DECRETO DEL PRESIDENTE

Adozione del Regolamento per l'utilizzo dei sistemi informatici e di telecomunicazione dell'Ente

IL PRESIDENTE

VISTO il D.Lgs. del 4 agosto 2016 n. 169 di riorganizzazione, razionalizzazione e semplificazione della disciplina concernente le Autorità Portuali di cui alla legge 28 gennaio 1994, n. 84 e il successivo D.Lgs. n. 232/2017 che aggiorna ed integra il precedente sopra citato;

VISTO il D.Lgs. del 4 agosto 2016 n. 169 di riorganizzazione, razionalizzazione e semplificazione della disciplina concernente le Autorità Portuali di cui alla legge 28 gennaio 1994, n. 84 e il successivo D.Lgs. n. 232/2017 che aggiorna ed integra il precedente sopra citato;

VISTO il Decreto del Ministro delle Infrastrutture e dei Trasporti n. 284 del 12 novembre 2025 con il quale il Dott. Matteo Gasparato è nominato Presidente dell'Autorità di Sistema Portuale del Mare Adriatico Settentrionale;

VISTO il 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)*" (di seguito RGPD), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, che introduce la figura del Responsabile dei dati personali (RDP) e il Decreto di adeguamento n. 101 del 4 settembre 2018;

CONSIDERATO quanto previsto dal provvedimento "Misure e accorgimenti prescritti per i titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008" (G.U. n. 300 del 24 dicembre 2008) del Garante per la protezione dei dati personali;

VISTI gli artt. 31, 34 e 35 del D. Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";

VISTI inoltre i provvedimenti dell'Autorità Garante per la protezione dei dati personali del Provvedimento del 12 febbraio 2009 (1598443) e del 25 giugno 2009 "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolai dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga i termini per il loro adempimento", relativi alle misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di "amministratore

di sistema", ai requisiti tecnici, professionali e di condotta dei soggetti incaricati all'assolvimento di tale ruolo e agli obblighi e alle modalità di nomina di uno o più incaricati;

Visto il Decreto n. 1985 del 27 dicembre 2016 "Adozione del Regolamento per l'utilizzo dei sistemi informatici e di telecomunicazione dell'Ente";

Visto il Decreto n. 346 del 12 dicembre 2019 "Adozione del Regolamento per l'utilizzo dei sistemi informatici e di telecomunicazione dell'Ente" che sostituiva il Decreto n. 1985 del 27 dicembre 2016;

RITENUTA la necessità di aggiornare gli atti di regolamentazione dell'uso dei sistemi informativi e di individuazione e gestione delle misure di sicurezza informatica in attuazione delle disposizioni recate dal D. Lgs. 4 settembre 2024, n. 138 e delle connesse direttive della Agenzia nazionale per la cybersicurezza nazionale;

SENTITO il Responsabile per la Transizione digitale e Direttore della Direzione Digitale e Innovazione, ing. Sebastiano Ferrara;

DECRETA

ARTICOLO 1 – Adozione
Con effetto immediato entra in vigore l'allegato Regolamento per l'utilizzo dei sistemi informatici e di telecomunicazione dell'Ente, che sostituisce quello precedente di cui al Decreto n. 346 del 12 dicembre 2019;

ARTICOLO 2 – Vigilanza
La Direzione Digitale e Innovazione è incaricata di vigilare sulla corretta applicazione del presente Regolamento attraverso la propria Area Gestione Operativa Servizi IT.

Il Presidente
Matteo Gasparato

Firmato digitalmente da:
MATTEO GASPARATO
Data: 31/12/2025 18:28:30

APPOSIZIONE NUMERO DI REPERTORIO

Il presente Decreto viene registrato nel Registro dei Decreti dell'Autorità di Sistema Portuale del Mare Adriatico Settentrionale in data 31/12/2025 con il numero 1511.

