanto, l'utente, prima di allontanarsi dalla propria PdL, attiva il blocco o la disconnessione dalla sessione corrente o eventualmente spegnerla in caso di suo perdurante inutilizzo. **Infatti, lasciare la postazione incustodita può consentirne l'utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso**.

2.3.13 Per ragioni di sicurezza informatica, non è consentito collegare dispositivi di proprietà personale dell'utente quali computer portatili, telefoni cellulari, hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali, etc. alle PdL, alle risorse informatiche e alle reti informatiche agenziali.

2.3.14 Non è consentita la memorizzazione di file audio, video, foto o qualsivoglia formato di carattere personale sul disco rigido della PdL, sulle risorse di rete o cloud e sulle unità di archiviazione esterne assegnate se non strettamente attinenti all'attività lavorativa.

2.3.15 Eventuali installazioni di software da parte dell'utente che comportino violazioni della normativa a tutela dei diritti d'autore sul software (che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore) sono sanzionate penalmente e possono determinare l'insorgere di una responsabilità amministrativa a carico dell'ARPAS.

2.3.16 Nei casi di smarrimento o furto accertato dei dispositivi assegnati o del loro contenuto, gli utenti devono segnalare tempestivamente l'accaduto ai soggetti di seguito indicati:

a) autorità giudiziaria (sporgendo denuncia);
b) responsabile della propria struttura;
c) responsabile del SSII mediante comunicazione formale.

Ove detti eventi siano riconducibili ad un comportamento negligente o imprudente dell'utente e/o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti

2.3.17 Il sistema informatico dell'Agenzia è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software di tipo minaccia informatica. Nel caso il software antivirus rilevi la presenza di una minaccia informatica, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente quanto accaduto al SSII.

2.4 GESTIONE DATI E CONDIVISIONI DI RETE

2.4.1 Si distinguono unità di archiviazione di rete condivise con la propria struttura e/o con altri utenti (cd. "*cartelle di rete*") e unità di archiviazione locale sulla PdL di ogni utente (cd. "*cartelle locali*").

2.4.2 Le *cartelle di rete* sono aree di condivisione e di archiviazione di informazioni strettamente destinate ad attività lavorative e non possono pertanto essere utilizzate per la memorizzazione di file non attinenti ad attività istituzionali. Non possono quindi essere collocati sulle *cartelle di rete* - nemmeno per periodi brevi - file personali o comunque aventi contenuto diverso da quello strettamente connesso all'attività lavorativa.

2.4.3 Per ogni *cartella di rete* è individuato un referente, avente la responsabilità di definire l'elenco degli utilizzatori e dei profili di abilitazione, nonché di verificare il corretto utilizzo della cartella da parte degli utilizzatori stessi. La richiesta di attivazione/modifica/cancellazione di una cartella di rete va inoltrata al servizio SSII, mediante protocollo, compilando l'apposito modulo disponibile sulla Intranet agenziale.

2.4.4 Per ragioni tecniche, i permessi della condivisione di rete potranno essere impostati in maniera selettiva solo sulla cartella radice e sul suo primo livello.

2.4.5 Al referente della condivisione spetta verificare periodicamente e comunque almeno annualmente, le abilitazioni assegnate agli utilizzatori, segnalando tempestivamente al servizio SSII la necessità di assegnare, modificare o cancellare l'accesso alla cartella da parte degli utilizzatori.

2.4.6 Il servizio SSII svolge periodici controlli a campione sulle cartelle di rete e può procedere autonomamente alla rimozione di dati non connessi alle attività proprie dell'Agenzia.

2.4.7 Le *cartelle locali* (Documenti e Preferiti) localizzate nel proprio profilo locale della PdL vengono sincronizzati automaticamente sul server e sono di esclusiva pertinenza dell'utente.

2.4.8 La destinazione finale dei documenti prodotti e/o memorizzati dall'utente sono le *cartelle di rete*, mentre dati e documenti ospitati sulle *cartelle locali* sono da considerarsi, anche per ragioni tecniche, limitati nello spazio e nel numero. Per ragioni di razionalizzazione delle risorse, lo spazio riservato alle *cartelle locali* (cd. *quota*) è predefinito e non estendibile salvo motivate condizioni.

2.4.9 Le *cartelle di rete* e le *cartelle locali* devono essere mantenute con diligenza a cura degli utilizzatori mediante la periodica – almeno semestrale – revisione dei dati salvati e l'eliminazione di quelli obsoleti o, comunque, non più utilizzati o necessari. È necessario evitare la duplicazione di dati onde consentire uno sfruttamento razionale delle unità di rete.

2.4.10 I server agenziali centralizzati sono le uniche entità predisposte alla condivisione di risorse. Non è consentito condividere localmente (sulla propria PdL) e direttamente dischi, cartelle o altre risorse.

2.4.11 In caso di ripristino della PdL non sono oggetto di salvataggio i dati memorizzati in posizioni differenti dalle *cartelle locali* (ad es. Desktop), dischi o altre unità di archiviazione locali (es. disco C: e D: interni). Pertanto, gli AdS non effettuano il backup di tali dati localizzati sulle PdL e non rispondono in alcun modo dell'eventuale perdita degli stessi.

2.4.12 Il servizio SSII provvede al backup dei dati ospitati sui server (completo mensile con *retention* di un anno, incrementale giornaliero con *retention* di 60 giorni). Nel caso di perdita di dati in rete, pertanto, sarà possibile richiedere il recupero del file così come salvato nell'ultima versione di backup. **Per questi motivi è obbligatorio l'utilizzo delle unità di rete per il salvataggio di file di particolare importanza e rilevanza**.

2.5 CONDIVISIONI IN CLOUD

2.5.1 Onde consentire alle strutture agenziali ed agli utenti di disporre di aree temporanee per la condivisione di dati all'esterno, non diversamente trasmissibili mediante posta elettronica o sistema di gestione documentale per il tramite della PEC, il servizio SSII valuta, dietro apposita richiesta del responsabile della struttura interessata, l'attivazione di una cartella condivisa sullo spazio di cloud storage Agenziale. Tale spazio cloud è attivato, mantenuto e gestito dal servizio SSII che ne gestisce ruoli e permessi. Le condivisioni hanno lo scopo di ospitare dati temporanei per:

a) lo scambio di dati tra dispositivi mobili in assegnazione e le postazioni di lavoro Agenziali;
b) la condivisione in sola lettura di file di grandi dimensioni.

2.5.2 Il servizio di condivisione in cloud è attivato dal servizio SSII con la formula "*as is*", ovvero rilasciato alle condizioni del fornitore originale, senza alcun tipo di garanzia in merito alla conservazione, al backup e alla disponibilità del dato, considerato che si tratta di un'area di deposito dati assolutamente temporanea. Per esigenze di contingentamento dello spazio a disposizione, già di per sé limitato, la capienza massima complessiva viene stabilita inizialmente dal servizio SSII in funzione delle esigenze della struttura interessata.

2.5.3 Le credenziali di accesso dei vari utenti verranno comunicate al responsabile della struttura interessata che risponderà del corretto utilizzo della stessa da parte dei vari membri, li sensibilizzerà sulle buone pratiche da seguire e comunicherà al servizio SSII ogni irregolarità o anomalia rilevata. Relativamente alla riservatezza e l'integrità dei file caricati, è cura e responsabilità di ciascun utente, che ne determina il livello di condivisione e utilizzo, effettuare un uso corretto della piattaforma messa a disposizione.

2.5.4 Relativamente alle condivisioni in cloud, valgono le seguenti disposizioni:

a) l'accesso alla cartella avviene, per ragioni di sicurezza, solo ed esclusivamente con autenticazione a più fattori, configurata dal servizio SSII, da realizzarsi tramite mail o applicativo installato presso la postazione di lavoro; in alternativa, è facoltà dell'utente utilizzare un'apposita applicazione installata sul proprio smartphone (personale o di servizio);
b) nella condivisione non è consentito ospitare dati sensibili ai sensi del D. Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" e successive modifiche e integrazioni, e del Regolamento EU 2016/679 (GPDR);
c) allo stesso modo, non è consentito ospitare contenuti personali e, comunque, non strettamente collegati alle attività istituzionali che dipendono dal ruolo rivestito all'interno dell'Agenzia, nemmeno per brevi periodi;
d) è obbligatorio procedere all'eliminazione dei contenuti una volta che questi sono stati condivisi e/o scaricati;
e) ogni account è associato a una persona fisica ed è perciò strettamente personale: le credenziali di accesso non possono, per nessun motivo, essere comunicate ad altre persone né cedute a terzi;

f) le utenze che non devono più accedere alla condivisione (perché ad esempio trasferite, cessate dal servizio o revocate dal dirigente responsabile) devono essere prontamente notificate al servizio SSII;
g) ogni utente ha la facoltà di cambiare in ogni momento la password di accesso;
h) non è consentito utilizzare il servizio per effettuare azioni e/o comunicazioni che arrechino danni o turbative alla rete o a terzi utenti o che violino le leggi vigenti e i regolamenti dell'Agenzia;
i) non è consentito trasmettere o condividere informazioni che possano presentare forme o contenuti di carattere inappropriato così come da Regolamenti Agenziali;
j) non è consentito caricare nella condivisione materiale che violi diritti d'autore o altri diritti di proprietà intellettuale o industriale o che costituisca concorrenza sleale così come da Regolamenti Agenziali.

2.5.5 La violazione delle seguenti disposizioni comporterà l'immediata sospensione, temporanea o permanente, dell'account associato alla condivisione. Il servizio SSII procederà alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza dei sistemi o che violi di quanto previsto dalle suddette disposizioni.

