Autorità di Sistema Portuale del Mar Adriatico Settentrionale

Regolamento per l'utilizzo dei Sistemi Informatici e di Telecomunicazione

Sommario

Premessa 6
1. Riferimenti normativi 9
2. Oggetto e finalità 11
3. Definizioni e Acronimi 13
4. Principi generali 15
5. Tutela del lavoratore 16
6. Gestione degli accessi 17
6.1 Gestione, assegnazione e revoca delle credenziali di accesso 17
6.2 Autenticazione multifattoriale (MFA) 19
6.3 Privilegi e separazione dei ruoli 19
6.4 Gestione delle utenze nelle postazioni specialistiche e negli ambienti segregati 20
6.5 Tracciamento e conservazione dei log di accesso 20
7. Infrastruttura di rete e Filesystem 21
7.1 Connessione sicura 23
7.2 Accesso da ambienti segregati 24
7.3 Utilizzo dei dati negli ambienti segregati 24
7.4 Monitoraggio e Logging 25
8. Utilizzo degli Strumenti 25
8.1 Dispositivi BYOD (Bring Your Own Device) 27
8.2 Aggiornamenti e patch obbligatorie 28
8.3 Monitoraggio e Logging 28
9. Internet e navigazione sicura 29
10. Utilizzo della Posta Elettronica 30
10.1 Trattamento dei metadati 33
10.2 Gestione della casella di Posta Elettronica e conservazione dei messaggi 34

11. Strumenti di messaggistica 35
12. Partecipazioni a Social Media 36
13. Telefoni, fotocopiatrici, scanner, stampanti e plotter 37
14. Assistenza agli utenti e manutenzioni 38
15. Sicurezza dei Dati 39
15.1 Ambiente Cloud oppure On-premise 40
15.2 Sicurezza delle applicazioni 40
16. Gestione incidenti 41
16.1 Segnalazione tempestiva 41
16.2 Data Breach 42
17. Controlli sugli Strumenti 42
17.1 Principi e presupposti 42
17.2 Tipologie di controllo 43
17.3 Separazione dei ruoli 43
17.4 Procedura dei controlli individuali 44
17.5 Accesso a posta elettronica, Teams, file e dispositivi 44
17.6 Utilizzo e conservazione delle evidenze 44
18. Conservazione dei dati 45
19. Sanzioni e norme finali 45

Premessa

Si specifica che tutti gli strumenti utilizzati dagli utenti, intendendo con ciò: PC, notebook, tablet, smartphone, kit di firma digitale, e-mail ed altri strumenti ICT con relativi software e applicativi (di seguito più semplicemente "Strumenti Informatici", "Strumenti" o "Servizi ICT"), sono messi a disposizione dall'Autorità di Sistema Portuale del Mare Adriatico Settentrionale (di seguito anche "ADSPMAS") al fine di consentire lo svolgimento delle mansioni lavorative.

Gli Strumenti Informatici, nonché le relative reti alle quali è possibile accedere tramite gli stessi, sono domicilio informatico di ADSPMAS. Nell'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo dell'Ente, l'utente è tenuto ad usare la massima diligenza, nel rispetto degli obblighi di cui agli **articoli 2104 e 2105 del Codice civile**. Gli strumenti, le reti e le banche dati possono essere utilizzati esclusivamente per ragioni di servizio. Qualsiasi uso non conforme può comportare gravi rischi alla sicurezza ed alla integrità dei sistemi informativi dell'Ente, essere suscettibile di valutazione ai sensi della normativa di cui al CCNL e, in casi gravi, assumere rilevanza anche sotto il profilo penale.

Le precauzioni di tipo tecnico predisposte dall'Ente possono proteggere le informazioni durante il loro transito fra i sistemi della rete locale e quando queste risiedono sul server. Nel momento in cui esse raggiungono fisicamente la postazione dell'utente finale, la loro protezione dipende esclusivamente da quest'ultimo.

L'Ente si impegna a garantire a tutti gli incaricati un adeguato aggiornamento in merito ai rischi, alle procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati tramite l'utilizzo di strumenti informatici e dell'infrastruttura digitale dell'Ente.

Ogni utente è tenuto a rispettare il presente Regolamento, che è reso disponibile tramite le modalità specificate al capitolo 19.

I dati personali e le altre informazioni riferibili agli utenti, generati o registrati mediante gli Strumenti Informatici, sono trattati esclusivamente per finalità determinate e legittime, connesse a esigenze organizzative e produttive, sicurezza del lavoro, tutela del patrimonio e sicurezza dei sistemi. L'eventuale utilizzo delle informazioni per finalità connesse al rapporto

di lavoro è ammesso soltanto quando i dati siano stati raccolti nel rispetto dell'art. 4 della legge n. 300/1970, dell'informativa resa agli interessati, della normativa in materia di protezione dei dati personali e dei principi di necessità, proporzionalità, pertinenza, minimizzazione e limitazione della conservazione.

Le prescrizioni di seguito previste integrano le istruzioni impartite alle persone autorizzate al trattamento ai sensi dell'art. 29 del Regolamento (UE) 2016/679 e dell'art. 2-quaterdecies del D.Lgs. 196/2003, nel quadro delle seguenti fonti normative e regolamentari:

- *Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, "General Data Protection Regulation" (GDPR)*;
- *D. Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", che contiene la disciplina rilevante in materia di privacy, come modificato dal Decreto legislativo 10 agosto 2018, n. 101*;
- *Provvedimenti del Garante per la protezione dei dati personali in materia di "misure di sicurezza", in particolare con riguardo agli Amministratori di Sistema (Provvedimento generale del 27 novembre 2008, successivamente modificato dal Provvedimento del 12 febbraio 2009 [1598443] e del 25 giugno 2009)*;
- *Direttiva (UE) 2022/2555 (NIS2) del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148;*
- *Decreto Legislativo 4 settembre 2024, n. 138, che recepisce sul suolo nazionale la Direttiva NIS2;*
- Nonché le informazioni già fornite in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

La Direzione dell'Ente, in ottemperanza agli obblighi previsti dal *Decreto Legislativo n. 138/2024*, che recepisce in Italia la *Direttiva Europea NIS 2 (Direttiva (UE) 2022/2555)*, e in linea con i principi di sicurezza delle informazioni previsti dallo standard *ISO 27001:2022,* assume la responsabilità diretta della supervisione e dell'attuazione delle misure di sicurezza

organizzative, fisiche e tecnologiche necessarie alla protezione del patrimonio informativo, approvando il presente Regolamento e garantendo le risorse necessarie per la sua applicazione.

1. Riferimenti normativi

ADSPMAS si impegna a garantire la conformità a tutte le normative vigenti e alle loro evoluzioni, ai requisiti contrattuali e ispirandosi agli standard internazionali applicabili in materia.

Di seguito si riportano Leggi, Regolamenti e Standard che sottendono alla definizione dei processi e delle misure di sicurezza adottate con il presente Regolamento.

- *Legge 20.5.1970, 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";
- Decreto Legislativo 14 settembre 2015, n. 151, che ha modificato l'art. 4 dello Statuto dei Lavoratori in materia di controlli a distanza;
- *Regolamento Europeo 679/2016 "General Data Protection Regulation*" (GDPR);
- *Linee guida AgID* sulla formazione, gestione e conservazione dei documenti informatici, nonché alle ulteriori *disposizioni AgID in materia di sicurezza informatica e gestione dei log applicabili alle pubbliche amministrazioni*;
- *Linee guida del Garante per posta elettronica e internet,* pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- *Direttiva (UE) 2022/2555* (NIS2) e Decreto Legislativo 4 settembre 2024, n. 138;
- Standard *ISO/IEC 27001:2022* e relativi controlli di sicurezza come stabili all'interno dell'*Annex A;*
- Linee guida *NIST SP 800-63 (Digital Identity Guidelines)* e controlli di sicurezza previsti da NIST SP 800-53 *(Security and Privacy Controls for Information Systems and Organizations)*;
- *Piano Triennale per l'Informatica nella Pubblica Amministrazione*.

Alla luce dell'*articolo 23 del D.lgs. n. 151/2015* (*c.d. Jobs Act*) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, e tenuto conto dell'evoluzione degli strumenti digitali utilizzati nell'ambito lavorativo, il presente Regolamento disciplina le modalità di utilizzo degli Strumenti Informatici e telematici messi a disposizione dell'Ente. La finalità è quella di promuovere una corretta "cultura informatica", affinché l'utilizzo degli Strumenti Informatici e telematici dell'Ente avvenga esclusivamente per le finalità istituzionali

e operative previste, nel rispetto delle disposizioni normative vigenti, dei principi di sicurezza e delle regole organizzative adottate dall'Ente. Si vuole fornire a tutto il personale le indicazioni necessarie al fine di evitare il verificarsi di qualsiasi abuso o uso non conforme, mitigando il rischio di sicurezza associato allo scorretto utilizzo degli Strumenti informatici.