Decreto n. 1511 del 31/12/2025 - Adozione del Regolamento per l'utilizzo dei sistemi informatici e di telecomunicazione dell'Ente

Martina Buran
Ufficio Protocollo

Firmato digitalmente da:
MARTINA BURAN
Data: 31/12/2025 16:00:35

Autorità di Sistema Portuale
del Mare Adriatico Settentrionale
Porti di Venezia e Chioggia

Santa Marta, Fabbricato 13
30123 Venezia
T +39 041 533 4111
F +39 041 533 4254

C.F. e P.IVA: 00184980274
adspmas@port.venice.it
www.port.venice.it
PEC: autoritaportuale.venezia@legalmail.it

Funded by the European Union
NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Autorità di Sistema Portuale del Mare Adriatico Settentrionale
Porti di Venezia e Chioggia

Autorità di Sistema Portuale del Mar Adriatico Settentrionale

Regolamento per l'utilizzo dei Sistemi Informatici e di Telecomunicazione

Misura PNRR M1C1 | 1.5

Progetto "Potenziamento delle capacità di sicurezza informatica e innovazione nei porti di Venezia e Chioggia"

Sommario

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 "AdSP MAS") 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 AdSP MAS. 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 20.

I dati personali e le altre informazioni dell'utente registrati negli Strumenti Informatici o che si possono eventualmente raccogliere tramite il loro uso, sono trattati per esigenze organizzative

e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. Per tutela del patrimonio si intende altresì la sicurezza informatica e la tutela del sistema informatico. Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal *Regolamento (UE) 2016/679 "General Data Protection Regulation"*.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite ai soggetti autorizzati al trattamento (*ex art. 4, par. 10, del Regolamento (UE) 2016/679*) in attuazione del seguente quadro normativo:

- "*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*", in vigore in tutti gli Stati dell'Unione europea a partire dal 25 maggio 2018;
- *Direttiva (UE) 2022/2555 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 (direttiva NIS 2)*;
- *Decreto legislativo 10 agosto 2018, n. 101, che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679*;
- *D. Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", che contiene la disciplina rilevante in materia di privacy (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).*

- 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 aziendale, 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 Information Security Governance previsti dallo standard *ISO 27001:2022,* assume la responsabilità diretta della supervisione e dell'attuazione delle misure di sicurezza, approvando il presente regolamento e garantendo le risorse necessarie per la sua applicazione.

1. Riferimenti normativi

AdSP MAS si impegna a garantire la conformità a tutte le normative vigenti e alle loro evoluzioni, ai requisiti contrattuali, 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.

- Alla luce della *Legge 20.5.1970, n. 300*, 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 attuazione del *Regolamento Europeo 679/16 "General Data Protection Regulation*" (d'ora in avanti Reg. 679/16 o GDPR);
- In conformità alle *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*;
- Ai sensi delle "*Linee guida del Garante per posta elettronica e internet"* In Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- In attuazione della *Direttiva (UE) 2022/2555* relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (d'ora in avanti NIS2);

- In conformità allo standard *ISO/IEC 27001:2022* e in riferimento ai controlli di sicurezza come stabili all'interno dell'*Annex A;*
- In conformità alle linee guida *NIST SP 800-63 (Digital Identity Guidelines)* e ai controlli di sicurezza previsti da NIST SP 800-53 *(Security and Privacy Controls for Information Systems and Organizations)*;
- In coerenza con il *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, 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». La finalità è quella di promuovere una corretta "cultura informatica" affinché l'utilizzo degli Strumenti Informatici e telematici messi a disposizione dall'Ente sia conforme alle finalità per le quali sono state messe a disposizione del personale e nel pieno rispetto della legge. Si vuole fornire a tutto il personale le indicazioni necessarie con l'obiettivo principale 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".

È riconosciuto al datore di lavoro di potere svolgere attività di monitoraggio, che nella fattispecie saranno svolte solo dal Responsabile Area GOIT (cfr. Decreto Amministratori di Sistema) o dal personale da lui delegato, sempre nel pieno rispetto della normativa vigente.