2.6 DISPOSITIVI MOBILI

2.6.1 L'Agenzia mette a disposizione, a seconda del ruolo o della funzione del singolo utente, pc portatili e tablet per determinate esigenze di servizio. Al riguardo, l'assegnazione e l'uso di tali dispositivi devono rispondere all'interesse ed alle esigenze dell'Agenzia, al miglioramento della qualità del lavoro e della produttività, alla capacità dell'Agenzia di soddisfare i bisogni nuovi della collettività, in un'ottica di efficacia, efficienza, economicità.

2.6.2 Come per qualsiasi altra dotazione, i dispositivi mobili rappresentano un bene aziendale che è dato in uso per scopi esclusivamente lavorativi.

2.6.3 Ogni utente assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e, conseguentemente, anche della sua diligente conservazione.

2.6.4 I dispositivi devono essere dotati di password di sicurezza (cd. codice PIN del dispositivo o sequenza grafica o attivazione mediante soluzioni biometriche – impronta digitale o riconoscimento facciale) che ne impedisca l'utilizzo da parte di soggetti non autorizzati; ogni utente deve adottare le necessarie e dovute cautele per assicurare la segretezza delle proprie credenziali di accesso e, qualora ritenga che un soggetto non autorizzato possa esserne venuto a conoscenza, dovrà provvedere immediatamente a cambiarla, dandone comunque comunicazione al SSII.

2.6.5 In caso di furto, danneggiamento o smarrimento del dispositivo mobile si attua quanto disposto dal punto 2.3.16. Per ragioni di sicurezza, gli AdS attueranno la procedura di *remote-wipe* (cancellazione da remoto di tutti i dati sul dispositivo), rendendo il dispositivo inutilizzabile ed i dati in esso contenuti irrecuperabili. Si attua

2.6.6 Il dispositivo viene rilasciato alle varie strutture Agenziali con impostata la configurazione definita dal servizio SSII secondo regole di sicurezza informatica e con privilegi limitati. L'eventuale

installazione di applicazioni, sia gratuite che a pagamento, deve essere espressamente autorizzata, rimanendo, diversamente, a carico dell'utente eventuali relative spese, nonché le responsabilità derivanti dall'installazione non autorizzata.

2.7 FIRMA DIGITALE

2.7.1 L'utente titolare del certificato di firma digitale è tenuto a custodire il dispositivo di firma e gli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, adottando misure organizzative e tecniche idonee ad evitare nocumento ad altri.

2.7.2 Il certificato di firma digitale è riservato e strettamente personale. A tal proposito, si rammenta a ciascun utente titolare del certificato che il PIN utilizzato per la generazione della firma deve essere custodito onde evitare l'uso da parte di terzi.

2.7.3 In caso di cessazione di un utente a qualsiasi titolo, il corrispondente certificato di firma digitale sarà revocato.

ART. 3 - NETWORKING E INTERNET

3.1 NAVIGAZIONE INTERNET

3.1.1 Ciascun utente che accede alla rete per il tramite della connettività agenziale presta particolare attenzione nell'utilizzo di Internet e dei servizi relativi, in quanto ogni operazione effettuata è associata all'"*Indirizzo Internet Pubblico*" assegnato all'Agenzia.

3.1.2 L'utilizzo della rete è consentito esclusivamente per scopi inerenti allo svolgimento dell'attività lavorativa per l'Agenzia e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative.

3.1.3 Al fine di prevenire la navigazione in siti e/o servizi web non pertinenti all'attività lavorativa, l'Agenzia adotta uno specifico sistema di blocco o filtro automatico che impedisce determinate operazioni di rete o l'accesso a determinate risorse inserite in una "*black list"*. Eventuali eccezioni a specifiche risorse web di comprovata reputazione o palesi falsi positivi sono segnalate dal responsabile di struttura al servizio SSII che, valutata la circostanza, provvede all'inserimento degli stessi nella cd. "*white list*".

3.1.4 Non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, origine etnica, opinione e appartenenza sindacale e/o politica.

3.1.5 Non è consentito lo scambio e/o la condivisione (es. i c.d. sistemi di *Peer-to-Peer*) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, etc., protetto da diritto d'autore.

3.1.6 Non è consentito configurare o utilizzare servizi di rete quali DNS, DHCP, server internet (Web, FTP), proxy server etc., diversi da quelli ufficiali gestiti dal SSII.

3.1.7 Non è consentito intercettare pacchetti sulla rete (cd. *sniffing*); conseguentemente, non è consentito l'uso di software atti a carpire, in maniera invisibile, dati personali, password e ID dell'utente, o a controllare ogni attività, ivi inclusa la corrispondenza ed i dati personali.

3.1.8 L'ampiezza di banda totale dell'Agenzia è condivisa dalle varie sedi con parametri di assegnazione stabiliti dal SSII in funzione del corretto utilizzo e della corretta ripartizione delle risorse disponibili.

3.1.9 Non è consentito utilizzare la banda disponibile in modalità esclusiva e/o in misura superiore al trend medio agenziale, effettuando download di dati, anche attinenti alle attività istituzionali, che implichino tempi di scaricamento o un consumo di banda eccessivi. Onde evitare di saturare la banda assegnata ad ogni sede dell'Agenzia, eventuali esigenze particolari andranno segnalate al servizio SSII che le valuterà caso per caso. In situazioni limite e/o pregiudizievoli per la corretta erogazione della banda disponibile, il servizio SSII procederà d'ufficio ad attuare le necessarie misure correttive di limitazione della banda.

3.1.10 In caso di abusi singoli o reiterati, il servizio SSII inoltrerà un preventivo richiamo al rispetto delle regole indirizzato a tutto il personale. Qualora, nonostante il richiamo generalizzato, l'indebito utilizzo della rete perduri, il servizio SSII procederà all'invio di avvisi più circoscritti, e – solo se a seguito della gradualità dei controlli emergano fondati sospetti – verranno allora effettuati controlli nominativi o su singoli dispositivi e postazioni.

3.2 CONNESSIONI DI RETE

3.2.1 Ogni dispositivo autorizzato ad accedere alla rete è, normalmente, collegato direttamente alla rete mediante un cavo Ethernet attestato su una borchia a muro (eventualmente tramite un telefono VoIP). La configurazione degli accessi alla rete è tale per cui detto dispositivo può funzionare solo ed esclusivamente sulla borchia a muro alla quale è collegato (cd. *port security*).

3.2.2 Non è consentito collegare il dispositivo su un'altra borchia differente da quella assegnata dal SSII.

3.2.3 Non è consentito collegare alle borchie di rete hub, switch, access point o altro dispositivo dotato di scheda di rete e/o di networking che non sia stato preventivamente autorizzato dal SSII.

3.2.4 Non è consentito creare hotspot WiFi mediante apparati o dispositivi collegati alla rete Agenziale se non installati e/o configurati dal servizio SSII.

3.3 VPN

3.3.1 Il servizio SSII gestisce il servizio di *Virtual Private Network* (di seguito VPN) che consente agli utenti e al personale esterno l'accesso alla rete Agenziale dalla rete pubblica.

3.3.2 L'accesso è strettamente personale ed è realizzato mediante autenticazione (username e password). Tali credenziali sono fornite dal servizio SSII: ogni richiesta di modifica deve essere preventivamente richiesta al servizio.

3.3.3 I dipendenti possono chiedere una VPN per accedere alla rete Agenziale da remoto, mediante nota inviata dal proprio responsabile di struttura al servizio SSII. Nella richiesta dovranno essere specificati i riferimenti del dipendente (nome, cognome, numero di cellulare e la sede lavorativa).

3.3.4 Gli utenti esterni all'Agenzia (es. fornitori) possono disporre di un accesso VPN limitatamente agli ambienti di lavoro sui quali devono operare. La struttura agenziale interessata dovrà inviare

apposita richiesta protocollata al servizio SSII specificando l'oggetto dell'attività, gli eventuali dispositivi interni coinvolti, la data di inizio e la data di fine delle prestazioni necessarie nonché i riferimenti del personale terzo (nome, cognome, numero di cellulare e nominativo della ditta esterna). Ricevuta la richiesta, il servizio SSII ne valuterà la congruità e, in caso affermativo, invierà via mail o via PEC all'utente esterno le necessarie informative sull'utilizzo della VPN e la modulistica necessaria per l'attivazione della VPN; tutta la documentazione dovrà essere restituita compilata e firmata digitalmente al servizio SSII. Terminata questa procedura il servizio SSII procederà al rilascio delle credenziali per l'accesso alla VPN.

3.3.5 Per ragioni di sicurezza, ogni accesso viene memorizzato su log di sistema che vengono conservati fino a 10 giorni per eventuali accertamenti.

ART. 4 - POSTA ELETTRONICA E SOCIAL MEDIA

4.1 ATTIVAZIONE E CESSAZIONE DELLE CASELLE DI POSTA ELETTRONICA

4.1.1 L'attivazione e cessazione della posta elettronica agenziale viene svolta dal servizio SSII mediante i propri AdS.

4.1.2 Tutti i dipendenti, a tempo determinato e indeterminato, devono possedere un account di posta elettronica (utenza). In caso di nuove assunzioni, la casella viene creata d'ufficio dal servizio SSII; le relative credenziali vengono comunicate al responsabile di struttura del nuovo dipendente.

4.1.3 Ogni casella di posta elettronica, nominativa o di servizio, è associata ad un utente che ne è responsabile.

4.1.4 L'intestatario della casella è responsabile della lettura e dell'invio dei messaggi, ed è responsabile della custodia e dell'aggiornamento della password di accesso esclusiva alla casella.

4.1.5 Account di posta servizio o impersonali dovranno essere richiesti dal responsabile di struttura al servizio SSII che ne valuterà l'attivazione. Le credenziali verranno consegnate direttamente al responsabile di struttura che ha fatto richiesta e che ne sarà a tutti gli effetti il titolare.