2. Oggetto e finalità

Il presente Regolamento intende fornire le indicazioni per una corretta e adeguata gestione degli Strumenti informatici, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente e si applica a tutti gli utenti intesi come:

- i dipendenti (senza distinzione di ruolo e/o livello);
- i collaboratori e consulenti dell'Ente a prescindere dal rapporto contrattuale con lo stesso intrattenuto (lavoratori somministrati, collaboratori coordinati e continuativi, in stage, prestatori d'opera Intellettuale, ecc.), che venissero autorizzati a far uso di strumenti tecnologici dell'Ente o di accedere alla rete informatica dell'Ente e ad eventuali dati ed informazioni ivi conservati e trattati.

Pertanto, le regole di seguito previste devono intendersi a carico tanto dei primi quanto dei secondi, ferma restando la condizione che si dia opportuno conto del presente Regolamento negli accordi contrattuali presi con le parti.

Si specifica, infine, che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati *hardware* o strumenti *software* aventi come scopo il controllo a distanza dell'attività dei lavoratori.

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".

Le attività di monitoraggio sono disposte dall'Autorità secondo le competenze e le garanzie definite al capitolo 17 del presente Regolamento. Il Responsabile Area ICT e MEPA, o il personale formalmente autorizzato, svolge esclusivamente l'esecuzione tecnica dei controlli, senza autonomo potere di disporre controlli individuali, salvo gli interventi tecnici urgenti necessari a contenere un rischio imminente per la sicurezza dei sistemi, soggetti a immediata tracciatura e successiva comunicazione al Segretario Generale.

Tutti gli interventi sono finalizzati a garantire la confidenzialità, l'integrità e la disponibilità delle informazioni dell'Amministrazione. In particolare: la confidenzialità o riservatezza riguarda la

conoscibilità e fruibilità delle informazioni ai soli soggetti autorizzati; l'integrità è relativa alla completezza ed inalterabilità delle informazioni; la disponibilità concerne l'accessibilità ed usabilità delle informazioni nel tempo da parte dei soggetti autorizzati. La finalità è, altresì quella di garantire l'integrità e la disponibilità anche dei beni materiali dell'Amministrazione.

3. Definizioni e Acronimi

AgID (Agenzia per l'Italia Digitale)	Agenzia tecnica della Presidenza del Consiglio che garantisce la realizzazione degli obiettivi dell'Agenda digitale italiana coordinando tutte le amministrazioni del Paese.
Backup	Copia di dati e sistemi per garantirne il ripristino in caso di perdita, guasto o incidente.
BCC/CCN (Blind Carbon Copy/Copia Carbone Nascosta)	Modalità di invio e-mail che consente di inserire destinatari nascosti agli altri.
Blacklist	Elenco di indirizzi, domini o IP bloccati per motivi di sicurezza.
BYOD (Bring Your Own Device)	Uso di dispositivi personali sul lavoro.
CCNL	Contratto Collettivo Nazionale di Lavoro.
CIE (Carta d'Identità Elettronica)	Carta d'identità elettronica.
Cyber Hygiene	Pratiche di base per mantenere la sicurezza informatica.
Database	Sistema organizzato per archiviare, gestire e recuperare dati in modo strutturato.
DPO (Data Protection Officer)	Figura responsabile della supervisione della conformità alla normativa sulla protezione dei dati all'interno di un'organizzazione.
Freeware/Shareware	Software gratuito o a prova limitata
GDPR (General Data Protection Regulation)	Regolamento Generale sulla Protezione dei Dati dell'Unione Europea.
Guestbook	Registro digitale per raccogliere dati di accesso a servizi da parte di visitatori o utenti.
ICT (Information and Communication Technology)	Tecnologie e sistemi per la gestione e trasmissione delle informazioni, inclusi hardware, software, reti e servizi digitali.
ISO/IEC 27001:2022	Standard internazionale per la gestione della sicurezza delle informazioni (Information Security Management System, ISMS).

Least Privilege	Principio di sicurezza che limita i privilegi di utenti e processi al minimo necessario per svolgere le loro funzioni, riducendo il rischio di compromissione o abuso dei sistemi.
MFA (Multi-Factor Authentication)	Metodo di autenticazione che richiede due o più fattori distinti per verificare l'identità di un utente, aumentando la sicurezza rispetto alla sola *password*.
MTA (Mail Transfer Agent)	Software che gestisce l'invio e la ricezione delle e-mail tra server (es. Postfix, Sendmail).
MUA (Mail User Agent)	Applicazione utilizzata dall'utente per leggere e inviare e-mail (es. Outlook, Thunderbird, webmail).
NIS2	Direttiva europea sulla sicurezza delle reti e dei sistemi informativi, che sostituisce la precedente NIS (2016).
NIST (National Institute of Standards and Technology)	Ente statunitense che definisce standard e linee guida per la sicurezza informatica e lo sviluppo sicuro del software.
OWASP (Open Web Application Security Project)	Progetto internazionale che fornisce linee guida e best practice per la sicurezza delle applicazioni, incluso l'OWASP Top Ten.
PEC (Posta Elettronica Certificata)	Sistema di posta elettronica che garantisce la trasmissione sicura e certificata dei messaggi.
Phishing	Tecnica fraudolenta che consiste nell'inviare mail o messaggi ingannevoli al fine di ottenere dati sensibili (es. credenziali).
Proxy	Server o servizio che funge da intermediario tra un client e la risorsa a cui vuole accedere (ad esempio un sito web), inoltrando le richieste e le risposte.
Re-hosting	Migrazione di sistemi.
Repository	Archivio centralizzato per conservare e gestire file, codice o documentazione, spesso con controllo delle versioni.
Separation of Duties	Separazione di ruoli e responsabilità.
SLA (Service Level Agreement)	Accordo che definisce i livelli di servizio garantiti da un fornitore, come disponibilità, tempi di risposta e performance del servizio.
SPID (Sistema Pubblico di Identità Digitale)	Sistema che consente ai cittadini e alle imprese di accedere ai servizi online della Pubblica Amministrazione e dei privati aderenti tramite un'identità digitale unica.

SUA	Sportello Unico Amministrativo.
User/Utente	Utente del Sistema Informativo.
VPN (Virtual Private Network)	Tecnologia che crea un canale di comunicazione sicuro e cifrato tra dispositivi e reti, garantendo riservatezza e integrità dei dati trasmessi.

4. Principi generali

I principi che sono a fondamento del presente Regolamento sono gli stessi espressi nel GDPR, e, precisamente: a) 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 (*art. 5 e 6 del Reg. 679/16*); b) i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (*art. 5 commi 1 e 2*), osservando il principio di pertinenza e non eccedenza. In questo modo, il presente Regolamento vuole garantire la sicurezza dei tre pilastri delle informazioni e dei sistemi, ovvero Riservatezza, Integrità e Disponibilità (RID).

La Riservatezza implica che i dati siano accessibili solo a persone autorizzate; l'Integrità richiede che i dati e i sistemi non vengano alterati in modo non autorizzato; la Disponibilità garantisce che le informazioni e i servizi siano sempre fruibili quando necessario. Ciò significa che i dati devono essere trattati solo quando è strettamente necessario, per finalità chiare e legittime, evitando ogni utilizzo al di fuori degli scopi previsti.

Ogni utente è responsabile del corretto utilizzo degli strumenti e della protezione delle informazioni contenute negli stessi. A tal fine, l'utente si attiene alle seguenti regole generali di trattamento:

- È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni dei quali l'utente 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 autorizzato o meno a riceverli, mediante richiesta preventiva al proprio Responsabile di Area;
- È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, database e quant'altro;

- È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni quando l'utente 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.

Per garantire l'integrità e la disponibilità dei dati e dei sistemi, gli utenti sono inoltre tenuti a:

- Segnalare tempestivamente eventuali anomalie o sospette alterazioni;
- Non ostacolare l'accesso ai sistemi critici e rispettare le procedure di backup e continuità operativa;
- Utilizzare esclusivamente canali e strumenti autorizzati da ADSPMAS per la trasmissione di informazioni.

5. Tutela del lavoratore

Alla luce dell'*art. 4, comma 1, L.n. 300/1970*, la regolamentazione della materia 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 Reg. 679/16*.

6. Gestione degli accessi

6.1 Gestione, assegnazione e revoca delle credenziali di accesso

6.1.1 Attivazione nuova utenza

Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dal Responsabile Area ICT e MEPA contestualmente all'o*n-boarding* del dipendente, o comunque su formale richiesta del Responsabile dell'Area nell'ambito della quale verrà inserito ed andrà ad operare il nuovo utente. Le richieste di attivazione nuova utenza devono essere presentate tramite E-mail al Responsabile Area ICT e MEPA con in copia per conoscenza il RTD ed il Direttore responsabile dell'interessato.

Nel caso di attivazione utenza per collaboratori esterni la richiesta dovrà essere inoltrata al Responsabile Area ICT e MEPA direttamente dalla Direzione o dal Responsabile dell'Area con il quale il collaboratore si coordina nell'espletamento del proprio incarico.

La richiesta di attivazione delle credenziali dovrà essere completa di:

a) Nome,

b) Cognome,

c) Codice fiscale,

d) Numero di telefono,

e) Elenco di risorse per le quali deve essere abilitato l'accesso.

Ogni successiva variazione delle abilitazioni di accesso dovrà essere formalmente richiesta al Responsabile Area ICT e MEPA, previa approvazione del Responsabile di riferimento.