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 Tecnology)	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 cloud.
Repository	Archivio centralizzato per conservare e gestire file, codice o documentazione, spesso con controllo delle versioni.
Separation Role	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 AdSP MAS 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. Catalogo servizi ICT e portale dei servizi integrati

In conformità con il Piano Triennale per l'Informatica (*cfr. Piano Triennale dell'Informatica*), il catalogo ICT di AdSP MAS raccoglie in modo strutturato le tipologie di servizio disponibili, i livelli di servizio garantiti (SLA), le modalità di richiesta e i canali di assistenza.

Ogni dipendente è tenuto a consultare il catalogo per individuare il servizio di interesse e seguire le procedure indicate per la richiesta o per l'assistenza.

Il portale dei servizi integrati costituisce il punto di accesso centralizzato ai servizi digitali e ai procedimenti amministrativi.

Tutti i dipendenti devono utilizzare il portale per l'erogazione e la gestione dei servizi, nel rispetto delle modalità di accesso e delle procedure pubblicate.

7. Gestione degli accessi

7.1 Gestione, assegnazione e revoca delle credenziali di accesso

7.1.1 Attivazione nuova utenza

Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dal Responsabile Area GOIT contestualmente all'*on-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 l'apertura di un ticket.

Nel caso di attivazione utenza per collaboratori esterni la richiesta dovrà essere inoltrata 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 GOIT, 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 8 caratteri, contenente lettere maiuscole, minuscole, numeri e caratteri speciali. Si consiglia di non inserire nella *password* riferimenti agevolmente riconducibili all'utente (*username*, nomi o date relative alla persona).

È necessario procedere alla modifica della *password* a cura dell'utente al primo accesso e, successivamente, almeno ogni sei mesi; in particolare, nel caso di trattamento 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*) la periodicità della variazione dovrà essere ridotta a tre mesi.

7.1.2 Password persa o dimenticata

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

Qualora l'utente venisse a conoscenza delle *password* di altro utente, è tenuto a darne immediata notizia al Responsabile Area GOIT, che provvederà ad informare l'utente ed effettuare 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 GOIT.

7.1.3 Cessazione utenza

Nel caso di cessazione del rapporto di lavoro con l'utente, questi verrà disabilitato nel Dominio e in tutti gli applicativi per i quali era stato autorizzato all'accesso/uso. Dopo aver disabilitato i permessi, il Responsabile dell'Area GOIT procede all'eliminazione dell'utenza dall'Active Directory.

7.1.4 Eccezioni

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

7.2 Autenticazione multifattoriale (MFA)

In combinazione alle credenziali, viene reso disponibile l'applicativo *Microsoft Authenticator*, da installare sul proprio dispositivo aziendale, quale strumento di supporto all'autenticazione multifattoriale.

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.

7.3 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 differenti (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 GOIT.

7.4 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 dati di accesso, 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 log vengono conservati per un periodo definito dalle *policy* del fornitore, generalmente compreso tra 6 e 12 mesi, salvo diversa disposizione normativa o esigenze legate a indagini. Al termine del periodo di conservazione i dati vengono eliminati in modo sicuro.

La consultazione dei log è strettamente riservata al personale autorizzato, al Responsabile della sicurezza interna, al Responsabile Area GOIT 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.

8. 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 7.1 "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 18. Ogni materiale personale rilevato dal Responsabile Area GOIT 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 18 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 GOIT 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, la cartella "Documenti" o "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come *Hard disk* portatili o *NAS* ad uso esclusivo. Tutte queste 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 GOIT 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, OneDrive, WeTransfer*, ecc.). In caso di necessità l'Ente metterà a disposizione modalità in linea con le presenti direttive.

Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia degli archivi, con cancellazione dei file obsoleti e/o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

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 GOIT 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 GOIT.