4.1.6 L'accesso alla posta elettronica verrà inibito quando l'utente terminerà il suo rapporto con l'Agenzia oppure cesserà la necessità della casella non nominativa. L'Agenzia non ha alcun obbligo di memorizzare o inoltrare i contenuti della posta personale in arrivo/in uscita una volta terminato il rapporto di lavoro o la collaborazione. In tali casi la casella di posta verrà resa inaccessibile all'assegnatario entro il termine massimo di 30 giorni e verrà quindi definitivamente eliminata (vedi https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9215890 - Provvedimento Garante Privacy del 4 dicembre 2019 [9215890]).

4.2 GESTIONE ED UTILIZZO DELLE CASELLE DI POSTA ELETTRONICA

4.2.1 L'accesso alla posta elettronica avviene tramite nome utente e password individuali. È responsabilità dell'utente proteggere la riservatezza delle informazioni relative alle proprie credenziali.

4.2.2 Onde incrementare il livello di sicurezza e la protezione dei dati personali, laddove implementato da parte gestore di posta elettronica, l'accesso alla casella di posta avverrà solo ed esclusivamente con autenticazione a più fattori da realizzarsi tramite applicativo installato presso la postazione di lavoro; in alternativa è facoltà dell'utente utilizzare un'apposita applicazione installata sul proprio smartphone (personale o di servizio).

4.2.3 L'utente ha l'obbligo di modificare le credenziali temporanee assegnategli in fase di creazione della casella al primo accesso.

4.2.4 L'utente deve utilizzare password di lunghezza adeguata, non inferiori a 8 caratteri maiuscoli e minuscoli oltre che numeri e caratteri speciali. Laddove il sistema non lo imponga l'utente ha l'obbligo di modificare la propria password una volta ogni 45 giorni nel caso in cui si ritenga che la propria password sia stata compromessa, l'utente deve modificarla immediatamente.

4.2.5 Per ragioni di sicurezza informatica, l'accesso alla propria casella di posta elettronica potrà avvenire esclusivamente tramite webmail.

4.2.6 Al fine di sfruttare razionalmente lo spazio disponibile per la memorizzazione dei messaggi di posta, ogni utente è soggetto a limiti di utilizzazione; il sistema avvisa l'utente all'approssimarsi del raggiungimento della quota limite impostata. Quando la quota viene superata non è più possibile inviare o ricevere messaggi fino a quando non viene liberato spazio sufficiente; in caso di trattamento di volumi di posta considerevoli, si può richiedere un giustificato e motivato aumento della dimensione della casella al servizio SSII.

4.2.7 Ai sensi dell'Art. 11-bis (introdotto dall'art. 1, comma 1, lettera a), del d.P.R. n. 81 del 13.06.2023) comma 2 del DPR 16 aprile 2013, n. 62, "*l'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'amministrazione. L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti il servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale*".

4.2.8 Ai sensi dell'Art. 11-bis (introdotto dall'art. 1, comma 1, lettera a), del d.P.R. n. 81 del 13.06.2023) comma 3 del DPR 16 aprile 2013, n. 62, "*Il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'amministrazione di appartenenza. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.*"

4.2.9 Ai sensi dell'Art. 11-bis (introdotto dall'art. 1, comma 1, lettera a), del d.P.R. n. 81 del 13.06.2023) comma 5 del DPR 16 aprile 2013, n. 62, "*è vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione*".

4.2.10 Non è consentito utilizzare la posta elettronica per scopi illegittimi o illegali, compresi violazione del copyright, oscenità, calunnia, frode, diffamazione, plagio, molestie, intimidazioni, falsificazione, furto d'identità, sollecitazioni a schemi piramidali illegali e manomissione del

computer (ad esempio diffusione di virus informatici in modo volontario o per negligenza nella gestione della casella).

4.2.11 Non è consentito divulgare, copiare o inoltrare informazioni o messaggi riservati a destinatari non autorizzati tramite il sistema di posta elettronica.

4.2.12 Non è consentito allegare al testo delle e-mail materiale potenzialmente insicuro (ad es. programmi, script, macro) così come file di dimensioni eccessive; in quest'ultimo caso potranno essere richieste al Servizio Sistema Informativo e Informatico modalità alternative, ad esempio creazione di aree dedicate o servizi in cloud.

4.2.13 Non è consentito effettuare inoltri di e-mail e/o re-indirizzamenti automatici (es. procedure di "*forward*", "*re-direct*") ad account privati sia a tutela del patrimonio dati dell'ARPAS che a tutela della sicurezza stessa.

4.2.14 Non è consentito inviare dati, documenti, progetti, disegni, materiali, informazioni dell'Agenzia riservati e qualsiasi altro contenuto protetto (e ciò anche attraverso l'inoltro di messaggi tra utenti), relativi a cittadini, fornitori, dipendenti, consulenti per motivi non strettamente inerenti allo svolgimento delle proprie mansioni.

4.2.15 Non è consentito condividere le password degli account di posta elettronica con un altro soggetto o tentare di ottenere o carpire la password dell'account di posta elettronica di un altro soggetto.

4.2.16 In caso assenza improvvisa o prolungata o per ferie l'utente deve inserire un messaggio di risposta automatica che notifichi ai mittenti il proprio periodo di assenza, la mancata lettura del messaggio ed eventuali recapiti alternativi.

4.2.17 L'utente deve apporre la seguente dicitura al fine di gestire tutti i messaggi inviati al destinatario sbagliato: "*Le informazioni contenute nella presente comunicazione e i relativi allegati possono essere riservate e sono, comunque, destinate esclusivamente al destinatario sopra indicato. La diffusione, distribuzione e/o copiatura del documento trasmesso da parte di qualsiasi soggetto diverso dal destinatario è proibita e, pertanto, l'utilizzo non autorizzato del contenuto di questo messaggio costituisce violazione dell'obbligo di non prendere cognizione della corrispondenza tra altri soggetti, salvo più grave illecito, ed espone il responsabile alle relative conseguenze. Se avete ricevuto questo messaggio per errore, vi preghiamo di distruggerlo (compresi i file allegati) senza farne copia e di informare immediatamente per telefono*".

4.3 MONITORAGGIO E RISERVATEZZA

4.3.1 Gli AdS del servizio SSII sono incaricati a fornire il supporto necessario agli utenti per ogni problema legato alle caselle di posta. L'indirizzo di posta elettronica è un dato personale e le operazioni di lettura, invio e gestione dei messaggi di posta elettronica comportano un trattamento di dati personali. Da ciò discende la necessità che, anche per quanto riguarda la posta elettronica, vengano osservati e rispettati i principi e le regole sancite dal GDPR (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE).

4.3.2 Gli AdS del servizio SSII possono operare, per specifiche esigenze di servizio o per ragioni di sicurezza informatica, sulla posta dell'utente, previo il consenso di quest'ultimo, nel rispetto delle prescrizioni del presente regolamento, del segreto professionale e secondo ogni codice deontologico e di condotta. Nonostante l'Agenzia non detenga alcun diritto di accesso attivo alle mail degli utenti, i messaggi di posta elettronica potrebbero inavvertitamente essere letti dallo staff tecnico, comunque vincolato contrattualmente alla riservatezza, durante il normale svolgimento della gestione del sistema di posta elettronica. In caso di prolungata assenza o impedimento dell'utente, che renda indispensabile ed indifferibile intervenire per esclusive necessità di lavoro o di operatività e di sicurezza del sistema, il responsabile di struttura, in qualità di fiduciario, può richiedere formalmente, attraverso richiesta scritta indirizzata anche all'interessato, che venga effettuato il reset della password dell'utente stesso. La nuova password sarà comunicata solamente al responsabile di struttura.

4.4 SOCIAL MEDIA

4.4.1 L'utilizzo dei social media (Facebook, Twitter, Linkedin, Instagram ecc.) è gestito dalla Direzione Generale per il tramite della propria Struttura preposta, per fini promozionali delle attività e degli eventi organizzati dall'Agenzia, nel rispetto di specifiche direttive ed istruzioni operative, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

4.4.2 Si riporta l'Art. 11-ter (introdotto dall'art. 1, comma 1, lettera a), del d.P.R. n. 81 del 13.06.2023) del DPR 16 aprile 2013, n. 62, (**Utilizzo dei mezzi di informazione e dei social media**):

1. *Nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla pubblica amministrazione di appartenenza.*
2. *In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'amministrazione di appartenenza o della pubblica amministrazione in generale.*
3. *Al fine di garantirne i necessari profili di riservatezza le comunicazioni, afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.*
4. *Nei codici di cui all'articolo 1, comma 2, le amministrazioni si possono dotare di una "social media policy" per ciascuna tipologia di piattaforma digitale, al fine di adeguare alle proprie specificità le disposizioni di cui al presente articolo. In particolare, la "social media policy" deve individuare, graduandole in base al livello gerarchico e di responsabilità del dipendente, le condotte che possono danneggiare la reputazione delle amministrazioni.*

ART. 5 - GESTIONE INFORMATICA DELLE STRUTTURE TECNICHE E DELLA RETE DEI LABORATORI

5.1 APPARECCHIATURE INFORMATICHE E STRUMENTI PER LO SVOLGIMENTO DELLE ATTIVITA' LABORATORISTICHE, DI CAMPO E SPECIALISTICHE TECNICHE

5.1.1 Le Strutture che svolgono attività tecnica e laboratoristica e le loro articolazioni organizzative, sono responsabili dell'acquisizione, configurazione, gestione, aggiornamento, manutenzione e fuori uso del hardware, del software e dei relativi sistemi operativi a corredo, nonché dei sistemi informativi specialistici in uso alle strutture tecniche e ai laboratori secondo quanto disposto dall'art. 6.

5.1.2 Per ragioni di sicurezza informatica, i suddetti dispositivi devono essere attestati su una rete dedicata, separata dalla rete degli uffici; la messa in rete di un dispositivo deve essere richiesta da parte del responsabile della struttura interessata al servizio SSII che effettuerà una verifica sulla compatibilità tecnica del collegamento. Effettuata questa prima valutazione il servizio SSII provvederà al collegamento in rete dell'apparecchiatura

5.1.3 Laddove richiesto dal responsabile della struttura interessata, il servizio SSII predisporrà un accesso, mediante VPN, disponendo le necessarie configurazioni che consentano all'operatore esterno, accreditato presso i laboratori, di effettuare da remoto le operazioni di installazione e configurazione dei dispositivi. L'attivazione della VPN si svolge secondo le procedure descritte nel punto 3.3.

