CONSIGLIO REGIONALE DELLA SARDEGNA

PIANO TRIENNALE PER L'INFORMATICA 2021-2023

INDICE

CRONOLOGIA REVISIONI E SINTESI MODIFICHE

Data	Versione	Provvedimento di Approvazione	Sintesi delle modifiche
28/02 /2022			4\4
0.<			

ACRONIMI E DEFINIZIONI

Accessibilità	Insieme di regole finalizzate a rendere accessibili strumenti, dati e servizi anche a persone con disabilità
AgID	Agenzia per l'Italia Digitale
ANA	Anagrafe Nazionale degli Assistiti
ANAC	Autorità Nazionale Anticorruzione
ANNCSU	Archivio Nazionale dei Numeri Civici delle Strade Urbane (banca dati)
ANPR	Anagrafe Nazionale della Popolazione Residente
AOO	Area organizzativa omogenea
API	Application Programming Interface - interfaccia per la programmazione di applicazioni
Base dati catastale	Banca dati del sistema catastale nazionale
BDAP	Banca dati delle operazioni contabili delle Pubbliche amministrazioni
BDNCP	*Banca Dati* Nazionale dei Contratti Pubblici
BPM	Business process management
CAD	Codice dell'Amministrazione Digitale
CED	Centro Elaborazione Dati
CEF	Connecting Europe Facility - Programma europeo noto come "Meccanismo per collegare l'Europa"
CERT	Computer Emergency Response Team- struttura per la risposta ad emergenze informatiche
CKAN	Comprehensive Kmowledge Archive Network
CIE	Carta di Identità elettronica (evoluzione del documento cartaceo, gestita a livello nazionale)

Cloud Marketplace AgID	Catalogo dei servizi e delle infrastrutture qualificate da AgID
CNS	Carta Nazionale dei Servizi
Consip	Concessionaria servizi informativi pubblici
CSIRT Italia	Centro per la sicurezza informatica nazionale che sostituisce CERT-PA
CSP	Cloud Service Provider - Fornitore di servizi cloud
DAF	Data & Analytics Framework - piattaforma per la valorizzazione del patrimonio informativo pubblico
DCAT-AP IT	Data Catalogue Vocabulary – Application Profile Italia - profilo applicativo del vocabolario “Data Catalog Vocabulary”
Developers Italia	Piattaforma che contiene il catalogo del software pubblico e che offre risorse utili per lo sviluppo dei servizi digitali
DIS	Dipartimento nazionale Informazioni per la Sicurezza
DPO	Data Protection Officer - Responsabile Protezione Dati
eIDAS	Electronic Identification Authentication & Signature - regolamento europeo per l’identificazione elettronica e servizi fiduciari
EIF	European Interoperability Framework - quadro europeo di interoperabilità
EIP-SCC	European Partnership on Smart City and Communities - partenariato europeo su smart city e communities
FatturaPA	Sistema di fatturazione elettronica attiva e passiva
FICEP	First Italian Crossborder eIDAS Proxy - progetto nazionale per la realizzazione del nodo eIDAS italiano
FNCS	Framework nazionale per la Cyber Security
FNCS	Framework Nazionale per la Cyber Security
GDPR	General Data Protection Regulation - Regolamento europeo sulla protezione dei dati
IaaS	Infrastructure as a Service – modello di servizio CLOUD
ICT	Information and Comunications Technology - tecnologia dell’informazione e della comunicazione
INAD	Indice nazionale dei domicili digitali delle persone fisiche e degli altri enti di diritto privato non tenuti all’iscrizione in albi professionali
infosec.cert-pa.it	Servizio Cert-PA che ha lo scopo di fornire uno strumento per una corretta valutazione delle minacce cibernetiche portate verso le infrastrutture informatiche.
INI-PEC	Indice Nazionale degli Indirizzi di Posta Elettronica Certificata di professionisti e imprese
INSPIRE	Infrastruttura per l'Informazione Territoriale in Europa
IoC	Indicatori di compromissione (artefatto che con alta probabilità indica un’intrusione informatica)