8.1 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 GOIT.

AdSP MAS, inoltre, mette a disposizione degli ospiti una rete WiFi dedicata (*WiFi Guest*), 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 AdSP MAS 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 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.

AdSP MAS 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 AdSP MAS. Ogni dipendente è tenuto a garantire la riservatezza e l'integrità delle informazioni gestite durante l'attività lavorativa agile.

Il Responsabile Area GOIT 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.

8.2 Monitoraggio e Logging

I log di accesso al sistema o alla Intranet sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso il Responsabile Area GOIT, 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 18 del presente Regolamento.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del *Regolamento Europeo 679/16 "General Data Protection Regulation"*.

9. 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. Ogni utilizzo non inerente all'attività lavorativa è vietato.

L'accesso agli Strumenti è protetto da *password*; per l'accesso devono essere utilizzati *username* e *password* assegnate dal Responsabile Area GOIT (*cfr. 7.1*). A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.

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 GOIT ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della *password* di accensione (BIOS), senza preventiva autorizzazione scritta da parte del Responsabile Area GOIT.

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

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 GOIT.

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 GOIT. 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 GOIT 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 GOIT.

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

Dal momento della cessazione del rapporto di lavoro 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 GOIT;
- Autorità Giudiziaria (sporgere denuncia);
- Direttore della propria Struttura di appartenenza.

9.1 Dispositivi BYOD (Bring You 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 GOIT, 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 GOIT, e comunque coperti da una licenza regolare e documentabile.

9.2 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 team ICT. L'inosservanza di queste disposizioni può esporre l'organizzazione a rischi significativi e comportare responsabilità disciplinari.

9.3 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 GOIT, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio informativo.

I controlli possono avvenire secondo le disposizioni previste al successivo capitolo 18 del presente Regolamento. Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del *Regolamento Europeo 679/16 'General Data Protection Regulation'*.

10. 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 GOIT.

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 GOIT 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 GOIT, ed in copia al Segretario Generale, 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 18 e 19 del presente Regolamento. Al termine dell'attività il Responsabile Area GOIT ripristinerà i filtri alla situazione iniziale.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di *remote banking*, acquisti on-line e simili, salvo i casi direttamente autorizzati per iscritto dal Segretario Generale e dal Responsabile Area GOIT, 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 per la sicurezza interna, del Responsabile Area GOIT e del Segretario Generale.

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, per il tramite del Responsabile Area GOIT, non effettua il controllo sistematico delle pagine web visualizzate dal singolo utente, né controlla con sistemi automatici i dati di navigazione dello stesso. Si informa tuttavia che al fine di garantire il Servizio Internet e la sicurezza dei sistemi informativi, nonché per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, l'Ente registra per un massimo di 365 giorni i dati di navigazione (file di log riferiti al traffico web). Eventuali controlli avverranno nelle forme indicate al successivo capitolo 18 del presente Regolamento. Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del *Regolamento Europeo 679/16 "General Data Protection Regulation*".

11. 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 7.1 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 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 a con 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 GOIT 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. Nel caso di allegati ancora più voluminosi è necessario rivolgersi per iscritto al Responsabile Area GOIT. 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.

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 GOIT 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 AdSP MAS 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.

11.1 Trattamento dei metadati

AdSP MAS, 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 metadati sono inscindibili dal messaggio e vengono registrati per garantire il corretto funzionamento delle infrastrutture di posta elettronica. La loro conservazione è limitata al tempo strettamente necessario, normalmente non superiore a 21 giorni, salvo casi particolari in cui, per esigenze tecniche o di sicurezza, il termine possa essere esteso.

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.