ART. 6 - ACQUISIZIONE DI HARDWARE E SOFTWARE

6.1 Si definiscono "dotazione informatica di base assegnata in uso ad ogni singolo utente" tutti quei complementi "generalisti" funzionali ad attività non rientranti nell'ambito di convezioni, progetti specifici e attività peculiari o specialistiche di settore.

6.2 Al servizio SSII competono seguenti approvvigionamenti di hardware e software:

a) PdL (PC, monitor, tastiera, mouse, etc…) ad uso esclusivo della dotazione informatica di base assegnata in uso ad ogni singolo utente;
b) Sistemi operativi delle PdL, software di gestione, di produttività individuale e suite di collaboration ad uso esclusivo della dotazione informatica di base assegnata in uso ad ogni singolo utente;
c) hardware e software (server, apparati di networking, backup, antivirus, monitoraggio, etc..) per la gestione sistemistica del dominio unico Agenziale e funzionali al corretto funzionamento del sistema informatico dell'Agenzia;
d) servizi di posta elettronica ad uso esclusivo della dotazione informatica di base assegnata in uso ad ogni singolo utente;
e) servizi di firma elettronica ad uso esclusivo della dotazione informatica di base assegnata in uso ad ogni singolo utente;

f) servizi cloud, cloud storage e di collaboration ad uso esclusivo della dotazione informatica di base assegnata in uso ad ogni singolo utente;

g) hardware e software in ambito networking legato al sistema informatico dell'Agenzia ad uso esclusivo della dotazione informatica di base assegnata in uso ad ogni singolo utente.

6.3 In caso di acquisizione di beni e servizi informatici non rientranti nella categoria di cui al punto 6.2 ivi compresa l'acquisizione di licenze, noleggio hardware e software e manutenzione di hardware e software (sia on premise che in cloud) legati a software specialistici e sistemi informativi di competenza di una determinata struttura Agenziale, ciascuna struttura interessata all'acquisizione, per il tramite del proprio RUP o del proprio Dirigente, dovrà indirizzare una richiesta di parere tecnico-economico al RTD il quale ne valuterà la coerenza e compatibilità con l'intero sistema informativo e informatico agenziale (ai sensi dell'art. 17 del D.Lgs. 82/2005 comma lett. j-bis). Al termine della fase di valutazione il RTD rilascerà parere tecnico-economico obbligatorio e vincolante.

6.4 Nel solo caso di acquisizione di beni o servizi di natura informatica asserviti a strumentazione tecnica specifica di cui il bene/servizio informatico costituisce aspetto accessorio non prevalente, il parere tecnico-economico obbligatorio del RTD si intende non vincolante.

6.5 In caso di acquisizione di nuovi software, in ottemperanza dell'art. 68 del D. Lgs. 82/2005 e delle Linee guida su acquisizione e riuso di software per le pubbliche amministrazioni (https://www.agid.gov.it/it/design-servizi/riuso-open-source/linee-guida-acquisizione-riuso-software-pa), il RUP allegherà alla richiesta apposita valutazione comparativa delle soluzioni.

6.6 Il RTD ed il SSII forniscono, su richiesta, il necessario supporto tecnico alle strutture agenziali per gli aspetti di propria competenza, intendendosi quelli inerenti alla compatibilità con il sistema informativo e informatico dell'Agenzia, gli aspetti di cybersecurity e di interoperabilità e l'eventuale conformità al D. Lgs. 82/2005 ed alle linee guida AgID.

ART. 7 - CONTROLLI E SANZIONI

7.1 I log inerenti all'utilizzo di strumenti nonché i relativi file sono registrati e possono essere oggetto di controllo.

7.2 In caso di anomalie, gli AdS del servizio SSII, previa preventiva informazione alla struttura di riferimento, potranno effettuare controlli anonimi che si concluderanno con un avviso generalizzato indirizzato ai dipendenti del settore in cui è stata rilevata la criticità, nel quale si evidenzierà l'utilizzo irregolare degli strumenti e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

7.3 Se, nonostante l'avviso di cui al punto precedente, la situazione di anomalia persiste ed è tale da cagionare un danno all'amministrazione, potranno essere effettuati controlli su base individuale e il dipendente responsabile potrà essere segnalato al servizio di appartenenza per l'avvio dell'iter disciplinare; sono comunque vietati controlli prolungati, costanti o indiscriminati.

7.4 L’Agenzia si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare necessario al fine di proteggere l’integrità, la sicurezza e/o la funzionalità dei propri beni, dati e strumenti informatici.

REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

AGENTZIA REGIONALE PRO S'AMPARU DE S'AMBIENTE DE SARDIGNA
AGENZIA REGIONALE PER LA PROTEZIONE DELL'AMBIENTE DELLA SARDEGNA

ARPAS

Direzione Generale
Servizio Sistema informativo e informatico

Regolamento informatico dell'ARPAS

Allegato A

Normativa di riferimento, definizioni, protezione persone fisiche e trattamento dei dati personali

Ottobre 2023

Sommario

Normativa di riferimento (Regolamento)

- Codice di comportamento del personale ARPAS - art. 11 comma 6
- D.Lgs. 101/2018, disposizioni per l'adeguamento della normativa nazionale al GDPR articolo 2, comma 1 lettera f) che nel DLgs 196/2003 modificato diventa:

  articolo 2-sexies (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante), comma 2, lettera dd) *instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva*

  articolo 2 quaterdecies (Attribuzione di funzioni e compiti a soggetti designati), comma 1 *Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità* **e comma 2** *Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.*
- DECRETO DEL PRESIDENTE DELLA REPUBBLICA 16 aprile 2013 , n. 62 – "Regolamento recante codice di comportamento dei dipendenti pubblici"
- Legge 20.05.1970, n. 300 (Statuto dei lavoratori), recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento"; in particolare l'art. 4, comma 1, secondo cui la regolamentazione dell'uso degli strumenti informatici non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali;
- Regolamento Europeo 679/16 "General Data Protection Regulation" (d'ora in avanti Reg. 679/16 o GDPR); in particolare viene garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 2016/679;
- Decreto Legislativo 30.06.2003, n. 196 (Codice in materia di protezione dei dati personali);
- Linee guida del Garante per posta elettronica e internet dell'1 marzo 2007 (Gazzetta Ufficiale n. 58 del 10 marzo 2007);
- Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico del 14 giugno 2007 (Gazzetta Ufficiale n. 161 del 13 luglio 2007);
- Provvedimento del Garante del 30 luglio 2019. Il Garante ha predisposto un modello di notifica che forma parte integrante del provvedimento ed ha sancito che i termini temporali, il contenuto e le modalità della comunicazione delle violazioni di dati personali indicati nei provvedimenti

precedenti si intendono eliminati e sostituiti dai termini indicati nel GDPR e ripresi dal Provvedimento stesso.

- D.Lgs. n. 151/2015 (c.d. Jobs Act) che, l'articolo 23, modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa»;
- Codice dell'amministrazione digitale (D.lgs 7 marzo 2005 n. 82)
- Linee Guida AgID sulla Sicurezza Informatica del 07.05.2020
- Direttiva sull'utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro (Direttiva Funzione pubblica n.2 del 26 maggio 2009)
- Legge istituitiva dell'ARPAS (Legge Regionale 18 maggiuo 2996 n . 6)
- Regolamento generale e di organizzazione dell'ARPAS ai sensi dell'art. 10, comma 5, lett. e) della L.R. n. 6 del 18 maggio 2006
- Determinazione di nomina del Responsabile della Transizione Digitale ai sensi dell'art. 17 commi 1 e 1 D.Lgs n. 82/2005 (Determinazione n. 1112/2019 del 05.08.2019)
- Codice di comportamento dei dipendenti pubblici (D.P.R. del 16 aprile 2013, n. 62 modificato con D.P.R. 13 giugno 2023 n. 81)
- Ulteriori misure urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) (Decreto Legge 30 aprile 2022, n. 36 conv. in Legge 29 giugno 2022, n. 79)
- Pianificazione della formazione e sviluppo delle competenze funzionali alla transizione digitale, ecologica e amministrativa promosse dal Piano Nazionale di Ripresa e Resilienza (Direttiva 23 marzo 2023)
- Codice Civile:
    - Art. 2104 - ***Diligenza del prestatore di lavoro***: Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale. Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende.
    - Art. 2105 - ***Obbligo di fedeltà***: Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio
    - Art. 2106 - ***Sanzioni disciplinari***: L'inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo alla applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione

- Normativa in materia di diritto d'autore e di altri diritti connessi al suo esercizio introdotta con la Legge n.633/41 per la protezione delle opere dell'ingegno di carattere creativo qualunque ne sia il modo o la forma di espressione

- Normativa in materia di protezione del software introdotta con il D.Lgs. n.518/92 "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratori"; tale provvedimento normativo ha infatti aggiunto l'art. 171-bis, avente ad oggetto la tutela di programmi per elaboratori, all'art.171 della Legge n° 633/1941. L'art. 171-bis, il cui testo è stato ultimamente modificato dalla L. n°248/2000 "Nuove norme di tutela del diritto d'autore", prevede sanzioni penali a carico di coloro che duplicano, detengono, distribuiscono o vendono programmi per elaboratore oggetto di copyright; pertanto la norma pone il divieto assoluto di fare copie illegali di materiale protetto da leggi a tutela del diritto d'autore e di rendere tale materiale disponibile a terzi per effettuarne delle copie
- Legge 20 maggio 1970, n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento" (Statuto dei Lavoratori);
- Costituzione della Repubblica Italiana, art. 15 sancisce che "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge"
- Codice Penale art. 616 - Violazione, sottrazione e soppressione di corrispondenza – "Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da lire sessantamila a un milione. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni. Il delitto è punibile a querela della persona offesa. Agli effetti delle disposizioni di questa sezione, per «corrispondenza» si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza
- Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
- Decreto Legislativo 30 giugno 2003, n° 196 (mod. dal D.Lgs 24/2023) "Codice in materia di protezione dei dati personali", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali e della dignità dei soggetti a cui si riferiscono i dati, imponendo l'adozione di misure di sicurezza che riducano il rischio informatico e consentano un efficace controllo sull'utilizzo e la conservazione dei dati. Il decreto prevede un livello minimo di sicurezza per i dati personali definendo le misure fisiche, logiche e organizzative che devono essere adottate al fine di: evitare possibili distruzioni, perdite,

alterazioni di dati; garantire che l'accesso ai dati sia effettuato dalle sole persone incaricate al trattamento e quindi autorizzate; garantire che il trattamento avvenga per le finalità e nelle modalità consentite.