IPA	Indice delle Pubbliche Amministrazioni
ISA	Interoperability solutions for public administrations, businesses and citizens - soluzioni di interoperabilità per amministrazioni pubbliche, imprese e cittadini
LAnn	Acronimo seguito da un numero che indica la linea di azione prevista per un determinato argomento dal Piano Triennale per la Transazione al Digitale
Lavoro agile	Definito nell'ordinamento italiano come modalità di esecuzione del rapporto di lavoro subordinato senza precisi vincoli di orario o luogo di lavoro. E' anche noto come smart working
malware	Software codice anche contenuto in un documento in grado di apportare danni ad un sistema informatico
MIUR	Ministero dell'Istruzione, dell'Università e della Ricerca
NDV	National Vulnerability Database - repository governativo statunitense di dati sulla gestione delle vulnerabilità
NoiPA	Sistema per la gestione dei dati dei dipendenti delle PA
NSO	Nodo di smistamento degli ordini di acquisto delle PA
Open source	Software il cui codice sorgente è rilasciato con una licenza che lo rende modificabile o migliorabile da parte di chiunque
PA	Pubbliche Amministrazioni
PaaS	Platform as a Service – modello di servizio CLOUD
PAC	Pubblica amministrazione centrale
PagoPA	Sistema di pagamenti elettronici verso la PA
PAL	Pubblica amministrazione locale
PDNT	Piattaforma Digitale Nazionale Dati
PEC	Posta elettronica certificata
PEO	Posta elettronica ordinaria
Piano	Piano triennale per l'informatica nella Pubblica Amministrazione 2020 - 2022
PRA	Pubblico Registro Automobilistico
procurement	electronic procurement - processo di "approvvigionamento elettronico", cioè di procacciamento e acquisizione di beni e servizi attraverso Internet
PSN	Polo strategico nazionale
PSP	Prestatori di servizi di pagamento sistema PagoPA
Registro Imprese	Anagrafe nazionale delle imprese (banca dati)

RNDT	Repertorio Nazionale Dati Territoriali (banca dati)
RTD	Responsabile della Transazione al Digitale (art. 17 , c. 1 CAD)
SaaS	Software as a Service – modello di servizio CLOUD
SAML	Security Assertion Markup Language - standard informatico per lo scambio di dati di autenticazione e autorizzazione tra. domini di sicurezza distinti
SBN	Catalogo del servizio Bibliotecario Nazionale
servizi.gov.it	Base dati del catalogo nazionale dei servizi pubblici a cittadini e imprese
SGPA	Sistema di Gestione dei Procedimenti Amministrativi nazionali
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
SINFI	Sistema Informativo Nazionale Federato delle Infrastrutture
SIOPE	Sistema informativo sulle operazioni degli enti pubblici
SPC	Sistema Pubblico di Connettività
Siope - Siope+	Sistema informativo sulle operazioni degli Enti Pubblici e sua evoluzione
SPID	Sistema Pubblico di Identità Digitale
PSN	Polo Strategico Nazionale
PDND	Piattaforma Digitale Nazionale Dati
VPN	Acronimo di Virtual Private Network – canale di comunicazione riservato anche utilizzato per accedere dall'estero alle reti territoriali provate
WAI	Acronimo di Web Analytics Italia - piattaforma nazionale di raccolta ed analisi dei dati statistici relativi al traffico dei siti e servizi delle PA.
WCAG	Web Content Accessibility Guidelines - linee guida per l'accessibilità dei contenuti web
WiFi	Tecnologia per la distribuzione di connessione internet senza l'utilizzo di fili