A ciascuna utenza corrisponde una credenziale di accesso che consiste in un codice per l'identificazione dell'utente (altresì nominati *username*, nome utente o *user-id*), ed una relativa *password*. La *password* è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza senza divulgarla.

A seguito del primo accesso, la *password* deve essere cambiata con una a scelta dell'utente, purché rispetti i requisiti di adeguata robustezza: deve essere composta da almeno 12 caratteri e non deve contenere informazioni facilmente riconducibili all'utente, quali username, nome, cognome, data di nascita o altri riferimenti personali.

La modifica della password deve avvenire, inoltre:

- in caso di sospetta o accertata compromissione, secondo le modalità indicate nel successivo capitolo 6.1.2;
- su richiesta motivata del Responsabile Area ICT e MEPA;
- quando imposto dalle caratteristiche tecniche del servizio.

Non è richiesta una rotazione periodica indiscriminata, salvo specifiche valutazioni del rischio o vincoli del sistema. L'Ente adotta, ove tecnicamente possibile, meccanismi di autenticazione multifattoriale (MFA), controlli automatici contro l'utilizzo di password compromesse o deboli e misure di rilevazione e prevenzione dei tentativi di accesso anomali.

6.1.2 Password persa o dimenticata

La *password* deve essere immediatamente sostituita nel caso si sospetti o vi sia certezza che abbia perso segretezza.

Qualora un utente venga a conoscenza, anche accidentalmente, delle credenziali di accesso di un altro utente, è tenuto a comunicarlo immediatamente al Responsabile Area ICT e MEPA, che provvederà ad informare l'interessato e ad effettuare le necessarie misure di sicurezza, incluso il reset della *password*.

Nel caso venga dimenticata la *password*, ne dovrà essere richiesta una nuova, con le stesse modalità di attivazione nuova utenza, al Responsabile Area ICT e MEPA.

6.1.3 Cessazione utenza

Nel caso di cessazione, distacco o aspettativa, l'utenza è tempestivamente disabilitata, sono revocati le sessioni attive e sono rimossi i privilegi. L'eliminazione definitiva dall'Active Directory avviene solo decorso il periodo di conservazione definito dal Responsabile Area ICT e MEPA in accordo con i vertici dell'Ente, in modo da garantire tracciabilità, audit e gestione delle esigenze documentali, nel rispetto del principio di limitazione della conservazione.

6.1.4 Eccezioni

Per alcuni applicativi e servizi messi a disposizione agli utenti, ADSPMAS l'accesso avviene tramite verifica di identità digitale (SPID e CIE) per garantire un accesso verificato.

6.2 Autenticazione multifattoriale (MFA)

In combinazione con le credenziali, l'Ente rende disponibile un sistema di autenticazione multifattoriale. Qualora il secondo fattore sia installato su un dispositivo personale, l'utente riceve preventiva informazione sui dati trattati, sulle misure di sicurezza e sulle eventuali alternative organizzative messe a disposizione dall'Ente. L'utilizzo del dispositivo personale non comporta accesso dell'Ente ai contenuti privati non pertinenti al servizio di autenticazione.

La Multi-Factor Authentication (MFA) è una misura di sicurezza che richiede l'impiego di due o più fattori di verifica indipendenti (ad esempio *codice OTP, One Time Password* o dati biometrici) per confermare l'identità dell'utente.

L'adozione del MFA garantisce ai dipendenti un livello di protezione superiore rispetto alla sola autenticazione con credenziali statiche, poiché anche in caso di compromissione della *password* è necessario un ulteriore fattore di verifica per completare l'accesso.

Ogni dipendente è tenuto a utilizzare il MFA per accedere alle piattaforme digitali dell'Ente che lo consentono.

6.3 Privilegi e separazione dei ruoli

Per garantire la protezione dei sistemi e la sicurezza delle informazioni, l'assegnazione dei privilegi deve rispettare il principio del minimo privilegio (*least privilege*) e la separazione dei ruoli (*separation of duties*).

Ogni utente deve disporre limitatamente delle autorizzazioni necessarie per svolgere le proprie mansioni in funzione del principio "*need to know*", mentre le funzioni e mansioni critiche sono affidate a figure specializzate e formalmente individuate (cfr. Decreto Amministratori) per ridurre il rischio di errori o abusi.

I privilegi associati a ciascuna utenza devono essere tracciati e sottoposti a revisione periodica, con revoca immediata in caso di cambio ruolo o cessazione del rapporto.

Per quanto riguarda l'accesso al personal computer assegnato, questo avverrà con privilegi "*User*" e tramite le credenziali di accesso di Dominio che vengono assegnate/rimosse/sospese dal Responsabile Area ICT e MEPA.

6.4 Gestione delle utenze nelle postazioni specialistiche e negli ambienti segregati

Le postazioni impiegate in ambienti di sviluppo, laboratorio, ricerca, collaudo o test devono essere configurate secondo il principio del minimo privilegio (*least privilege*).

L'attività ordinaria dell'utente deve essere svolta mediante un account personale privo di privilegi amministrativi.

Qualora esigenze tecniche richiedano l'installazione di software, la modifica delle configurazioni o l'esecuzione di altre attività amministrative, tali operazioni devono essere eseguite mediante un account amministrativo separato e nominativo, utilizzato esclusivamente per il tempo necessario all'esecuzione delle attività autorizzate.

L'account amministrativo non deve essere utilizzato per la navigazione Internet, la consultazione della posta elettronica, l'accesso ai servizi documentali o altre attività ordinarie.

L'utilizzo delle utenze privilegiate deve essere tracciato e soggetto a registrazione degli eventi secondo quanto previsto dalle disposizioni interne in materia di logging e monitoraggio.

Le utenze con privilegi amministrativi devono essere periodicamente riesaminate dal Responsabile Area ICT e MEPA al fine di verificare la permanenza dell'effettiva necessità operativa.

6.5 Tracciamento e conservazione dei log di accesso

Per garantire la sicurezza dei sistemi e la conformità al *Regolamento (UE) 2016/679 (GDPR)*, alle *linee guida AgID* e alla *Direttiva (UE) 2022/2555 (NIS2)*, l'Ente monitora e conserva i log relativi alle attività di autenticazione, accesso e utilizzo delle utenze informatiche, mantenendone la piena responsabilità e garantendone la conformità a disposizioni normative.

I log di accesso costituiscono uno strumento essenziale per assicurare i principi di Riservatezza, Integrità e Disponibilità (RID), nonché per consentire attività di audit e verifica in

caso di anomalie o incidenti di sicurezza e vengono comunque raccolti nel rispetto del principio di minimizzazione previsto dal GDPR (*art.5, p. 1, lettera c*).

I tempi di conservazione dei log sono stabiliti e periodicamente riesaminati dall'Ente, quale Titolare del trattamento, per ciascuna categoria di dato e finalità, in un'apposita matrice di conservazione approvata dall'Ente. Le impostazioni del fornitore sono configurate, ove possibile, in coerenza con tali tempi. Ogni prolungamento è motivato e documentato; al termine i dati sono cancellati o resi anonimi in modo sicuro.

La consultazione dei log è strettamente riservata al personale autorizzato, al Responsabile Area ICT e MEPA e al personale da lui delegato, oltre che alle Autorità competenti nei casi previsti dalla legge. Ogni accesso ai log è tracciato e verificabile.

Per garantire la riservatezza, l'integrità e la disponibilità dei log, sono adottate misure tecniche e organizzative quali cifratura, controlli di integrità, restrizioni di accesso basate su ruoli e procedure di backup. Queste misure assicurano che i log non possano essere alterati e siano sempre disponibili per le finalità di sicurezza e conformità di cui sopra.

7. Infrastruttura di rete e Filesystem

Per l'accesso alle risorse informatiche dell'Ente attraverso la rete locale, ai sensi *dell'art.32 del Regolamento UE 2016/679 (GDPR)*, ciascun utente deve essere in possesso di credenziali di autenticazione (cfr. Capitolo 6.1 "Gestione, assegnazione e revoca delle credenziali di accesso").

È assolutamente proibito accedere alla rete ed ai sistemi informativi utilizzando credenziali di altre persone.

L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i file di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro. Gli Strumenti Informatici e tutte le cartelle di rete possono ospitare esclusivamente contenuti professionali. Pertanto, è vietato il salvataggio di documenti non inerenti all'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, e-mail personali, film e quant'altro.

Poiché in caso di violazioni contrattuali e giuridiche, sia il datore di lavoro, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e

l'integrità del proprio sistema informatico, con le modalità e secondo i principi meglio descritti al successivo capitolo 17. Ogni materiale personale rilevato dal Responsabile Area ICT e MEPA a seguito di interventi di sicurezza informatica, ovvero di manutenzione/aggiornamento su server ed anche sugli Strumenti, viene rimosso secondo le regole previste nel successivo capitolo 17 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare.

Le risorse di memorizzazione elencate di seguito non sono sottoposte al controllo regolare del Responsabile Area ICT e MEPA e non sono oggetto di backup periodici, a differenza degli Strumenti in uso per gli utenti. A titolo esemplificativo e non esaustivo si citano: il disco C o altri dischi locali dei singoli PC, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come *Hard disk* portatili o *NAS* ad uso esclusivo.