- Decreto Legislativo 7 marzo 2005, n° 82 - Codice dell'amministrazione digitale., il cui art. 47, comma 3, prevede che "Entro ventiquattro mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni centrali provvedono a: a. istituire almeno una casella di posta elettronica istituzionale ed una casella di posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, per ciascun registro di protocollo; b. utilizzare la posta elettronica per le comunicazioni tra l'amministrazione ed i propri dipendenti, nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.".
- Provvedimento 1° marzo 2007 del Garante per la protezione dei dati personali "Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori." (Pubblicato nella Gazzetta Ufficiale n. 58 del 10 marzo 2007).
- Circolare Agenzia per l'Italia Digitale 18 aprile 2017, n.2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)".
- Decreto Legislativo 10 agosto 2018, n° 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).", che modifica in parte il codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.
- Linee guida del Garante per posta elettronica e internet (Del. n. 13 del 1° marzo 2007 pubblicate in G.U. n. 58 del 10 marzo 2007)

Definizioni

Ai sensi del D.lgs. 196/03 e del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 intitolato "misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", si intende per:

- "**trattamento**" - qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- "**trattamento informatico**" - trattamento effettuato con l'ausilio di strumenti elettronici;

- "**dato personale**" - qualunque informazione riguardante persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- "**dati identificativi**" - i dati personali che permettono l'identificazione diretta dell'interessato;
- "**dati sensibili**" - i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- "**dati giudiziari**" - i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- "**titolare**" - la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- "**responsabile**" - la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali; in riferimento al trattamento dei dati con strumenti elettronici particolare rilevanza assume il "responsabile del trattamento dei dati informatici e telematici", di cui al punto successivo;
- "**responsabile del trattamento dei dati informatici e telematici**" (denominato D.I.T.) - per le sue specifiche competenze è identificato nel Responsabile del Servizio Sistemi Informativi. Le competenze del Responsabile di cui sopra riguardano l'attività di controllo e gestione degli impianti di elaborazione o di sue componenti, di basi di dati, di reti, di apparati di sicurezza e di sistemi software complessi (nella misura in cui consentono di intervenire su dati), l'individuazione ed attuazione di tutte le procedure fisiche, logiche ed organizzative per tutelare la sicurezza e la riservatezza nel trattamento dei dati informatici. Il Responsabile del trattamento dati informatici e telematici designa, per iscritto, gli amministratori di sistema, previa individuazione delle caratteristiche di esperienza, capacità ed affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
- "**incaricati**", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- "**amministratore di sistema**", la persona fisica dedicata alla gestione ed alla manutenzione di impianti di elaborazione o di sue componenti e tutte le figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati personali, quali gli amministratori di basi di dati, di reti informatiche, di apparati di sicurezza e di sistemi software complessi, nella misura in cui

consentano di intervenire sui dati personali; soggetti che, pur non essendo preposti ordinariamente ad operazioni implicanti una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), possono, nelle loro consuete attività, essere concretamente responsabili di specifiche fasi lavorative comportanti elevate criticità rispetto alla protezione dei dati personali. Vanno considerati a tutti gli effetti alla stregua di trattamenti di dati personali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware, anche quando non consultati "in chiaro" dall'amministratore.

- "**interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- "**utente**", soggetto che accede ed utilizza i servizi e gli strumenti del sistema informatico dell'Agenzia;
- "**comunicazione**", il dare conoscenza dei dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal Responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "**diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- "**banca di dati**", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- "**comunicazione elettronica**", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
- "**reti di comunicazione elettronica**", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento ed altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- "**rete pubblica di comunicazioni**", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al

pubblico;

- "**misure minime**", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 del Codice della Privacy;
- "**risorse informatiche**", sono annoverate tra le risorse informatiche:
    - i server;
    - le workstation, i personal computer, i notebook e qualsiasi altra tipologia di elaboratore elettronico, compresi i dispositivi mobili;
    - le stampanti, i plotter, i fotocopiatori e i fax;
    - tutti gli strumenti informatici interconnessi con la rete di ARPAS;
    - gli apparati di rete;
    - tutto il software e i dati acquisiti o prodotti da parte degli utenti o di terzi autorizzati;
    - file di qualsiasi natura, archivi di dati anche non strutturati ed applicazioni informatiche.

Ai fini del Regolamento (UE) 2016/679 e del presente Regolamento s'intende per:

- **dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **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;

- **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;
- **titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- **responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **destinatario**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- **terzo**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- **consenso dell'interessato**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- **violazione dei dati personali**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- **dati genetici**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **dati biometrici**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

- **dati relativi alla salute**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **stabilimento principale**:
  a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
  b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;
- **rappresentante**: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
- **impresa**: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
- **gruppo imprenditoriale**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- **norme vincolanti d'impresa**: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
- **autorità di controllo**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
- **autorità di controllo interessata**: un'autorità di controllo interessata dal trattamento di dati personali in quanto:
  a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
  b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

c) un reclamo è stato proposto a tale autorità di controllo;

- **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;
- **obiezione pertinente e motivata**: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
- **servizio della società dell'informazione**: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);
- **organizzazione internazionale**: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Principi generali e di riservatezza nelle comunicazioni

- I principi che sono a fondamento del presente Regolamento sono gli stessi espressi nel GDPR, e, precisamente:
  - **il principio di necessità**, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;
  - **il principio di correttezza**, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa e ciò all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regole non adeguatamente conosciute dagli interessati;
  - **i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime**, osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto

della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza".

- È riconosciuto al datore di lavoro di potere svolgere attività di monitoraggio, che nella fattispecie saranno svolte solo dall'Amministratore di Sistema, sempre nel rispetto della succitata normativa.
- Il dipendente si attiene alle seguenti regole di trattamento:
    - È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, particolari, giudiziari, sanitari o altri dati, elementi e informazioni dei quali il dipendente/collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile.
    - È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro.
    - È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni quando il dipendente/collaboratore si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti alla pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office e di ricezione di Clienti / Fornitori o colleghi di lavoro.
    - Per le riunioni e gli incontri con Clienti, Fornitori, Consulenti e Collaboratori dell'Ente è necessario utilizzare le eventuali / zone sale dedicate.
- Ogni dipendente o collaboratore che agisce sotto l'autorità del Titolare del trattamento, qualora abbia conoscenza del verificarsi di una violazione dei dati personali, avvisa, con immediatezza e comunque entro 24 ore, secondo le modalità che saranno indicate con apposita circolare di prossima pubblicazione, il Titolare del trattamento e il Dirigente Responsabile per la gestione dei *data breach*. In ogni caso, entro il medesimo termine, il dipendente o collaboratore avvisa anche il dirigente della struttura organizzativa presso la quale presta servizio.
- Sono incaricati del trattamento i dipendenti e i collaboratori che agiscono sotto l'autorità del Titolare del trattamento, i quali ai sensi dell'articolo 29 del Regolamento (UE) 2016/679 hanno accesso a dati personali e al loro trattamento previa formale designazione e dopo essere stati debitamente istruiti e formati.
- Il Titolare (o Dirigente formalmente delegato) o, in alternativa, il responsabile del trattamento, designa e nomina per iscritto gli incaricati, in numero sufficiente a garantire la gestione delle attività.
- Con l'atto di nomina, ai singoli incaricati saranno affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei beni e degli strumenti informatici. In ogni caso, prima dell'utilizzo dei beni e degli strumenti informatici, essi saranno istruiti al loro corretto uso, sulle disposizioni della normativa e regolamenti di riferimento e sul presente Regolamento.

Tutela e informazione del lavoratore e lavoratrice

- Alla luce dell'art. 4, comma 1, L. 300/1970, la regolamentazione della materia indicata nell'art. 1 del presente Regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.
- È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Regolamento (UE) n. 2016/679.
- Il presente Regolamento, nelle parti in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici aziendali, e relativamente ai trattamenti di dati personali svolti dall'Agenzia e finalizzati alla effettuazione di controlli leciti, così come definiti nell'articolo 5 del Regolamento (UE) n. 2016/679, vale quale informativa ai sensi dell'articolo 13 e dell'articolo 14 del Regolamento (UE) n. 2016/679 e del successivo Decreto legislativo 101/2018, e così come indicato dal Garante al punto 3.3 delle Linee guida del Garante per posta elettronica e internet del 1 marzo 2007 (Gazzetta Ufficiale n. 58 del 10 marzo 2007).

REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA
AGENTZIA REGIONALE PRO S'AMPARU DE S'AMBIENTE DE SARDIGNA
AGENZIA REGIONALE PER LA PROTEZIONE DELL'AMBIENTE DELLA SARDEGNA
ARPAS

Direzione Generale
Servizio Sistema informativo e informatico

Regolamento informatico dell'ARPAS
Allegato B
Buone pratiche di tenuta delle postazioni di lavoro a distanza

Ottobre 2023

Sommario

REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORATO AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale degli affari generali e della società dell'informazione
Unità di progetto Responsabile della protezione dati per il sistema Regione

BUONE PRATICHE DI TENUTA DELLE POSTAZIONI DI LAVORO A DISTANZA (REV. ARPAS)

A cura di

INNOVATORI SARDEGNA

Redazione: **Regione Autonoma della Sardegna**
Direzione generale degli affari generali e della società dell'informazione
Unità di progetto Responsabile della protezione dati per il sistema Regione
ARPAS
Servizio Sistema Informativo e Informatico
Servizio Supporti Direzionali

A cura di

INNOVATORI SARDEGNA

Sommario

1. Scopo del documento

Il presente documento, a cura della Direzione generale degli affari generali e della società dell'informazione in collaborazione con l'Unità di Progetto Responsabile per la Protezione dei Dati del Sistema Regione, adottato e rivisto nei contenuti da ARPAS, raccoglie e illustra le istruzioni di carattere generale per la tenuta delle postazioni di lavoro nell'ambito della prestazione lavorativa svolta a distanza, allo scopo di aumentare la sicurezza informatica e ridurre i rischi legati al trattamento dei dati personali. L'utilizzo di dispositivi personali o aziendali destinati a essere introdotti ed utilizzati in ambienti esterni al luogo di lavoro aumenta il rischio di smarrimento, furto o compromissione del dispositivo derivante dall'uso quotidiano privato ovvero da condotte improprie.
Ad essere trattati in modo illegittimo potrebbero essere non soltanto i dati personali contenuti nel dispositivo ma anche le credenziali di accesso ad altri sistemi, ai quali si accede di solito dal dispositivo stesso e i dati e le informazioni contenute nei sistemi informativi dell'amministrazione.
È pertanto fondamentale chiarire che l'utilizzo del proprio dispositivo debba essere il più possibile aderente alle seguenti **11 raccomandazioni di AgID per uno smart working sicuro**:

- *Segui prioritariamente le policy e le raccomandazioni dettate dalla tua Amministrazione*
- *Utilizza i sistemi operativi per i quali attualmente è garantito il supporto*
- *Effettua costantemente gli aggiornamenti di sicurezza del tuo sistema operativo*
- *Assicurati che i software di protezione del tuo sistema operativo (Firewall, Antivirus, etc.) siano abilitati e costantemente aggiornati*
- *Assicurati che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dalla tua Amministrazione*
- *Non installare software proveniente da fonti/repository non ufficiali*

- *Blocca l'accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro*
- *Non cliccare su link o allegati contenuti in e-mail sospette*
- *Utilizza l'accesso a connessioni Wi-Fi adeguatamente protette*
- *Collegati a dispositivi mobili (pen-drive, hdd-esterno, etc.) di cui conosci la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione)*
- *Effettua sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa.*

Per ulteriori approfondimenti riguardo le indicazioni fornite da AgID si può consultare il sito al seguente link:

https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/03/17/smart-working-vademecum-lavorare-online-sicurezza

Nel presente documento si approfondiscono ulteriormente alcuni degli aspetti salienti legati allo smart-working sicuro.

Prioritariamente, si richiama l'esigenza di informare tempestivamente il Titolare del trattamento in caso si venisse a conoscenza di eventi di violazione dei dati – c.d. *data breach* - secondo la procedura adottata dalla Regione Sardegna con deliberazione 21/8 del 24 aprile 2018 – disponibile al seguente link:

https://delibere.regione.sardegna.it/protected/751/0/def/ref/DBR753/

contenente le direttive recepite dall'ARPAS con Determinazione 721/2018 dell'8 giugno 2018.

Si raccomanda altresì di concordare le azioni indispensabili per un collegamento sicuro con il servizio sistema informativo e informatico, prima di utilizzare i propri dispositivi e in ogni caso per ogni chiarimento in merito all'utilizzo della postazione.

2. Destinatari del documento

Sono destinatari del presente documento i dipendenti dell'ARPAS.
Per ciascun ambito trattato, si è proceduto ad una breve analisi degli specifici aspetti di rischio riguardanti il non corretto trattamento dei dati personali e la sicurezza informatica, nonché l'applicabilità delle contromisure al contesto degli uffici regionali. In coda ad ogni scheda è stato inserito un quadro sintetico di riferimento, strutturato (ove possibile e/o pertinente) in tre punti:

- **I rischi** che l'ambito rappresenta per quanto riguarda la sicurezza e il trattamento dei dati personali;
- **I possibili rimedi attuabili a livello di ufficio** o struttura (interventi a cura dei dirigenti, degli amministratori di sistema)
- **I possibili rimedi attuabili dai singoli dipendenti** (indicazioni utilizzabili anche dagli uffici, a supporto della redazione delle singole lettere di incarico per il personale).

3. Arredi e postazione di lavoro

Un corretto allestimento degli arredi e delle postazioni di lavoro degli utenti (scrivanie, monitor, etc.) favorisce il benessere lavorativo e l'efficienza degli uffici ma è fondamentale anche per garantire una buona sicurezza informatica e un corretto trattamento dei dati personali anche presso la propria abitazione.
Pertanto, si raccomanda, di organizzare una postazione di lavoro dedicata all'interno della propria abitazione, riducendo al minimo le interferenze con altri soggetti eventualmente presenti nell'abitazione.
Nel caso in cui si posseggano diversi dispositivi personali, si raccomanda di dedicare uno di essi in via esclusiva allo smart working e di dedicare gli altri dispositivi agli usi personali.
Avendo la possibilità di accedere ai sistemi informativi dell'ARPAS, il prelievo di fascicoli cartacei contenenti dati personali e l'utilizzo di dispositivi removibili (es: chiavette USB), deve essere ridotta allo stretto indispensabile e secondo le istruzioni specifiche fornite con il presente documento.

4. Dispositivi personali

L'utilizzo di dispositivi personali nel luogo di lavoro è sempre stato fonte di perplessità e divieti, specialmente nella pubblica amministrazione. In realtà il fenomeno è in forte crescita e non a caso, dal 2016, è stato persino recepito dal legislatore con un'apposita modifica del Codice dell'Amministrazione Digitale volta addirittura a favorirlo, compatibilmente "**col rispetto delle condizioni di sicurezza nell'utilizzo**"[1]. Ciò vuol dire che se da un lato l'utilizzo di dispositivi personali deve essere incentivato al fine di facilitare il lavoro, il dialogo con i cittadini-utenti e di sfruttare i benefici, anche di risparmio, che possono derivarne per la pubblica amministrazione, dall'altro non può esserne consentito un utilizzo indiscriminato, con conseguente compromissione della sicurezza aziendale.

Considerata la particolare situazione di emergenza, si raccomandano le seguenti azioni prima di collegarsi ai sistemi aziendali con i propri dispositivi personali:

- garantire l'aggiornamento dei sistemi operativi utilizzati. Evitare l'utilizzo di sistemi operativi obsoleti quali ad esempio Windows XP e Windows 7[2];

- adottare sistemi antivirus e anti-malware aggiornati. **In particolare, verificare l'aggiornamento dell'antivirus e se possibile procedere a una scansione completa del sistema prima di procedere al primo collegamento con la rete dell'ARPAS o in ogni caso appena ricevuta notifica delle presenti raccomandazioni;**

- se possibile, utilizzare un'utenza di sistema dedicata all'attività lavorativa, differente da quella privata, senza diritti di amministratore[3];

[1] Codice dell'Amministrazione Digitale, art. 12, comma 3-bis.

[2] Si ricorda che Microsoft non fornisce più supporto per Windows 7, comprese le patch di sicurezza, a partire dal 14 Gennaio 2020.

https://support.microsoft.com/it-it/help/4057281/windows-7-support-ended-on-january-14-2020

[3] Si ricorda che è sempre una buona pratica utilizzare le utenze con privilegi elevati unicamente per compiere operazioni di manutenzione e non per l'uso quotidiano o lavorativo. Maggiori informazioni al seguente link: https://support.microsoft.com/it-it/help/4026923/windows-10-create-a-local-user-or-administrator-account

- utilizzare software libero se non si dispone dei pacchetti Office più comuni; ad esempio è raccomandabile il software *LibreOffice*, scaricabile dal sito https://it.libreoffice.org/ ;

- aumentare il grado di complessità delle password utilizzate per l'accesso al dominio e sostituirle più frequentemente;
- non consentire ad altri soggetti di utilizzare la postazione durante le sessioni lavorative, evitare la conservazione di credenziali di accesso (password, etc.…) e dati personali su post-it, agende o bloc-notes lasciati incustoditi nell'abitazione;
- non inserire documentazione di carattere personale all'interno delle cartelle condivise;
- ridurre allo stretto indispensabile lo scarico dei dati sulla propria postazione e in ogni caso eliminare definitivamente i documenti non più necessari al termine del lavoro;
- coprire videocamera e microfono del proprio dispositivo con un adesivo o un cartoncino;
- nel caso di dispositivi mobili:
    - ridurre al minimo le app installate e privilegiare l'utilizzo di quelle provenienti da aziende o sviluppatori noti;
    - verificare periodicamente le *autorizzazioni* di sicurezza concesse alle app ed eliminare le autorizzazioni non necessarie (es: https://www.androidpit.it/app-android-autorizzazioni)

Rischi:

- Accessi fisici non autorizzati, intrusioni;
- Perdita e/o manomissione di dati e dispositivi;
- Compromissione rete aziendale.

5. WI-FI e connessione a reti esterne

Un elemento di rischio abbastanza elevato è rappresentato dalla connessione dei dispositivi (d'ufficio e non) a reti di comunicazione esterne a quella dell'ARPAS, quali quelle wi-fi gratuite o le reti delle abitazioni private. L'utente dovrebbe essere consapevole che utilizzare *reti terze*, in particolare quelle pubbliche senza autenticazione, può essere particolarmente rischioso dal punto di vista dell'intercettazione dei dati, nonché può aumentare la probabilità di essere oggetto di attacchi informatici di tipo intrusivo.