11.2 Gestione della casella di Posta Elettronica e conservazione dei messaggi

Si informa che, ai sensi dell'*articolo 2214 del Codice civile e dell'articolo 22 del D.P.R. 600/73*, l'Ente deve conservare per dieci anni sui propri Server tutti e soli i messaggi di posta elettronica a contenuto di rilevanza giuridica e commerciale provenienti da e diretti a domini della stessa; sarà cura del dipendente, ove cessato, segnalarne la rilevanza ed inoltrare tali messaggi al destinatario delle proprie consegne, così come individuato dall'Ente.

Si informa altresì che l'Ente, per il tramite del Responsabile Area GOIT, non controlla sistematicamente il flusso di comunicazioni e-mail né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail. Tuttavia, in caso di assenza improvvisa o prolungata dell'utente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, ovvero per motivi di sicurezza del sistema informatico, l'Ente per il tramite del Responsabile Area GOIT può, secondo le procedure indicate al successivo capitolo 18 del presente Regolamento, accedere all'account di posta elettronica, prendendo visione dei messaggi, salvando o cancellando file.

Si informa inoltre che, in caso di cessazione del rapporto lavorativo, verrà immediatamente inibito l'accesso alla casella e-mail affidata all'incaricato, che rimarrà comunque attiva con apposito messaggio di risposta automatica per n. 30 giorni, al termine dei quali verrà completamente disattivata e i contenuti cancellati, salvo quanto sopra previsto. Le

informazioni eventualmente raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del *Regolamento Europeo 679/16 "General Data Protection Regulation*".

12. 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 GOIT. 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 esclusivamente a scopi professionali. Anche su tali strumenti di messaggistica istantanea è attivo il monitoraggio e la registrazione dell'attività degli utenti, secondo le disposizioni dei punti 18 e 19 del presente Regolamento.

L'applicativo utilizzato per la messaggistica istantanea interna è *Microsoft Teams*. L'utenza associata al servizio coincide con quella configurata per Outlook, garantendo continuità tra le funzionalità dell'ecosistema. In tal modo è possibile contattare direttamente i mittenti delle e-mail ricevute tramite Outlook sul relativo account Teams, verificarne la disponibilità e organizzare riunioni o *meeting* online attraverso entrambe le applicazioni. Parallelamente, anche su Teams è consultabile il profilo dell'utente con cui si intende interagire, comprensivo del ruolo e delle connessioni con altri utenti.

Oltre alle conversazioni individuali, l'utente può collaborare mediante chat di gruppo o canali dedicati (Team), concepiti come repository per documenti di lavoro, attività assegnate e materiali condivisi tramite collegamenti ipertestuali.

All'interno dei canali possono lavorare simultaneamente sullo stesso documento più utenti abilitati, apportando modifiche e commenti. In funzione delle esigenze operative, i membri del team possono essere aggiunti o rimossi in qualsiasi momento, nel rispetto del principio del privilegio minimo ("*least privilege*").

In ottemperanza al principio di separazione dei ruoli ("*role separation*"), è possibile concedere ad un utente l'accesso esclusivo a determinate sezioni o cartelle del canale, permettendogli di consultare, modificare e condividere solo determinati documenti.

Questo strumento permette infatti di sfruttare l'immediatezza della corrispondenza, adatta anche a toni informali, così come di tenere traccia delle attività da svolgere, di richieste attinenti alle operazioni in cui si è coinvolti, e attività similari.

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.

I dipendenti di AdSP MAS possono inoltre installare sul proprio dispositivo mobile applicazioni di messaggistica istantanea esterna, come ad esempio *Whatsapp*, previa autorizzazione da parte del Responsabile Area GOIT. L'utilizzo di questi canali di comunicazione e la fruizione dei contenuti online deve avvenire in modo consapevole e con la dovuta cautela, al fine di evitare potenziali fughe o esfiltrazioni di dati.

Per quanto riguarda l'utilizzo di applicazioni esterne, si applicano le medesime buone pratiche previste per le chat di *Teams*, trattandosi di strumenti destinati principalmente allo scambio di comunicazioni scritte.