RIFERIMENTI NORMATIVI

- Legge 9 gennaio 2004, n. 4 “Disposizioni per favorire e semplificare l’accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici”.
- Decreto Legislativo 7 marzo 2005, n.82 “Codice dell’Amministrazione Digitale”.
- DPCM 1° Aprile 2008 “Regole tecniche e di sicurezza per il funzionamento del Sistema Pubblico di Connettività» previste dall’art. 71 c.1 bis del D.Lgs. 7 marzo 2005, n.82, recante il Codice dell’Amministrazione Digitale”.
- Decreto Legge 18 ottobre 2012, n. 179 “Ulteriori misure urgenti per la crescita del Paese, art. 9, comma 7”.
- DPCM 24 gennaio 2013 “Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale”.
- DPCM 3 dicembre 2013 “Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005”.
- DPCM 3 dicembre 2013 “Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005”.
- D.L. 24 aprile 2014, n.66 “Misure urgenti per la competitività e la giustizia sociale”.
- DL 24 giugno 2014, n.90 “Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari”, convertito nella legge 11 agosto 2014, n.114.
- DPCM 24 ottobre 2014 “Definizione delle caratteristiche del Sistema Pubblico per la gestione dell’Identità Digitale (SPID) nonché dei tempi e delle modalità di adozione del sistema SPID da parte della Pubblica Amministrazione e delle imprese”.
- DPCM 13 novembre 2014 “Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005”.
- DPR 28 dicembre 2000, n. 445 “disposizioni legislative in materia di documentazione amministrativa, di seguito «Testo unico», e la gestione informatica dei documenti”.
- Regolamento UE n° 910/2014 “EIDAS (electronic Identification Authentication and Signature)”.

- Legge n. 124 del 07/08/2015 (Riforma Madia) “Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche” recante norme relative alla cittadinanza digitale.
- DL n. 179 del 2016 “Modifiche e integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche" (CAD 3.0).
- D.Lgs. 97/2016 (FOIA) Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità' e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche
- Regolamento UE 679/2016 (trattamento e circolazione dei dati personali).
- Direttiva UE 2016/2102 del Parlamento Europeo e del Consiglio del 26 ottobre 2016 (relativa all’accessibilità dei siti web e delle applicazioni mobili degli enti pubblici).
- DPCM 31 maggio 2017 “Piano Triennale 2017-2019 per l'informatica nella Pubblica Amministrazione”.
- Legge 22 maggio 2017, n. 81 Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato (lavoro agile);
- Circolare AGID n.2/2018 “Criteri per la qualificazione dei Cloud Service Provider per la PA”.
- Circolare AGID n.3/2018 “Criteri per la qualificazione di servizi SaaS per il Cloud della PA”.
- Decreto Legislativo 10 agosto 2018, n. 106 “Attuazione della direttiva (UE) 2016/2102 relativa all’accessibilità dei siti web e delle applicazioni mobili degli enti pubblici”.
- Regolamento (UE) 2018/1724 del Parlamento Europeo e del Consiglio del 2 ottobre 2018 che istituisce uno sportello digitale unico per l’accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE).
- D.P.C.M. del 21 febbraio 2019 “Piano triennale 2019 – 2021 per l'informatica nella Pubblica Amministrazione”.
- DPCM del 08/08/2019 (GU 08/11/2019) in materia di “Disposizioni sull’organizzazione e il funzionamento del Computer Security Incident Response Team – CSIRT italiano”.
- Linee guida di design per i servizi digitali della PA
- Linee guida sull’accessibilità degli strumenti informatici
- Linee guida per la formazione, gestione e conservazione dei documenti informatici
- Linee Guida AGID sull’acquisizione e il riuso del software per la Pubblica Amministrazione
- Linee guida per la sicurezza nel procurement ICT.