In tali casi, occorre particolare cautela sia dal punto di vista tecnico che comportamentale. Riguardo i comportamenti, appare opportuno effettuare la valutazione del suo grado di sicurezza (La rete è pubblica? Il wi-fi è libero? Il protocollo è obsoleto[4]? prima di connettersi ad una rete c'è un amministratore di sistema al quale rivolgersi?) e quindi decidere se sia indispensabile collegarsi, oppure sia possibile rimandare. Occorre inoltre valutare se la sicurezza sia sufficiente per effettuare operazioni critiche (es: utilizzare servizi web dell'ARPAS, inserire credenziali di accesso, comunicare dati personali, etc..) oppure sia meglio limitarsi ad effettuare operazioni semplici quali la mera navigazione o le ricerche sul web.

Dal punto di vista tecnico, le cautele sono molteplici e consistono nell'aumentare il livello di sensibilità dei software antintrusione installati sul dispositivo utilizzato (antivirus, personal firewall, antispam, etc.), nel preferire i siti e i servizi fruibili attraverso protocolli sicuri (navigazione su HTTPS e non HTTP, connessione a server di posta tramite SSL/STARTTLS, utilizzo di SFTP, …) sino ad utilizzare connessioni in VPN.

Si raccomanda, in ogni caso, di utilizzare il collegamento ai sistemi informativi agenziali per il tempo strettamente necessario all'esecuzione dei compiti assegnati.

Rischi:

- Intercettazione di dati

[4] Il protocollo WEP, ad esempio, è considerato insicuro e non dovrebbe essere più utilizzato, così come il WPA (versione 1).

- Intrusioni sui dispositivi

Rimedi per l'ufficio:

- Dotare i dispositivi di adeguati strumenti antintrusione;
- Sensibilizzare gli utenti all'uso sicuro delle reti wi-fi;

Rimedi per gli utenti:

- Valutare sempre le caratteristiche delle reti esterne prima di connettersi;
- Verificare il grado di sicurezza delle connessioni wi-fi;
- Utilizzare preferibilmente servizi web tramite protocolli sicuri;
- Non utilizzare reti wi-fi libere per l'accesso a servizi critici dell'ARPAS.

6. Supporti di archiviazione rimovibili

L'utilizzo di supporti di archiviazione rimovibili (chiavette USB, hard disk portatili, CD, etc.) è una pratica comune che comporta diversi rischi. La sempre maggiore capienza dei supporti invoglia gli utilizzatori a memorizzarvi grandi quantità di dati senza procedere a cancellazioni. Col tempo, si tende a perdere memoria di cosa è contenuto nei supporti e l'elevata miniaturizzazione aumenta il rischio di smarrimenti. La promiscuità nell'utilizzo dei supporti fa sì inoltre che questi siano bersaglio di software malevoli (virus, malware, etc.) volti a sfruttare tali dispositivi come veicolo delle infezioni, da un PC all'altro. Infine, l'affidabilità di alcuni supporti di bassa qualità non è elevata e quasi mai nota all'utente[5].

Rischi:

- perdita di dati;

[5] Le memorie flash alla base delle diffusissime chiavette USB hanno un limite massimo di scritture dettato dalla tecnologia costruttiva (detto endurance). Raggiunto tale limite, il comportamento della memoria può essere soggetto a malfunzionamenti di varie gravità, sino renderne impossibile l'utilizzo e il recupero dei dati.

- diffusione di dati a soggetti non autorizzati (interni e/o esterni all'ARPAS);
- introduzione di software malevoli all'interno dell'ARPAS;

Rimedi per l'ufficio:

- acquistare supporti di buona qualità e dotati di meccanismi di protezione/cifratura;
- fornire agli utenti alternative pratiche all'utilizzo di tali supporti, quali cartelle condivise su server dell'ARPAS o sul cloud;

Rimedi per gli utenti:

- ridurre al minimo l'utilizzo di tali supporti;
- non utilizzare supporti rimovibili al di fuori di quelli forniti dall'ufficio;
- in mancanza di idonee chiavette USB fornite dall'ufficio, valutare l'affidabilità di quelle proprie anche attraverso una scansione per verificare la presenza di virus, limitando comunque l'inserimento di dati personali e utilizzando credenziali di accesso e adeguati strumenti di protezione dei dati;
- controllare periodicamente il contenuto dei supporti e procedere alla cancellazione dei contenuti obsoleti;
- utilizzare la rete interna dell'ARPAS per spostare grosse moli di dati;
- preferire differenti metodi di condivisione di file per la condivisione con altri utenti interni e soprattutto esterni.

7. Posta elettronica

La posta elettronica rappresenta uno dei più importanti strumenti di lavoro del dipendente soprattutto nella prima fase di gestione del lavoro a distanza.

Per quanto riguarda le caselle personali o di servizio (non PEC), nonostante sia previsto l'utilizzo delle sole caselle istituzionali[6], ancora alcuni dipendenti inoltrano la propria corrispondenza verso caselle private (es: Gmail). Tale comportamento rappresenta una violazione del Regolamento, in quanto spesso i messaggi contengono dati personali. Tali dati finiscono per essere *trattati* da soggetti esterni all'ARPAS (imprese, sistemi informatici, amministratori di sistema) privi di apposito incarico o contratto, spesso anche al di fuori del territorio UE. Si ribadisce, pertanto, il divieto di utilizzare strumenti diversi da quelli forniti dall'ARPAS o reindirizzamenti a caselle di posta personali.

Rimedi per gli utenti:

- Disattivare ogni tipo di inoltro dei messaggi di posta istituzionale su proprie caselle private o non autorizzate;
- Disattivare l'anteprima dei messaggi;
- Rispettare scrupolosamente le buone pratiche di sicurezza nell'apertura dei messaggi di posta:
  - Eliminare immediatamente messaggi di posta contenenti dati personali per i quali non si è stati incaricati del trattamento. Avvisare prontamente il mittente;
  - Verificare sempre l'attendibilità dell'indirizzo email del mittente rispetto al nome, nonché il contenuto e lo stile di scrittura dell'oggetto e del corpo dei messaggi;
  - **Attenzione in particolare in questo periodo ai falsi messaggi riguardo l'emergenza COVID-19, in quanto sono stati riscontrati tentativi di pirateria informatica (hackeraggio) utilizzando tali modalità**;
  - In caso di dubbi, non aprire immediatamente link o allegati e contattare i colleghi informatici;
- Eliminare periodicamente la posta che non deve essere archiviata;

[6] "È vietato l'uso di altre caselle e-mail per l'invio di documenti d'ufficio e per qualsiasi altra attività che si riferisca ad informazioni e dati in possesso dell'ufficio".

- Rimuovere dal server messaggi o allegati contenenti dati personali *propri* (es: buste paga), eventualmente conservandoli nel proprio PC in maniera cifrata;
- Archiviare periodicamente la posta sul proprio PC, su cartelle oggetto di backup.

8. Gestione di credenziali, password e autenticazione

Ciascun dipendente dell'ARPAS deve gestire necessariamente le proprie credenziali personali: quelle del PC e quelle per l'accesso ai sistemi informativi dell'ARPAS. In realtà il numero è molto maggiore, dato che a queste si aggiungono spesso le credenziali delle caselle di posta elettronica, degli altri sistemi informatici, nonché tutte le varie combinazioni di username, password, PIN, PUK, *passphrase* e similari di cui ognuno è in possesso.

Il problema della gestione corretta – e al contempo semplice - delle credenziali non è affatto banale; sono ormai noti i problemi derivanti dall'utilizzo di password deboli, dal riutilizzo su più sistemi delle stesse credenziali e dalla cattiva conservazione del proprio *portachiavi personale*[7]. Gli utenti andrebbero sensibilizzati costantemente anche sotto questo aspetto; si raccomanda in particolare l'utilizzo di software specializzati, quali i *password manager,* che consentono una gestione professionale delle credenziali e dispongono altresì di funzionalità strettamente integrate[8] con i sistemi operativi e i dispositivi dell'utente.

Rischi:

- Smarrimento o furto di credenziali, *phishing*[9];
- Accesso abusivo a sistema informatico.

[7] Da intendersi in senso tecnico, cioè il sistema (tipicamente un file, un'agenda, un foglio di carta) in cui vengono conservate tutte le proprie password o credenziali segrete.

[8] Auto completamento dei campi dei moduli, riconoscimento automatico delle URL, generazione sicura di password complesse, supporto di dispositivi hardware per la memorizzazione della master password, integrazione SSH, etc...

[9] https://it.wikipedia.org/wiki/Phishing

Rimedi per gli utenti:

- Attenersi alle buone pratiche per la generazione di password (non banali, robuste, etc.);
- Utilizzare metodi *sicuri* per la memorizzazione delle credenziali. Un password manager raccomandato e gratuito è KeePass (https://keepass.info/, utilizzabile su più sistemi, anche contemporaneamente, compresi i dispositivi mobili).

9. Chat e videoconferenze

Durante il lavoro a distanza è fondamentale l'utilizzo di strumenti per garantire un'adeguata comunicazione. La posta elettronica è uno di questi ma non è adatta nei casi in cui occorre interloquire in tempo reale oppure partecipare ad una riunione.

Il mercato, compreso quello del software libero, offre una grande quantità di applicazioni di chat e videoconferenza, anche su dispositivi mobili, ma non tutte sono adatte alle esigenze di riservatezza di una pubblica amministrazione. Pur disponendo del sistema di videoconferenza agenziale Lifesize, attivabile su richiesta al servizio Sistema Informativo e Informatico, si raccomanda pertanto particolare cautela nell'utilizzo di strumenti provenienti da fonti non autorevoli o di dubbia affidabilità.