Le cartelle Desktop, Documenti e Immagini sincronizzate tramite OneDrive for Business sono considerate risorse aziendali gestite e, pertanto, non rientrano tra le aree di memorizzazione locali escluse dalle misure di protezione e conservazione dei dati adottate dall'Ente. Tutte le altre aree di memorizzazione non devono ospitare dati di interesse condiviso, poiché non sono garantite la sicurezza e la protezione contro l'eventuale perdita di dati. Pertanto, la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.

Senza il consenso scritto del Titolare del trattamento o suo apposito delegato, è vietato trasferire documenti elettronici dai sistemi informativi e Strumenti dell'Ente a *device* esterni (hard disk, chiavette USB, smartphone, tablet e altri supporti).

Senza il consenso scritto del Responsabile Area ICT e MEPA è vietato salvare documenti elettronici dell'Ente (ad esempio pervenuti via e-mail o salvati sul Server o sullo Strumento in dotazione) su *repository* esterne (quali ad esempio *Dropbox, Google Drive, WeTransfer*, ecc.). In caso di necessità l'Ente metterà a disposizione modalità in linea con le presenti direttive.

Gli utenti mantengono ordinati gli archivi di lavoro e rimuovono duplicati o file privi di utilità, nel rispetto delle regole di classificazione e conservazione e delle procedure di scarto. È vietata la cancellazione autonoma di documenti soggetti a protocollazione, fascicolazione, conservazione o obblighi di legge.

La risorsa di rete denominata "COMUNE" è messa a disposizione degli utenti principalmente per lo scambio temporaneo di file tra utenti, così da evitarne la trasmissione via e-mail; i file ivi

depositati dovranno essere rimossi non appena si completa lo scambio; il Responsabile Area ICT e MEPA provvederà d'ufficio ad una pulizia periodica della risorsa "COMUNE" cancellando file e cartelle più vecchi di 2 mesi e che non appartengano a richieste specifiche regolarmente autorizzate per iscritto dal Responsabile Area ICT e MEPA.

7.1 Connessione sicura

All'interno della sede lavorativa è resa disponibile una rete WiFi, che consente l'accesso a Internet e a specifiche risorse informatiche per i dispositivi non collegati alla rete LAN mediante cavo. L'accesso mediante rete WiFi viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a utenti nell'Ente che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. Le impostazioni e configurazioni della rete WiFi sono gestite e approvate dal Responsabile Area ICT e MEPA.

ADSPMAS, inoltre, mette a disposizione degli ospiti una rete WiFi dedicata (*APV-Ospiti*), destinata esclusivamente a visitatori e soggetti esterni che non necessitano di accedere alle risorse interne. Tale rete consente l'accesso limitato e controllato alla sola navigazione Internet, garantendo la separazione dalla rete interna di ADSPMAS e assicurando così un livello adeguato di sicurezza e protezione dei dati.

L'Ente mette a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno. Tale accesso avviene mediante software ISL o anche rete VPN (*Virtual Private Network*). Qualora presente un apposito accordo di riservatezza, l'accesso mediante VPN, o altra modalità, può essere concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche.

7.1.1 Lavoro agile

ADSPMAS ha consolidato il modello di lavoro agile, reso possibile dall'adeguamento delle infrastrutture digitali e dall'adozione di strumenti collaborativi avanzati. Il dipendente che opera in modalità agile deve utilizzare esclusivamente connessioni sicure e sistemi di autenticazione robusti per accedere alle risorse informatiche aziendali.

È obbligatorio attenersi alle procedure di accesso stabilite e garantire che ogni attività svolta da remoto avvenga nel rispetto delle regole di sicurezza informatica.

È fatto divieto di utilizzare connessioni non protette o modalità di accesso diverse da quelle indicate dall'Ente.

La fruizione del lavoro agile è subordinata all'impiego di strumenti di accesso sicuro, indispensabili per assicurare la continuità operativa e la tutela dei dati e delle informazioni trattate anche al di fuori degli ambienti fisici di ADSPMAS. Ogni dipendente è tenuto a garantire la riservatezza e l'integrità delle informazioni gestite durante l'attività lavorativa agile.

Il Responsabile Area ICT e MEPA si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica.

7.2 Accesso da ambienti segregati

Le reti di sviluppo, laboratorio, collaudo e test devono rimanere logicamente separate dall'ambiente di produzione.

L'utilizzo di connessioni VPN o di altre modalità di accesso dall'ambiente di sviluppo a quello di produzione costituisce una misura eccezionale e può essere autorizzato esclusivamente in via temporanea per esigenze tecniche adeguatamente documentate. Tale autorizzazione è subordinata alla preventiva valutazione del Responsabile dell'Area ICT e MEPA, deve essere limitata alle sole risorse strettamente necessarie e prevedere il tracciamento degli accessi, nel rispetto del principio del minimo privilegio.

Non è consentito utilizzare connessioni VPN verso la rete di produzione per finalità di ordinaria consultazione documentale o trasferimento di file qualora tali attività possano essere svolte mediante servizi o piattaforme autorizzate dall'Ente.

Non sono consentiti collegamenti permanenti o continuativi che possano ridurre l'efficacia della segregazione tra gli ambienti.

7.3 Utilizzo dei dati negli ambienti segregati

Gli ambienti di sviluppo, laboratorio, collaudo e test devono utilizzare, di norma, dati sintetici, anonimizzati o opportunamente pseudonimizzati.

Non è consentito utilizzare dati reali provenienti dagli ambienti di produzione salvo comprovata necessità tecnica, preventiva autorizzazione del Responsabile Area ICT e MEPA e adozione di adeguate misure di sicurezza e minimizzazione del dato.

È vietata la replica permanente, la sincronizzazione automatica o il trasferimento indiscriminato di basi dati, archivi documentali o altre informazioni dagli ambienti di produzione agli ambienti di sviluppo, laboratorio o test.

Le eventuali copie autorizzate devono essere limitate allo stretto necessario, mantenute per il tempo minimo indispensabile e successivamente rimosse secondo le procedure definite dall'Ente.

7.4 Monitoraggio e Logging

Al fine di garantire la sicurezza dell'infrastruttura tecnologica, ADSPMAS registra gli eventi relativi al funzionamento della rete, degli apparati di sicurezza, delle connessioni VPN, dei sistemi proxy e delle risorse condivise. Tali log possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso il Responsabile Area ICT e MEPA, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio. I controlli possono avvenire secondo le disposizioni previste al successivo capitolo 17 del presente Regolamento.

Le informazioni raccolte possono essere utilizzate per finalità connesse al rapporto di lavoro esclusivamente se acquisite nel rispetto dell'art. 4 della legge n. 300/1970, della disciplina sulla protezione dei dati personali, dell'informativa resa agli interessati e delle procedure di cui al capitolo 17.

8. Utilizzo degli Strumenti

L'utente è consapevole che gli strumenti forniti sono di proprietà dell'Ente e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ciascun utente è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Gli strumenti informatici e di telecomunicazione sono assegnati per finalità istituzionali e lavorative. È consentito un utilizzo personale occasionale e non significativo, purché non interferisca con l'attività lavorativa, non comporti costi aggiuntivi per l'Ente, non comprometta la sicurezza dei sistemi informativi, non violi disposizioni di legge o del presente Regolamento e non determini

pregiudizio all'immagine o al patrimonio dell'Autorità. Rimane in ogni caso vietato qualsiasi utilizzo personale sistematico, prevalente o incompatibile con le esigenze di servizio.

L'accesso agli Strumenti avviene tramite le credenziali assegnate all'utente secondo quanto stabilito dal capitolo 6 "Gestione degli accessi".

Gli strumenti devono essere custoditi con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente e per iscritto al Responsabile Area ICT e MEPA ogni malfunzionamento e/o guasto. Non è consentita l'attivazione della *password* di accensione (BIOS), senza preventiva autorizzazione scritta da parte del Responsabile Area ICT e MEPA.

Non è consentito all'utente modificare le caratteristiche *hardware* e *software* impostate sugli Strumenti assegnati, salvo preventiva autorizzazione scritta da parte del Responsabile Area ICT e MEPA.

Le postazioni appartenenti ad ambienti segregati o specialistici devono essere preventivamente installate, configurate oppure formalmente validate dal Responsabile Area ICT e MEPA o da personale da lui delegato. Eventuali configurazioni autonome dell'utente devono essere preventivamente autorizzate e documentate.

L'utente è tenuto a scollegarsi dal sistema o bloccare l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un PC incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Non è consentita l'installazione di programmi diversi da quelli autorizzati dal Responsabile Area ICT e MEPA.

È obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto.

È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da *copyright*.

È vietato l'utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti, salvo che il supporto utilizzato sia stato fornito dal Responsabile Area ICT e MEPA. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.

Le dotazioni periferiche vengono fornite all'utente per la conduzione delle attività lavorative quotidiane. Eventuali eccezioni (ad esempio, ma non limitatamente a: *smartphone*, fotocamere, *webcam*, stampanti, etc.) devono essere formalmente approvate dal Responsabile Area ICT e MEPA previa richiesta formale scritta.

È vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, *router*, *switch*, *modem*, stampanti, etc.) non autorizzato preventivamente per iscritto dal Responsabile Area ICT e MEPA.

Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, è tenuto a comunicarlo tempestivamente al Responsabile Area ICT e MEPA.

Dal momento della cessazione del rapporto di lavoro, in caso di distacco o aspettativa, gli Strumenti messi a disposizione dell'utente verranno resettati alle condizioni iniziali.

Nei casi di smarrimento, furto accertato o grave manomissione dei dispositivi assegnati o del contenuto degli stessi, gli utenti devono segnalare immediatamente e per iscritto il fatto ai soggetti di seguito indicati:

- Responsabile Area ICT e MEPA;
- Autorità Giudiziaria (sporgere denuncia);
- Direttore della propria Struttura di appartenenza.

8.1 Dispositivi BYOD (Bring Your Own Device)

L'Ente si riserva di poter autorizzare i dipendenti all'utilizzo dei propri dispositivi mobili al fine di accedere, conservare e trattare informazioni e applicazioni aziendali. Si parlerà in tal caso di modalità BYOD.

I dispositivi utilizzati in modalità BYOD dovranno rispondere a un livello di sicurezza almeno pari a quello dei dispositivi dell'Ente, in particolare per quanto riguarda l'accesso tramite username e *password*, la frequenza di backup e l'utilizzo di un programma antivirus regolarmente aggiornato. A tal fine, tali dispositivi dovranno essere preventivamente

sottoposti a verifica da parte del Responsabile Area ICT e MEPA, il quale potrà proporre eventuali modifiche della configurazione del dispositivo, e/o l'installazione di *software* per adeguarne i livelli di sicurezza.

I dispositivi BYOD, nonché di quelli di proprietà dell'Ente per i quali è stato esplicitamente autorizzato l'uso promiscuo, dovranno essere gestiti in modo da evitare commistioni fra i dati di proprietà dell'utilizzatore e quelli (personali o comunque riservati) di proprietà dell'Ente; per questi ultimi valgono tutte le limitazioni precedentemente indicate.

Sui dispositivi utilizzati per le modalità BYOD potranno essere installati solo *software* precedentemente concordati con il Responsabile Area ICT e MEPA, e comunque coperti da una licenza regolare e documentabile.

Qualsiasi controllo sul dispositivo personale è limitato all'ambiente o alle applicazioni di lavoro autorizzate.

8.2 Aggiornamenti e patch obbligatorie

Per garantire la sicurezza dei sistemi informativi e la protezione dei dati, tutti i dispositivi e le applicazioni aziendali devono essere mantenuti costantemente aggiornati. L'installazione delle patch di sicurezza rilasciate dai fornitori è obbligatoria e deve avvenire secondo le tempistiche definite dalle procedure interne, privilegiando gli aggiornamenti critici che risolvono vulnerabilità note. Gli utenti non sono autorizzati a disattivare o ritardare gli aggiornamenti automatici e devono collaborare affinché i dispositivi rimangano conformi agli standard di sicurezza. Qualsiasi anomalia o impossibilità di applicare un aggiornamento deve essere immediatamente segnalata al Responsabile Area ICT e MEPA. L'inosservanza di queste disposizioni può esporre l'organizzazione a rischi significativi e comportare responsabilità disciplinari.

8.3 Monitoraggio e Logging

I log relativi all'utilizzo di Strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui server o sui router, nonché i file con essi trattati, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso il Responsabile Area ICT e MEPA. Tali registrazioni sono usate esclusivamente per finalità organizzative e produttive, di protezione dei dispositivi e del patrimonio informativo, gestione degli incidenti, assistenza tecnica e verifica del corretto funzionamento degli Strumenti assegnati.

I controlli possono avvenire secondo le disposizioni previste al capitolo 17. Le informazioni raccolte possono essere utilizzate per finalità connesse al rapporto di lavoro esclusivamente se acquisite nel rispetto dell'art. 4 della legge n. 300/1970, della disciplina sulla protezione dei dati personali, dell'informativa resa agli interessati e delle procedure di cui al capitolo 17.

9. Internet e navigazione sicura

È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa, ad esempio i siti istituzionali, i siti degli Enti locali, piattaforme di fornitori e partner. L'accesso è regolato dal *proxy* con le sue policy di sicurezza debitamente implementate e aggiornate.

È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Ente, ad esempio, il download o l'upload di file audio e/o video, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.

È vietato a chiunque il download di qualunque tipo di *software* gratuito (*freeware*) o *shareware* prelevato da siti Internet, se non espressamente autorizzato dal Responsabile Area ICT e MEPA.

L'Ente si riserva di bloccare l'accesso a siti "a rischio" attraverso l'utilizzo di *blacklist* pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. In caso di blocco accidentale di siti di interesse si dovrà contattare per iscritto il Responsabile Area ICT e MEPA per uno sblocco selettivo.

Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri, è necessario richiedere lo sblocco mediante una e-mail indirizzata al Responsabile Area ICT e MEPA, ed in copia al RTD, nella quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, intervallo di tempo richiesto per completare l'attività. L'utente, nello svolgimento delle proprie attività, deve comunque tenere presente in modo particolare i capitoli 17 e 18 del presente Regolamento. Al termine dell'attività il Responsabile Area ICT e MEPA ripristinerà i filtri alla situazione iniziale.

È tassativamente vietato effettuare qualsiasi genere di transazione finanziaria, ivi comprese le operazioni di *remote banking*, acquisti on-line e simili, salvo i casi direttamente autorizzati per

iscritto dal RTD e dal Responsabile Area ICT e MEPA, con il rispetto delle normali procedure di acquisto.

È assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a internet tranne in casi del tutto eccezionali e previa autorizzazione scritta del Responsabile Area ICT e MEPA e del RTD.

È assolutamente vietata la partecipazione a Forum non professionali, ai Social Network, l'utilizzo di *chat line* (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in *guest books* anche utilizzando pseudonimi.

Si informa che l'Ente non effettua controlli sistematici delle pagine web visualizzate dal singolo utente né controlli automatici individualizzati sui dati di navigazione. I dati tecnici di navigazione e i log del proxy sono raccolti per il funzionamento e la sicurezza dei sistemi e conservati per il periodo strettamente necessario indicato nella matrice di conservazione di cui al capitolo 18. L'eventuale estensione del periodo ordinario è ammessa solo per motivate esigenze tecniche, di sicurezza, di accertamento di incidenti o di tutela di diritti ed è documentata. Eventuali controlli avvengono secondo il capitolo 17. Le informazioni raccolte possono essere utilizzate per finalità connesse al rapporto di lavoro esclusivamente se acquisite nel rispetto dell'art. 4 della legge n. 300/1970, della disciplina sulla protezione dei dati personali e dell'informativa resa agli interessati.

10. Utilizzo della Posta Elettronica

Le regole di seguito specificate sono adottate anche ai sensi delle "*Linee guida del Garante per posta elettronica e Internet*" pubblicate in Gazzetta Ufficiale *n. 58 del 10 marzo 2007* e del *Regolamento (UE) 2016/679 (GDPR)*. Ciascun utente si deve attenere alle seguenti regole di utilizzo dell'indirizzo di posta elettronica.

Come descritto al capitolo 6.1 del presente Regolamento, ad ogni utente viene fornito un account istituzionale nominativo, generalmente coerente con il modello "nome.cognome@port.venice.it". L'accesso all'account viene disattivato in caso di distacco, aspettativa o alla cessazione del rapporto di lavoro; la casella di posta rimarrà comunque attiva con apposito messaggio di risposta automatica per n. 30 giorni e, al termine di tale data, verrà disattivata. L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi lavorativi, ed è

assolutamente vietato ogni utilizzo di tipo privato. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.

L'Ente predispone, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati.

L'iscrizione a *e-mailing-list* o *newsletter* esterne con l'indirizzo ricevuto è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.

Allo scopo di garantire sicurezza alla rete, evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità aventi contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di *phishing* o altre frodi informatiche. In qualunque situazione di incertezza contattare il Responsabile Area ICT e MEPA per una specifica valutazione del singolo caso.

Non è consentito diffondere messaggi del tipo "*catena di S. Antonio*" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus o altre minacce. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.

Nel caso fosse necessario inviare allegati "pesanti" (consentito sino a 10 Mb) è opportuno ricorrere prima alla compressione dei file originali in un archivio formato .zip o equivalenti e condividerli sulle risorse di rete. Nel caso di allegati ancora più voluminosi è necessario rivolgersi per iscritto al Responsabile Area ICT e MEPA. Per opportuna informazione, inoltre, è consentita la ricezione di allegati sino a 30 Mb. Per la condivisione di allegati di maggiore dimensione, è possibile utilizzare le cartelle Sharepoint condivise oppure cartelle di rete condivise gestite con misure di sicurezza specifiche quali: controllo degli accessi, inventario dei dispositivi, gestione del rischio, autenticazione robusta e gestione degli incidenti, focalizzandosi su chi può accedere, come e cosa, e per proteggere i dati.

Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali, incluse le categorie particolari di dati di cui all'*art. 9 GDPR* o dati relativi a

condanne penali e reati ai sensi dell'*art. 10*, è obbligatorio che questi allegati vengano preventivamente protetti mediante cifratura o compressione con *password* con apposito software. La *password* di cifratura deve essere comunicata al destinatario attraverso un canale diverso dalla e-mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni, i dati personali e/o ex sensibili di competenza possono essere inviati soltanto a destinatari - persone o Enti - qualificati e competenti.

Non è consentito l'invio automatico della posta elettronica verso indirizzi e-mail privati (attivando per esempio un "inoltro" automatico delle e-mail entranti), nemmeno in periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è raccomandabile utilizzare un messaggio "*Out of Office*" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di e-mail alternativo preferibilmente di tipo collettivo, come, ad esempio, ufficio...@port.venice.it. Rivolgersi al Responsabile Area ICT e MEPA per tale eventualità.

In caso di assenza improvvisa prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione *auto-reply* o l'inoltro automatico su altre caselle e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare per iscritto un altro utente (fiduciario). Tale utente potrà verificare il contenuto di messaggi e inoltrare al Titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Dirigente responsabile assicurarsi che sia redatto un verbale attestante quanto avvenuto e informare il lavoratore interessato alla prima occasione utile.

L'invio massivo di e-mail deve essere effettuato esclusivamente per finalità di servizio, possibilmente su autorizzazione scritta del Dirigente responsabile competente. Per evitare che le eventuali risposte siano inoltrate a tutti i destinatari, generando traffico eccessivo ed indesiderato, è necessario utilizzare la copia nascosta (Bcc o Ccn) se la tipologia del messaggio lo consente.

È vietato inviare messaggi di posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione.

La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. Anche la conservazione di

messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sulle condivisioni.

I messaggi in entrata vengono sistematicamente analizzati tramite controlli anti-malware e antispam. I messaggi che dovessero contenere virus vengono eliminati dal sistema e il mittente/destinatario viene avvisato mediante messaggio specifico. Per le comunicazioni aventi valore legale o ufficiale, si raccomanda l'utilizzo della Posta Elettronica Certificata (PEC), ai sensi del *DPR 11 febbraio 2005, n. 68*, e richiamata dal *Codice dell'Amministrazione Digitale (D.Lgs. 82/2005)*, che attribuiscono alla PEC lo stesso valore legale della raccomandata con ricevuta di ritorno.

Le caselle PEC attivate da ADSPMAS consentono la trasmissione e la ricezione di documenti ufficiali in sostituzione della posta cartacea, garantendo la prova dell'invio e della consegna. L'uso della PEC è raccomandato ogniqualvolta sia necessario inviare comunicazioni formali a soggetti esterni con valore legale, ottenere conferma dell'avvenuta ricezione dei messaggi o trasmettere documenti ufficiali a destinatari per i quali la PEC costituisce il canale previsto dalle normative o dalle procedure interne.

10.1 Trattamento dei metadati

ADSPMAS, nel rispetto delle normative vigenti e delle regole di sicurezza informatica (Provv. n.364 del 6 giugno 2024 "Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati"), disciplina l'utilizzo della posta elettronica aziendale e il trattamento dei dati tecnici ad essa collegati.

Il sistema di posta elettronica genera automaticamente metadati, ossia informazioni registrate nei log dei server (MTA) e delle postazioni client (MUA). Questi metadati comprendono, tra gli altri, gli indirizzi e-mail del mittente e del destinatario, gli indirizzi IP dei server coinvolti, gli orari di invio e ricezione, la dimensione del messaggio, la presenza e la dimensione di eventuali allegati e l'oggetto del messaggio.

I sistemi di posta elettronica generano automaticamente metadati associati alle operazioni di invio, ricezione e smistamento dei messaggi. La conservazione dei metadati necessari al funzionamento e alla sicurezza del servizio è limitata, di regola, a 21 giorni; un periodo superiore è ammesso soltanto in presenza di comprovate e documentate esigenze tecniche o

organizzative e previa verifica della compatibilità con l'art. 4 della legge n. 300/1970 e con la normativa in materia di protezione dei dati personali.

È fatto divieto di tentare di alterare, cancellare o accedere ai metadati registrati dai sistemi; ad ogni modo l'accesso ai metadati è consentito esclusivamente ai soggetti autorizzati e adeguatamente istruiti, e ogni operazione è tracciata per garantire responsabilizzazione e sicurezza.

10.2 Gestione della casella di Posta Elettronica e conservazione dei messaggi

I messaggi che costituiscono documenti amministrativi o assumono rilevanza giuridica, amministrativa, contabile o fiscale devono essere acquisiti al sistema di gestione documentale, protocollati o fascicolati ove previsto e conservati secondo le regole di conservazione dell'Ente e la normativa applicabile. La casella di posta elettronica non costituisce, di per sé, sistema di conservazione permanente. Gli utenti provvedono tempestivamente alla corretta acquisizione dei messaggi rilevanti nei sistemi istituzionali.

L'Ente non controlla sistematicamente il contenuto delle comunicazioni e-mail. In caso di assenza improvvisa o prolungata, cessazione del rapporto, imprescindibili esigenze di continuità operativa, sicurezza o tutela del patrimonio, l'accesso alla casella può essere disposto esclusivamente secondo la procedura descritta al capitolo 17 del presente documento, limitatamente alle informazioni strettamente necessarie, privilegiando le caselle condivise e gli strumenti meno invasivi. Ogni accesso è autorizzato, tracciato e verbalizzato; l'interessato è informato appena ciò non pregiudichi la finalità legittima del controllo.

In caso di cessazione del rapporto, l'accesso dell'utente alla casella è immediatamente inibito; può essere attivato per un periodo massimo di 30 giorni un messaggio automatico che indichi un recapito istituzionale alternativo, senza comunicare dati non necessari. Decorso tale periodo, la casella è disattivata. I documenti rilevanti devono essere previamente acquisiti al sistema di gestione documentale; i restanti contenuti sono cancellati secondo la matrice di conservazione e le procedure dell'Ente.

11. Strumenti di messaggistica

Agli utenti è permesso utilizzare sistemi di messaggistica istantanea interna per permettere una efficace e agevole comunicazione tra i colleghi, mediante i soli strumenti autorizzati dal Responsabile Area ICT e MEPA. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed e-mail.

È consentito un utilizzo legato principalmente a scopi professionali, rimanendo consentito un utilizzo personale occasionale e non significativo, purché non interferisca con l'attività lavorativa, non comporti costi aggiuntivi per l'Ente, non comprometta la sicurezza dei sistemi informativi, non violi disposizioni di legge o del presente Regolamento. Gli strumenti di messaggistica possono generare registrazioni tecniche, log di accesso, informazioni sugli eventi di sistema e metadati. Pertanto, anche su tali strumenti di messaggistica istantanea è attivo il monitoraggio e la registrazione dell'attività degli utenti, secondo le disposizioni del capitolo 17 del presente Regolamento. L'Autorità non effettua controlli sistematici sul contenuto delle conversazioni. L'accesso al contenuto delle chat, dei messaggi, dei file condivisi e degli altri contenuti presenti nelle piattaforme collaborative è consentito esclusivamente nei casi e con le modalità previste dall'art. 17 del presente Regolamento, nel rispetto dell'art. 4 della Legge n. 300/1970, del GDPR e dei principi di necessità, proporzionalità e minimizzazione.

Microsoft Teams costituisce lo strumento di collaborazione e messaggistica interna adottato dall'Ente. L'utilizzo deve avvenire esclusivamente per finalità lavorative e nel rispetto delle autorizzazioni assegnate.

Il dipendente deve, comunque, tener conto delle buone pratiche indicate per una *cyber hygiene* adeguata, comunicando quindi solo lo stretto necessario ad altri utenti non coinvolti e prestando attenzione a non includere soggetti che non dispongono delle autorizzazioni necessarie a visualizzare o ad interagire con determinati materiali.

Le applicazioni di messaggistica esterna, compreso WhatsApp, non costituiscono canali istituzionali e non possono essere utilizzate per trasmettere documenti, dati personali, istruzioni operative o comunicazioni aventi rilevanza amministrativa. Eventuali comunicazioni

informali autorizzate devono essere prive di dati riservati e, se assumono rilevanza per l'attività dell'Ente, devono essere tempestivamente riportate sui canali istituzionali.

L'utilizzo di applicazioni esterne è ammesso soltanto nei limiti espressamente autorizzati dall'Ente e nel rispetto del divieto di trattare informazioni operative, riservate o soggette a protocollazione e conservazione.

I canali ufficiali dell'Ente devono essere utilizzati esclusivamente mediante dispositivi e applicazioni autorizzati. È vietato trasferire o duplicare contenuti istituzionali su account, social media o applicazioni personali.

12. Partecipazioni a Social Media

L'utilizzo a fini promozionali e commerciali di Facebook, Twitter, LinkedIn, dei blog e dei forum, anche professionali, (ed altri siti o social media) è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto. Tali attività devono essere svolte nel pieno rispetto delle politiche e delle misure di sicurezza ICT definite dall'Ente, rimanendo escluse iniziative individuali da parte di singoli utenti o collaboratori.