- Misure minime di sicurezza ICT per le Pubbliche Amministrazioni
- DPCM 17/07/2020 “Piano triennale 2020 – 2022 per l'informatica nella Pubblica Amministrazione”.
- Legge 11 settembre 2020, n. 120 (GU n. 228 del 14/09/2020) di conversione, con modificazioni, del D.L. n. 76/2020 recante «Misure urgenti per la semplificazione e l’innovazione digitali» (Decreto Semplificazioni).
- Decreto Semplificazioni "bis" - Decreto Legge 31 maggio 2021 n. 77.
- Legge Cost. 26 febbraio 1948 n. 3 Statuto speciale per la Sardegna.
- Regolamento interno del Consiglio regionale della Sardegna (approvato nella seduta antimeridiana del 22 luglio 1988. Modificato nelle sedute del 23 febbraio 1993, 25 febbraio e 9 marzo 1999, 4 ottobre 2000, 22 settembre 2005, 11 dicembre 2012 e 22 luglio 2013).
- Legge regionale 17 gennaio 1989, n. 4 Modifiche alla legge regionale 4 giugno 1988, n. 11 e disposizione varie (istituzione del difensore civico)
- Legge regionale 28 luglio 2008, n. 11 Istituzione del Comitato regionale per le comunicazioni (CORECOM) della Regione autonoma della Sardegna e Legge Regionale 30 giugno 2011, n. 15 Modifiche alla legge regionale 28 luglio 2008, n. 11.
- Legge regionale 7 febbraio 2011, n. 7 Sistema integrato di interventi a favore dei soggetti sottoposti a provvedimenti dell'autorità giudiziaria e istituzione del Garante delle persone sottoposte a misure restrittive della libertà personale.
- Legge regionale 7 febbraio 2011, n. 8 Istituzione del Garante regionale per l'infanzia e l'adolescenza.

PREMESSA

La redazione del "Piano Triennale per l'Informatica" da parte delle singole amministrazioni è stata raccomandata dalla Circolare del Ministro per la pubblica amministrazione n. 3 del 1° ottobre 2018, configurandola come una linea di attività da esplicitare nell'atto di nomina del responsabile per la transizione digitale, di cui ciascuna amministrazione deve dotarsi ai sensi dell'art. 17, comma 1, del Codice dell'amministrazione digitale. (rif. Normativo Decreto Legislativo 7 marzo 2005, n.82 "Codice dell'Amministrazione Digitale").

Esso rappresenta un utile strumento per perseguire le finalità previste dal "Piano triennale per l'informatica nella pubblica amministrazione", elaborato a livello statale, ormai giunto alla terza edizione (2021-2023).

Quest'ultima, diversamente dalle precedenti, orientate ad introdurre ed implementare un nuovo modello strategico dell'informatica nella pubblica amministrazione, pone l'accento sulla realizzazione degli obiettivi da parte delle singole amministrazioni e sulla misurazione dei risultati raggiunti.

In tale ambito diventa, quindi, centrale l'attività di monitoraggio che necessita di un atto di pianificazione il quale, nel caso di specie, essendo il primo predisposto da questo Ente, dovrà dare conto anche di quanto realizzato in precedenza.

Il Consiglio regionale della Sardegna, con la redazione del presente piano, si propone, pertanto, di effettuare una ricognizione di tutte le attività già poste in essere per realizzare il nuovo modello di amministrazione delineato dal Codice dell'amministrazione digitale (D. Lgs n. 82/2005) e di enucleare le azioni che intende attuare nell'arco del triennio.

La pandemia da Covid-19 ha determinato una dilazione diffusa e generalizzata degli adempimenti di evoluzione informatica imposti dal Codice dell'amministrazione digitale. In realtà, la transizione al digitale nella pubblica amministrazione ha mostrato un incedere lento già prima del verificarsi dell'emergenza sanitaria, tant'è che il legislatore è intervenuto, con la novella di cui al Dlgs. 179/2016, per istituire una figura cardine all'interno di ciascun Ente che accentri i compiti e le responsabilità relativi al passaggio al nuovo modello di amministrazione pubblica: il Responsabile della Transizione al Digitale (RTD).

Ogni amministrazione, pertanto, deve individuare un unico ufficio di livello dirigenziale che si occupi della materia.