Si raccomanda inoltre di prestare attenzione al fatto che la comunicazione avvenga su canali cifrati, possibilmente in modalità *end-to-end* [10], in quanto è sempre concreto il rischio di intercettazione, da parte di terzi non autorizzati, del contenuto delle conversazioni e dei messaggi scambiati. Ciò è ancora più importante nel caso in cui si vogliano comunicare delle credenziali di autenticazione ai sistemi (cosa che andrebbe comunque fatta in maniera multicanale: es: trasmissione della username via chat/posta e della password via telefono).

Infine, in particolare per le chat, si ricorda sempre la possibilità che parte dei contenuti scambiati permanga sulle memorie dei dispositivi (temporanee e non). Pertanto, appare

[10] https://it.wikipedia.org/wiki/Crittografia_end-to-end

non raccomandabile utilizzare tali strumenti per lo scambio sistematico di documenti, per i quali sono più adatti altri canali.

Rischi:

- Accesso o lettura da parte di terzi alle comunicazioni scambiate;
- Permanenza nelle memorie dei dispositivi di informazioni o documenti riservati;
- Utilizzo di software non affidabili, non sicuri o addirittura portatori di software malevolo.

Rimedi per gli utenti:

- Utilizzare soluzioni di chat e videoconferenza note e affidabili;
- Utilizzare soluzioni che garantiscano riservatezza e la cifratura *end-to-end* della comunicazione. In particolare, si suggerisce l'uso dell'App *Signal*, al posto di WhatsApp[11];
- Utilizzare le chat come modalità di comunicazione veloce / occasionale, ma non per lo scambio sistematico di documenti, magari riservati;
- Evitare o ridurre al minimo la trasmissione di credenziali di autenticazione (nome utente, password, pin, etc.) su canali non sicuri. In ogni caso, separare le credenziali su più canali di trasmissione.
- Utilizzare periodicamente programmi di pulizia dei file temporanei dei dispositivi.

10. Cartelle condivise

Le cosiddette “cartelle condivise”, utilizzate come luogo di memorizzazione e scambio dei documenti digitali, sono uno strumento di lavoro divenuto oramai comune all’interno

[11] La stessa Commissione Europea ha raccomandato al proprio staff l'uso dell’App *Signal* al posto di *WhatsApp*. Analoga decisione è stata emessa dall'Organizzazione delle Nazioni Unite.

dell'ARPAS. Grazie al collegamento in desktop remoto, gli utenti impegnati nel lavoro a distanza possono accedere alle cartelle condivise mediante la propria postazione collocata fisicamente nella sede di lavoro.

Tuttavia, tali cartelle, per quanto comode nell'utilizzo, pongono alcuni rischi legati alla sicurezza e al trattamento non corretto di dati personali.

Quanto detto assume ancora più rilevanza nel caso di documenti contenenti dati personali, per i quali debbono essere garantite tutte le misure di sicurezza e di conservazione previste dalle norme di settore.

Senza un forte controllo dell'organizzazione e dei contenuti delle cartelle stesse, al crescere dei volumi è facile perdere contezza di quanto in esse memorizzato. Questa situazione, ad esempio, impedisce di soddisfare correttamente le eventuali richieste di cancellazione di dati personali[12], oltre che di rispettare le prescrizioni in materia di *scarto* dei documenti digitali.

Un altro aspetto complicato delle cartelle condivise è la gestione dei permessi di accesso. Dando per scontato che sia totalmente fuori norma fornire a tutti i dipendenti dell'ufficio un accesso indiscriminato ai documenti contenenti dati personali, si evidenzia come sia molto oneroso gestire i permessi di accesso nelle cartelle condivise, a seconda del grado di riservatezza, del grado di coinvolgimento nei procedimenti, degli incarichi assegnati e della normale rotazione dei dipendenti negli uffici; pertanto si rischia molto facilmente di intercorrere in errori o di cristallizzare nelle cartelle situazioni organizzative ormai obsolete.

Le cartelle condivise andrebbero dunque utilizzate principalmente per lo scambio temporaneo di documenti in bozza, o per la memorizzazione di copie di file di lavoro troppo grandi per essere continuamente acceduti attraverso il sistema documentale dell'Agenzia Urbi (es: planimetrie, immagini, etc..). Andrebbero inoltre sottoposte a periodico svuotamento, anche forzato, della cui schedulazione dovrebbero essere

[12] Art. 17 del GDPR: *"L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti* [...]*"* (seguono motivi)

informati tutti gli utenti. Nei casi in cui si trattino dati di natura particolare, è necessario utilizzarle in accoppiata alle tecniche di cifratura.

Rischi:

- Accesso incontrollato a documenti contenenti dati personali;
- Cancellazione (o mancata cancellazione) di documenti contenenti dati personali;
- Difficoltà negli adempimenti legati all'esercizio dei diritti dei cittadini in materia di dati personali.

Rimedi per l'ufficio:

- Mantenere uno stretto controllo dell'organizzazione e dei contenuti delle cartelle condivise;
- Impostare un adeguato controllo degli accessi e delle autorizzazioni sui singoli file e cartelle;
- Prevedere un periodico svuotamento delle caselle, con tempistiche e modalità note agli utenti;

Rimedi per gli utenti:

- Utilizzare quanto più possibile il *workflow* del protocollo informatico dell'Agenzia per la creazione dei documenti digitali; utilizzarne la fascicolazione elettronica e la conservazione a norma;
- Verificare periodicamente i propri file nelle cartelle condivise ed eliminarli se non più necessari;
- Cifrare eventuali file contenenti dati personali che possono essere acceduti da soggetti non autorizzati.

12. Cloud e condivisione di documenti digitali

Il successo e la facilità d'uso delle tecnologie *cloud*, il basso costo, nonché la possibilità di fruizione da più dispositivi, hanno fatto sì che servizi quali *Google Drive*, *Dropbox* e similari siano sempre più utilizzati per l'archiviazione o lo scambio di documenti all'interno e verso l'esterno degli uffici.

Tuttavia, analogamente a quanto già osservato per servizi come *Gmail* (vedasi par. 8 – Posta elettronica) si ricorda che utilizzare tali strumenti senza accorgimenti, in mancanza di un contratto o di uno specifico accordo di servizio stipulato dall'ARPAS, non è raccomandabile, se non addirittura illegittimo, in particolar modo quando vengono trattati dati personali. I servizi cloud vengono infatti erogati da *data center* quasi sempre al di fuori del perimetro di controllo dell'ARPAS o della stessa Unione Europea, e sono oggetto di politiche di gestione decise in autonomia dal fornitore sia per quanto riguarda la regolamentazione (disponibilità, sicurezza, scarico di responsabilità in caso di danni, etc.) che le misure sui dati (backup, tempi di conservazione, etc.).

Gli utenti sono quindi tenuti a utilizzare strumenti di condivisione gestiti dall'ARPAS, o da fornitori sotto contratto. Ad esempio, le già citate cartelle condivise (per la condivisione di documenti all'interno della rete regionale), o la posta elettronica (per la condivisione con l'esterno, nei casi autorizzati). In casi di assoluta necessità può essere consentito l'utilizzo di servizi cloud differenti, a patto di adottare adeguate misure di sicurezza, come ad esempio la cifratura dei dati prima di caricarli.

Si ricorda inoltre che dal 1° gennaio 2019 tutte le Amministrazioni hanno l'obbligo di approvvigionarsi di servizi cloud unicamente da "fornitori qualificati", secondo la procedura formale prevista da AgID[13] e che pertanto ogni altro tipo di ricorso a cloud di terzi, al di fuori di tali regole, appare ancor più fuori norma.

Rischi:

[13] Il Cloud della PA: https://cloud-pa.readthedocs.io/it/latest/

- Impossibilità di rispettare i diritti degli interessati;
- Indisponibilità dei servizi e dei dati;
- Trattamento dati personali da parte di soggetti non autorizzati;

Rimedi per l'ufficio:

- Informare adeguatamente gli utenti riguardo i rischi e i divieti del memorizzare dati personali su sistemi cloud non autorizzati;
- Fornire strumenti adeguati alle esigenze dei dipendenti in materia di condivisione dei documenti informatici;
- Utilizzare solo fornitori e servizi cloud qualificati da AgID;

Rimedi per gli utenti:

- Limitare l'utilizzo dei servizi cloud allo stretto necessario;
- Non utilizzare servizi cloud non autorizzati per memorizzare dati personali. Nei casi in cui ciò è strettamente necessario, procedere a cifrare i documenti (o rimuovere i dati personali) prima di caricarli sul cloud.

Autori

Iniz.	*Nome e cognome*	*Struttura di appartenenza*	*Note*
AI	Dott. Alessandro Inghilleri	Unità di progetto Responsabile della Protezione Dati per il Sistema Regione	Redazione Revisione
FG	Ing. Fabrizio Gianneschi	Unità di progetto Responsabile della Protezione Dati per il Sistema Regione	Redazione
PB	Ing. Pierluigi Buttu	Servizio Agenda Digitale	Redazione
SC	Ing. Simone Cugia	Servizio delle Infrastrutture Tecnologiche	Revisione
NS	Ing. Nicoletta Sannio	Servizio dei Sistemi Informativi di Base e Applicativi del Sistema Regione	Revisione
FM	Dott.ssa Francesca Murru	Servizio Agenda Digitale	Revisione
RP	Ing. Riccardo Porcu	Direzione Generale degli Affari Generali e della Società dell'Informazione	Approvazione
GC	Dott. Giuseppe Corda	Servizio Sistema Informativo e Informatico	Revisione
PG	Dott. Paolo Garau	Servizio Sistema Informativo e Informatico	Revisione
CS	Dott. Carmine Sau	Servizio Supporti Direzionali	Revisione
AM	Ing. Andrea Morgera	Servizio Sistema Informativo e Informatico	Approvazione