È altresì ribadito il divieto di uso promiscuo dei canali di comunicazione ufficiali tramite dispositivi personali, con espresso divieto di impiegare i suddetti *social media* e applicazioni per finalità diverse da quelle strettamente operative, garantendo al contempo un comportamento conforme e rispettoso che non comprometta la reputazione di AdSP MAS.

13. 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, rimanendo escluse iniziative individuali da parte dei 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 AdSP MAS, 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.

14. Telefoni, fax, 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. 9), 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. 10).

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

È vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, fatta salva esplicita autorizzazione da parte del Responsabile di Ufficio.

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.

15. Assistenza agli utenti e manutenzioni

Il Responsabile Area GOIT 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 GOIT 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 GOIT, 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 GOIT 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 GOIT utilizzando l'apposito applicativo per l'Help Desk (http://apvticketing.intranet.apv) oppure, in alternativa se l'applicativo non è raggiungibile, via telefono interno al 4285 o 4261.

16. 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 a 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*).

16.1 Ambiente Cloud

AdSP MAS trasferisce i propri applicativi in ambiente Cloud per garantire sicurezza, continuità operativa e facilità di accesso. Tutti i dipendenti devono utilizzare esclusivamente le piattaforme cloud aziendali 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 cloud deve essere segnalata tempestivamente al Responsabile competente. Alla cessazione del rapporto di lavoro, l'accesso ai sistemi cloud viene disabilitato e il dipendente non è più autorizzato a utilizzare alcuna risorsa digitale dell'Ente.

16.2 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.

17. 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.

17.1 Segnalazione tempestiva

Ogni utente è tenuto a segnalare immediatamente qualsiasi evento o anomalia che possa (ad es. malfunzionamento PC, indisponibilità dei servizi applicativi e di rete) al Responsabile Area GOIT, secondo le modalità previste al precedente capitolo 15, che raccoglierà le segnalazioni e avvierà il relativo processo di classificazione e risoluzione dell'incidente medesimo al fine dl minimizzare gli eventuali impatti negativi sul normale svolgimento delle attività lavorative.

In conformità all'*art. 20 della Direttiva NIS2*, gli incidenti significativi devono essere portati all'attenzione dell'alta direzione, in quanto responsabile dell'approvazione e della supervisione delle misure di sicurezza e della conformità normativa.

L'alta direzione deve garantire che la segnalazione sia valutata tempestivamente e che siano adottate le decisioni necessarie per la gestione dell'incidente, inclusa l'eventuale notifica al CSIRT nazionale o all'autorità competente designata.

AdSP MAS 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.

17.2 Data Breach

Ogni incidente che coinvolge dati personali (cd. "*data breach*") deve essere segnalato in modo tempestivo al Responsabile Area GOIT, secondo le modalità previste al precedente capitolo 15, 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.

Per ottemperare agli obblighi imposti dalla normativa europea ogni utente, nel caso di incidente di una certa gravità sotto il profilo del rischio per i diritti e le libertà delle persone fisiche (*considerando 85, Regolamento (UE) 2016/679*); chiunque evidenzi un *data breach* deve comunicare il fatto al Responsabile del trattamento (DPO), il quale è tenuto ad avvisare il Titolare del trattamento. La notifica alle autorità è obbligatoria nel caso in cui il *data breach* rischi di ledere i diritti e le libertà degli interessati.

18. Controlli sugli Strumenti (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16)

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. Il datore di lavoro, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (*art. 4, comma 2*), di Sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la

necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. I controlli devono essere effettuati nel rispetto dell'art. 2 del presente Regolamento e dei seguenti principi:

- **Proporzionalità:** il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi.
- **Trasparenza:** l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.
- **Pertinenza e non eccedenza:** ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

L'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle Informazioni sul relativo uso, come analiticamente spiegato nei precedenti capitoli del presente Regolamento. Tali informazioni, che possono contenere dati personali eventualmente anche di categoria particolare relativi all'Utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite del Responsabile Area GOIT, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi (di seguito descritti ai due punti seguenti) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli Strumenti.