Il Consiglio regionale della Sardegna ha adempiuto a tale onere con deliberazione dell'Ufficio di Presidenza n. 157 del 30 novembre 2021, la quale, dato atto dell'assenza di un servizio interno dedicato all' *Information and Communication Technologies (ICT),* ha scelto il responsabile tra i titolari di incarichi dirigenziali di vertice, in base alle competenze amministrative e organizzative possedute.

La stessa delibera ha previsto poi la creazione di un gruppo di lavoro permanente idoneo a supportare la Responsabile per la transizione digitale nell'espletamento dei propri compiti, costituito con nota del Segretario generale n. 888 del 2 febbraio 2022.

Tale gruppo ha cominciato ad operare, con l'ausilio di una società esterna, ponendosi come primo obiettivo proprio la predisposizione del Piano triennale per l'informatica.

Il Consiglio regionale della Sardegna, inoltre, nella persona del Responsabile per la transizione digitale, ha stipulato un accordo con la Regione Autonoma della Sardegna, finalizzato alla collaborazione tra i due enti per la realizzazione di attività congiunte relative alla condivisione infrastrutturale e applicativa di sistemi informativi e telematici e per la concessione reciproca di luoghi fisici per la collocazione dei server presso i rispettivi data center.
In particolare si prevede la condivisione di interventi di natura tecnologica, lo scambio di servizi di alta qualificazione e di *know how*, nel settore dei sistemi informativi e telematici.
Pur essendo, il presente documento, il primo Piano triennale per l'informatica adottato dalla Amministrazione consiliare, l'Ente ha già da tempo avviato processi volti ad incentivare l'informatizzazione e la digitalizzazione per favorire lo snellimento dei procedimenti, oltre a razionalizzare e semplificare le attività gestionali, i documenti, la modulistica.
Negli ultimi anni, infatti, sono state adottate scelte di innovazione informatica in diversi ambiti.
In riferimento alla sicurezza informatica, l'Amministrazione si è dotata di sistemi di *firewall* e antivirus di ultima generazione, costantemente aggiornati nelle ultime versioni, e ha adottato sistemi di virtualizzazione dei *server*, anch'essi aggiornati.
Si è proceduto ad implementare un servizio di *email* interno.
È stato effettuato il passaggio del sito web dell'Ente, precedentemente in versione statica, ad un sistema CSM (nello specifico WordPress) in quanto la precedente versione risultava non ottimale per soddisfare gli obiettivi di accessibilità.
Si tratta ora di avviare azioni specifiche atte a favorire la digitalizzazione, nella consapevolezza che ciò costituisca un percorso complesso che richiede un cambio di mentalità e di organizzazione della struttura, in cui tutti i soggetti che prestano servizio all'interno dell'Amministrazione devono essere coinvolti.
E' necessario adottare un approccio culturale differente, in cui la cosiddetta "trasformazione digitale" si traduca in un miglioramento delle prestazioni delle persone (produttività), per migliorare i processi (efficienza) e, infine, i prodotti e i servizi offerti.
Per comprendere le particolarità con le quali può estrinsecarsi il processo di transizione al digitale e gli obiettivi specifici che lo stesso può perseguire in concreto è necessario effettuare un inquadramento giuridico dell'Ente.
Il Consiglio regionale, quale organo titolare della funzione legislativa e regolamentare della Regione Autonoma della Sardegna (art. 27 Statuto speciale, approvato con la legge costituzionale n. 3 del 1948), non svolge compiti di amministrazione attiva, né eroga servizi ai cittadini.
L'unica eccezione è rappresentata dal Servizio per le Autorità di Garanzia, (ovvero i servizi e le segreterie a supporto del Comitato Regionale per le Comunicazioni, del Garante regionale per l'infanzia e l'adolescenza, del Garante delle persone sottoposte a misure restrittive della libertà personale, del Difensore Civico), incardinato nell'Amministrazione consiliare, che fornisce servizi direttamente rivolti ai cittadini.
In particolare, il Co.re.com gestisce i procedimenti volti alla risoluzione delle controversie tra utenti e operatori di telefonia, Internet e pay-tv; raccoglie e gestisce le segnalazioni inerenti il rispetto della normativa vigente in tema di programmazione da parte dei fornitori di servizi media audiovisivi locali; gestisce i procedimenti di iscrizione e di aggiornamento al Registro degli operatori di comunicazione (Roc) operanti in Sardegna; gestisce le istruttorie inerenti le istanze in