In conformità agli *artt. 2104 e 2105 del Codice Civile*, che sanciscono rispettivamente l'obbligo di diligenza e quello di fedeltà, e nel rispetto del diritto della persona alla libertà di espressione, l'Ente ritiene opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partner, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro.

Il presente articolo deve essere osservato dall'utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come utente dell'Ente.

La condivisione dei contenuti nel social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti

svolti o in svolgimento presso gli uffici, nonché strategie, documentazione tecnica, *know-how* ed elenchi di clienti, fornitori o partner.

Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Ente. L'utente, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo di ADSPMAS, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione.

L'utente deve garantire la tutela della riservatezza e dignità delle persone ai sensi del *D.Lgs. 196/2003*, come modificato dal *D.Lgs. 101/2018*, e del *Regolamento (UE) 2016/679 (GDPR)*; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori, se non con il preventivo personale consenso di questi, e comunque non potrà postare nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso del Responsabile d'Ufficio.

Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali (es., post su prodotti, servizi, fornitori, partner, ecc.), egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ente, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

13. Telefoni, fotocopiatrici, scanner, stampanti e plotter

L'utente è consapevole che gli Strumenti di stampa, così come anche il telefono fisso, sono di proprietà dell'Ente e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto, ne viene concesso l'uso esclusivamente per tale fine.

Il telefono fisso affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.

Qualora venisse assegnato uno smartphone e relativa SIM card all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Agli smartphone si applicano le medesime regole sopra previste per gli altri dispositivi informatici (cfr. 8), per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare, si raccomanda il rispetto delle regole per una corretta navigazione In Internet (cfr. 9).

Per gli smartphone di proprietà dell'Ente è vietata l'installazione e l'utilizzo di applicazioni diverse da quelle autorizzate dal Responsabile Area ICT e MEPA.

È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Ufficio.

Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:

- Stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative;
- Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili).

Nel caso in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà presidiare il dispositivo di stampa od utilizzare la stampa protetta da PIN, per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate.

14. Assistenza agli utenti e manutenzioni

Il Responsabile Area ICT e MEPA o i suoi delegati possono accedere ai dispositivi informatici sia direttamente, sia mediante *software* di accesso remoto, per i seguenti scopi:

- Verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale;
- Verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;
- Richieste di aggiornamento *software* e manutenzione preventiva *hardware* e *software*.

Gli interventi tecnici possono avvenire previo consenso dell'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, il Responsabile Area ICT e MEPA

o i suoi delegati sono autorizzati ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

L'accesso in teleassistenza sui PC della rete richiesto da terzi (fornitori e/o altri) deve essere autorizzato per iscritto dal Responsabile Area ICT e MEPA, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.

Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o il Responsabile Area ICT e MEPA devono presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento.

È possibile rivolgersi al Responsabile Area ICT e MEPA utilizzando l'apposito applicativo per l'Help Desk (https://goiticket.port.venice.it) oppure, in alternativa se l'applicativo non è raggiungibile, via telefono interno al 4285 o 4261.

15. Sicurezza dei Dati

I dati personali, oggetto di trattamento, devono essere custoditi e controllati anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito a non conforme alle finalità della raccolta.

All'atto della dismissione di supporti che contengano dati personali è necessario distruggere per rendere inutilizzabile (cancellare il contenuto) i supporti medesimi, secondo quanto previsto dal *Provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008* sui "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali" (*doc. web n. 1571514*).

Tutti gli utenti devono porre attenzione nei trattamenti di categorie particolari di dati personali (*art. 9, Regolamento (UE) 2016/679*) nonché dei dati personali relativi a condanne penali e reati (*art. 10, Regolamento (UE) 2016/679*).

15.1 Ambiente Cloud oppure On-premise

ADSPMAS trasferisce i propri applicativi in ambienti adeguati a garantire sicurezza, continuità operativa e facilità di accesso. Tutti i dipendenti devono utilizzare esclusivamente le piattaforme messe a disposizione dall'Ente per accedere ai servizi ICT e svolgere le attività lavorative.

È obbligatorio attenersi alle procedure di accesso e alle modalità operative stabilite per ciascun servizio. È fatto divieto di utilizzare sistemi o applicativi non autorizzati o di aggirare le procedure di accesso previste. Ogni dipendente deve assicurarsi di operare unicamente attraverso gli strumenti messi a disposizione dall'Ente, nel rispetto delle regole di sicurezza e tracciabilità.

Ogni variazione o problema riscontrato nell'utilizzo delle piattaforme deve essere segnalata tempestivamente al Responsabile competente. Alla cessazione del rapporto di lavoro, l'accesso ai sistemi viene disabilitato e il dipendente non è più autorizzato a utilizzare alcuna risorsa digitale dell'Ente.

15.2 Sicurezza delle applicazioni

Nello sviluppo di applicazioni informatiche, devono essere rispettati i principi di sicurezza e di protezione dei dati "*by design*" e "*by default*", incorporando i principi e le misure a tutela della privacy e della sicurezza delle informazioni lungo l'intero ciclo di vita delle applicazioni, assicurando l'adozione di un processo conforme al *Software Development Life Cycle* (SDLC). Il nuovo Regolamento (UE) 2016/679, al 78° "considerando" iniziale stabilisce infatti che: "in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettato tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici". Inoltre, devono essere seguite le *best practice* e gli standard internazionali, tra cui ISO/IEC 27001:2022, OWASP *Application Security*

Verification Standard (ASVS) e le linee guida AgID per la sicurezza delle applicazioni nella Pubblica Amministrazione.

Le strutture dell'Ente che affidino ad un fornitore esterno l'incarico di sviluppare applicazioni devono, pertanto, prevedere nei relativi contratti di appalto, che siano rispettate le prescrizioni del sopra citato GDPR, e che siano rispettate le linee guida dei sopracitati standard di riferimento (ISO, OWASP e linee guida AgID), attraverso la previsione di apposite clausole, la sottoscrizione di opportune informative, l'individuazione e la nomina, ove necessario, del Responsabile esterno del Trattamento, ai sensi dell'art 28 del GDPR, e la sottoscrizione di uno specifico Accordo di riservatezza (c.d. "NDA – *Non Disclosure Agreement*").

Le stesse considerazioni valgano, inoltre, anche nel caso di applicazioni acquistate sul mercato.

Le applicazioni devono, inoltre, essere progettate e configurate per garantire l'interoperabilità dei dati, consentendo l'integrazione sicura con diverse fonti informative e con la Piattaforma Digitale Nazionale Dati (PDND), senza pregiudicare i canali tradizionali di interscambio con fonti non ancora disponibili sulla piattaforma nazionale.

16. Gestione incidenti

In conformità alla *Direttiva (UE) 2022/2555 (NIS2)*, allo standard *ISO/IEC 27001:2022* e al *Regolamento (UE) 2016/679 (GDPR),* l'organizzazione adotta un processo strutturato per la gestione degli incidenti di sicurezza informatica, al fine di garantire la continuità operativa e la protezione dei dati personali.

16.1 Segnalazione tempestiva

Ogni utente è tenuto a segnalare immediatamente qualsiasi evento o anomalia che possa compromettere la riservatezza, l'integrità o la disponibilità dei sistemi e dei dati (ad es. malfunzionamento del PC, indisponibilità dei servizi applicativi o di rete) al Responsabile Area ICT e MEPA, secondo le modalità previste al capitolo 14, che raccoglie la segnalazione e avvia il processo di classificazione e gestione dell'incidente al fine di minimizzarne gli impatti.

In conformità agli artt. 23, 24 e 25 del D.Lgs. 4 settembre 2024, n. 138, gli incidenti significativi sono portati senza ritardo all'attenzione degli organi di amministrazione e direttivi e gestiti secondo il Piano di gestione degli incidenti e delle violazioni dei dati personali adottata dall'Ente.

L'alta direzione assicura la tempestiva valutazione dell'incidente e l'attivazione dei soggetti formalmente designati. Quando ricorrono i presupposti normativi, la notifica al CSIRT Italia è effettuata nei termini e secondo le modalità previsti dal D.Lgs. 138/2024 e dagli atti applicativi dell'ACN, in accordo con la procedura interna vigente.

ADSPMAS assicura la documentazione e la conservazione delle segnalazioni per consentire eventuali verifiche da parte delle autorità competenti e garantisce che il corpo direzionale riceva formazione adeguata a comprendere e gestire i rischi di sicurezza informatica.

16.2 Data Breach

Ogni incidente che coinvolge dati personali (cd. "*data breach*") deve essere segnalato in modo tempestivo al Responsabile Area ICT e MEPA, secondo le modalità previste al precedente capitolo 14, che raccoglierà le segnalazioni e avvierà il relativo processo di classificazione e risoluzione dell'incidente medesimo al fine di minimizzare gli eventuali impatti negativi sul normale svolgimento delle attività lavorative.

Ogni sospetta violazione di dati personali, indipendentemente dalla gravità apparente, deve essere immediatamente segnalata al Responsabile Area ICT e MEPA e al referente interno individuato dal Piano di gestione degli incidenti. L'Autorità, quale Titolare del trattamento, documenta e valuta ogni violazione, con il supporto del Responsabile della protezione dei dati (RPD/DPO), e provvede, ove ne ricorrano i presupposti, alla notifica al Garante ai sensi dell'art. 33 GDPR e alla comunicazione agli interessati ai sensi dell'art. 34 GDPR. Il RPD/DPO non coincide con il Responsabile del trattamento di cui all'art. 28 GDPR e svolge funzioni di consulenza, sorveglianza e raccordo con l'Autorità di controllo.