Controlli per la tutela del patrimonio nonché per la sicurezza e la salvaguardia del sistema informatico o per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/Implementazione di programmi, manutenzione hardware, ecc.). Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni descritte ai capitoli 7.4, 8.2, 9.3 e 11.2 il

Titolare/Responsabile del trattamento dei dati personali per il tramite del Responsabile Area GOIT, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo):

1. Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento;

2. Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni descritte ai capitoli 7.4, 8.2 e 11.2 con possibilità di rilevare file trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite;

3. Qualora il rischio di compromissione del sistema informativo sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai capitoli 1 e 4, Il Titolare/Responsabile del Trattamento, unitamente al Responsabile Area GOIT, potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia prendendo tutte le misure tecnicamente necessarie alla soluzione del problema.

Controlli per esigenze produttive e di organizzazione. Per esigenze produttive e di organizzazione si intendono - fra le altre - l'urgente ed improrogabile necessità dl accedere a file o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un utente (quali file salvati, posta elettronica, chat, SMS, etc.) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato. Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni descritte ai capitoli 7.4, 8.2, 9.3 e 11.2 il Titolare/Responsabile del Trattamento, per il tramite del Responsabile Area GOIT, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo):

- Redazione di un atto da parte del Direttore e/o Responsabile Area che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento;
- Incarico al Responsabile Area GOIT di accedere alla risorsa con credenziali di Amministratore oppure tramite l'azzeramento e la contestuale creazione di nuove credenziali dI autenticazione dell'utente interessato, con avviso che al primo accesso alla risorsa, Io stesso dovrà inserire nuove credenziali;
- Redazione di un verbale che riassuma i passaggi precedenti.

In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e dl organizzazione del lavoro.

Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal *Regolamento Europeo 679/16 "General Data Protection Regulation".*

Tutti i controlli sopra descritti avvengono nel rispetto del principio di necessità e non eccedenza rispetto alle finalità descritte nel presente Regolamento. Dell'attività sopra descritta viene redatto verbale, sottoscritto dal Titolare/Responsabile del Trattamento e dal Responsabile Area GOIT che ha svolto l'attività. In caso di nuovo accesso da parte dell'utente allo Strumento informatico oggetto di controllo, Io stesso dovrà avvenire previo rilascio di nuove credenziali (salvo diverse esigenze tecniche). Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal *Regolamento Europeo 679/16* "*General Data Protection Regulation*".

19. Conservazione dei dati

In riferimento agli articoli *5 e 6 del Reg. 679/16* e in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad internet e dal traffico telematico (log di sistema e del server *proxy*), la cui conservazione non sia necessaria, saranno cancellati entro al massimo 365 giorni dalla loro produzione.

Tale termine è applicato in coerenza con quanto previsto dalle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici, che richiedono agli enti pubblici di definire tempi di conservazione proporzionati e basati su finalità specifiche, documentate e legittime, nonché nel rispetto dei principi di minimizzazione e limitazione della conservazione stabiliti dal GDPR. AdSP MAS, nel definire tali tempi, tiene conto anche delle indicazioni delle Linee guida AgID relative alla sicurezza informatica e alla gestione dei log, secondo cui i sistemi devono assicurare integrità, autenticità, disponibilità e riservatezza delle informazioni conservate. La durata della conservazione dei log, pur rimanendo fissata nel limite massimo sopra indicato, deve essere valutata dall'Ente anche alla luce delle effettive esigenze operative e tecniche, privilegiando - ove possibile - conservazioni più brevi quando non strettamente necessarie.

In casi eccezionali, ad esempio per esigenze tecniche o di sicurezza o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate.

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.

20. 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, nella sezione MyWork di ciascun dipendente. 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 dell'Ente.