materia di diritto di rettifica. Il Garante regionale per l'infanzia e l'adolescenza e il Garante delle persone sottoposte a misure restrittive della libertà personale raccolgono e gestiscono le segnalazioni pervenute direttamente dai cittadini in merito, rispettivamente, alla violazione dei diritti dei soggetti di minore età e di persone sottoposte a misure restrittive della libertà personale. Il Difensore civico al quale è possibile rivolgersi per mancata o insoddisfacente risposta a richiesta di notizie sullo stato di una pratica o di un procedimento riceve e gestisce le segnalazioni in materia di diritto di accesso agli atti e di accesso civico nell'ambito di procedimenti amministrativi.

Come già precisato, le attività che derivano dalle funzioni degli organi di garanzia, rappresentano una singolarità nell'ambito di una amministrazione volta al supporto della funzione legislativa e regolamentare.

In merito all'attività istituzionale, va detto, che le sedute del Consiglio regionale della Sardegna, ai sensi dell'art. 22 dello Statuto speciale sono pubbliche: tale obbligo corrisponde ad un'essenziale esigenza di informazione e controllo da parte del corpo elettorale.

Le forme con le quali viene assicurata la pubblicità sono disciplinate dal Regolamento interno consiliare che prevede la presenza del pubblico e la trasmissione televisiva delle sedute del Consiglio.

Da tale principio deriva, inoltre, il vincolo di documentazione dei lavori consiliari, in particolare la redazione e pubblicazione di una sintesi e di un resoconto integrale.

L'onere di pubblicità viene assolto con modalità digitali mediante il sito web del Consiglio regionale della Sardegna, attraverso due principali canali: il video in diretta streaming delle sedute, con relativo archivio delle precedenti, e la pubblicazione dei resoconti integrali delle sedute stesse.

Inoltre, in ossequio al generale principio di trasparenza dei vari livelli dell'attività di governo, che permea il nostro ordinamento, mediante un lento e progressivo processo di smaterializzazione di atti e documenti, vengono rese fruibili sul sito web una serie di informazioni riguardanti l'attività istituzionale.

La digitalizzazione dei documenti ha consentito al Consiglio regionale di creare delle banche dati che, attraverso i motori di ricerca, agevolano la consultazione di progetti di legge, atti di indirizzo e controllo e altri documenti che non rientrano nell'attività legislativa.

Tali strumenti sono utili per il cittadino che voglia conoscere l'attività dell'organo legislativo, ma anche per gli stessi Consiglieri, i loro collaboratori e i portatori di interessi in generale.

In relazione al periodo di riferimento del presente Piano il Consiglio Regionale della Sardegna intende perseguire i seguenti obiettivi generali:

- adozione di modalità organizzative e tecniche attraverso l'implementazione di sistemi di interoperabilità in particolare con le amministrazioni del sistema Regione;
- rafforzamento delle competenze informatiche, accompagnate da quelle inscindibili di protezione dei dati personali trattati con modalità digitali, per garantire il miglioramento delle capacità professionali e un'effettiva trasformazione culturale del personale consiliare;
- attivazione di misure volte alla semplificazione e razionalizzazione dei processi interni attraverso l'utilizzo delle tecnologie digitali;

- utilizzo delle tecnologie innovative (ICT) da applicare alle attività consiliari al fine di migliorare l'accessibilità alle informazioni e di rafforzare gli adempimenti connessi al principio di pubblicità;
- miglioramento della qualità dei dati e dei metadati attraverso il rafforzamento della componente open data al fine di favorirne la condivisione e promuovere il riutilizzo;
- incremento della qualità e della sicurezza dei servizi e delle infrastrutture ICT anche attraverso la migrazione ai sistemi cloud;
- potenziamento dei sistemi di protezione dei dati (cyber sicurezza) anche in relazione agli aspetti connessi al rispetto della normativa in materia di tutela dei dati personali.