17. Controlli sugli Strumenti

17.1 Principi e presupposti

I controlli sugli Strumenti Informatici sono effettuati esclusivamente per esigenze organizzative e produttive, sicurezza del lavoro, tutela del patrimonio, sicurezza dei sistemi, continuità operativa o accertamento di specifiche condotte illecite, nel rispetto dell'art. 4 della legge n. 300/1970, della normativa in materia di protezione dei dati personali e dei principi di necessità, proporzionalità, trasparenza, pertinenza, non eccedenza e limitazione della conservazione. Sono vietati controlli massivi, prolungati, costanti o indiscriminati.

Le informazioni raccolte sono utilizzabili per finalità connesse al rapporto di lavoro soltanto se acquisite lecitamente, previa adeguata informazione agli interessati e nel rispetto delle condizioni previste dall'art. 4, comma 3, della legge n. 300/1970. Resta ferma, ove applicabile, la necessità dell'accordo sindacale o dell'autorizzazione dell'Ispettorato nazionale del lavoro ai sensi dell'art. 4, comma 1.

17.2 Tipologie di controllo

a) Controlli tecnici ordinari: attività di manutenzione, aggiornamento, sicurezza, monitoraggio aggregato, prevenzione di malware, verifica della continuità e risoluzione di anomalie. Sono gestiti dal Responsabile Area ICT e MEPA nell'ambito delle attribuzioni formalmente conferite e, di regola, senza analisi individuale dei contenuti.

b) Accessi per continuità operativa: recupero di file o comunicazioni indispensabili in caso di assenza, irreperibilità o cessazione dell'utente. Sono richiesti con atto scritto e motivato dal Direttore o Responsabile della struttura interessata e autorizzati dal Segretario Generale. L'accesso è eseguito dal Responsabile Area ICT e MEPA, limitatamente ai dati indispensabili, e viene verbalizzato.

c) Controlli individuali o difensivi: verifiche riferibili a uno o più utenti, effettuate sulla base di un fondato e documentato sospetto di condotte illecite o di una concreta minaccia al patrimonio o ai sistemi. Devono essere mirate, circoscritte, di regola successive all'insorgenza del sospetto e proporzionate. Sono autorizzate dal Segretario Generale, previo coinvolgimento dell'Area competente per il personale e consultazione del RPD/DPO per i profili di protezione dei dati. Se il controllo riguarda il Segretario Generale, l'autorizzazione compete al Presidente.

d) Interventi urgenti di sicurezza: quando sussista un rischio imminente e grave per sistemi, dati o servizi, il Responsabile Area ICT e MEPA, o il personale espressamente individuato nel Piano di Risposta agli Incidenti, può adottare immediatamente le sole misure tecniche necessarie al contenimento, preservando le evidenze e informando senza ritardo il Segretario Generale e i soggetti previsti dalla procedura incidenti. L'intervento è successivamente verbalizzato e sottoposto a convalida.

17.3 Separazione dei ruoli

Il Presidente esercita le funzioni di competenza dell'organo di vertice e autorizza i controlli riguardanti il Segretario Generale. Il Segretario Generale autorizza gli accessi per continuità

operativa e i controlli individuali, salvo i casi riservati al Presidente. Il Responsabile Area ICT e MEPA cura esclusivamente l'esecuzione tecnica e la custodia delle evidenze. Il RPD/DPO fornisce consulenza indipendente sui profili privacy senza assumere funzioni decisionali o operative. L'Area competente per il personale presidia gli eventuali profili disciplinari. I fornitori possono intervenire solo se formalmente autorizzati e vincolati da obblighi contrattuali e di riservatezza.

17.4 Procedura dei controlli individuali

L'atto di autorizzazione indica almeno: fatto o esigenza che giustifica il controllo; finalità; strumenti e categorie di dati interessati; periodo temporale; soggetti autorizzati; criteri di ricerca; durata; misure di minimizzazione; modalità di conservazione delle evidenze e termine di cancellazione. Ove possibile, si procede per gradi, privilegiando dati aggregati o anonimi e passando all'identificazione del singolo solo quando necessario.

L'attività è svolta da personale specificamente autorizzato. È redatto un verbale contenente data, soggetti presenti, attività compiute, dati consultati o acquisiti, esito, misure adottate e tempi di conservazione. L'interessato è informato dell'accesso alla prima occasione utile, salvo che ciò possa pregiudicare indagini, tutela giudiziaria, sicurezza o altri interessi legittimi documentati.

17.5 Accesso a posta elettronica, Teams, file e dispositivi

L'accesso al contenuto di posta elettronica, chat, file o dispositivi assegnati è ammesso solo quando strettamente necessario e non siano disponibili mezzi meno invasivi. Le ricerche devono essere effettuate, ove tecnicamente possibile, mediante criteri selettivi riferiti all'oggetto, al periodo e alle informazioni di servizio necessarie, evitando l'esame generalizzato dell'intero account. I contenuti manifestamente personali o estranei alla finalità non sono acquisiti e non sono ulteriormente trattati, salvo obblighi di legge.

17.6 Utilizzo e conservazione delle evidenze

Le informazioni lecitamente raccolte possono essere messe a disposizione esclusivamente dei soggetti competenti per la finalità perseguita. Le evidenze sono protette da accessi non autorizzati, ne sono garantite integrità e tracciabilità e sono conservate per il tempo strettamente necessario. Ogni ulteriore utilizzo incompatibile con la finalità originaria è vietato, fatti salvi gli obblighi di legge e la tutela dei diritti dell'Ente in sede giudiziaria.

18. Conservazione dei dati

I tempi di conservazione dei dati tecnici e dei log sono definiti dall'Ente in una matrice di conservazione, approvata e periodicamente riesaminata, che indica per ciascuna categoria almeno: finalità, base giuridica, sistemi interessati, soggetti autorizzati, periodo ordinario, criteri di eventuale estensione e modalità di cancellazione o anonimizzazione. I termini non sono determinati dalle sole impostazioni dei fornitori e devono essere proporzionati alle finalità documentate.

Per i dati di navigazione e i log del proxy è adottato il periodo più breve compatibile con le effettive esigenze di funzionamento, sicurezza e accertamento degli incidenti. Per i metadati della posta elettronica necessari al funzionamento del servizio si applicano le previsioni del capitolo 10.1. La conservazione per finalità ulteriori, o per periodi superiori a quelli ordinari, richiede una specifica valutazione documentata della base giuridica, della necessità e della compatibilità con l'art. 4 della legge n. 300/1970.

In casi eccezionali, per esigenze tecniche o di sicurezza documentate, gestione di incidenti, esercizio o difesa di un diritto o adempimento di richieste dell'Autorità giudiziaria o di altra autorità competente, i dati pertinenti possono essere conservati oltre il termine ordinario, limitatamente al tempo necessario e mediante segregazione selettiva.

Tali eventuali proroghe sono registrate e motivate nel rispetto delle prescrizioni AgID e della normativa in materia di protezione dei dati personali. L'Ente si impegna ad applicare le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore e dalle Linee guida AgID, predisponendo procedure interne idonee a garantire un trattamento conforme ai principi di integrità, riservatezza e tracciabilità, nonché verificando periodicamente l'adeguatezza delle misure adottate.

19. Sanzioni e norme finali

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL e, nei confronti degli altri utenti, verificata la gravità della violazione contestata,

con la risoluzione od il recesso dal contratto ad essi relativo nonché con tutte le azioni civili e penali consentite.

Il presente Regolamento è soggetto a revisione periodica con cadenza annuale.

Copia del presente Regolamento verrà affissa nella bacheca aziendale, anche per quanto prevede *l'art.7 della Legge n. 300/1970*, nonché ai fini *dell'art. 4, comma 3, dello Statuto dei lavoratori.*

Verrà inoltre reso disponibile per la visualizzazione e il download sul portale web dell'Ente e all'interno del portale web HR Infinity Zucchetti. Si invita a renderlo noto e richiederne l'applicazione, eventualmente richiamandolo, dove possibile, nella relativa documentazione contrattuale, anche a collaboratori, consulenti, agenti od altri incaricati esterni (es. incaricati software house, incaricati dei professionisti di cui si avvale l'Ente, ecc.) che venissero autorizzati a far uso di strumenti tecnologici dell'Ente o ad accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati. Pertanto, il presente regolamento entra a far parte, per quanto occorra, del Codice disciplinare aziendale.

Il presente Regolamento integra le regole di utilizzo degli strumenti dell'Ente. L'eventuale rilevanza disciplinare delle violazioni è valutata nel rispetto della legge, del CCNL applicabile, del Codice disciplinare vigente, dei principi di proporzionalità e delle garanzie del procedimento disciplinare. La pubblicazione e la comunicazione del Regolamento non sostituiscono gli ulteriori adempimenti richiesti dall'art. 7 della legge n. 300/1970.