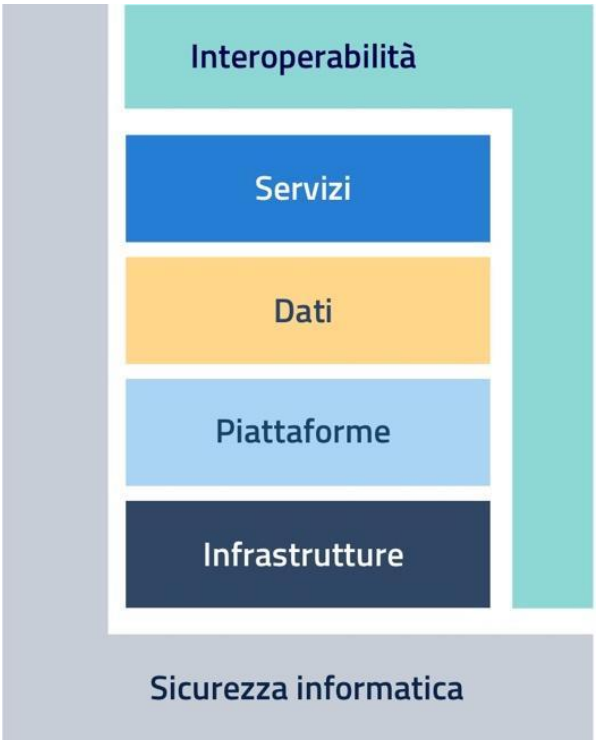
INTRODUZIONE

Il Piano triennale 2021 – 2023 detta indirizzi specifici per le amministrazioni e contiene elementi orientati fortemente alla responsabilizzazione delle PA.

Il Piano emanato da AgID è costituito sulla base di un Modello strategico di evoluzione del sistema informativo della Pubblica Amministrazione ed indirizza le PA nel raggiungimento dei risultati attesi.

Il modello strategico è la visione a medio/lungo termine verso la quale la PA deve tendere per sfruttare al meglio i benefici derivanti dall'uso delle tecnologie digitali. È stato pensato per superare l'approccio a "silos" (contenitori in cui i dati sono spesso replicati) storicamente adottato dalle PA e costituisce il quadro di riferimento su cui innestare e rendere operativi progetti, piattaforme e programmi.

AgID ha schematizzato il modello strategico del Piano con la seguente rappresentazione semplificata che è riportata nel Piano stesso:



Questa rappresentazione consente di descrivere in maniera funzionale la trasformazione digitale. Tale rappresentazione è costituita da due livelli trasversali: l'interoperabilità e la sicurezza dei sistemi informativi e dei livelli verticali di servizi, dati, piattaforme ed infrastrutture.

Il documento è organizzato in 9 capitoli, dove i primi sei approfondiscono le componenti tecnologiche: servizi, dati, piattaforme, infrastrutture, interoperabilità e sicurezza e i tre capitoli finali delineano gli strumenti di governance.

Entro il mese di settembre di ogni anno AgID pubblicherà la versione aggiornata del Piano, al fine di indirizzare le azioni per l'anno successivo. L'Agenzia ha il compito di guidare le PA nella fase di adeguamento alle indicazioni contenute nel Piano.

Entro il mese di dicembre di ogni anno le PA devono obbligatoriamente redigere il proprio piano per il triennio successivo.

La strategia del piano è quella di:

- Favorire lo sviluppo di una società digitale, dove i servizi mettono al centro i cittadini e le imprese, attraverso la digitalizzazione della pubblica amministrazione che costituisce il motore di sviluppo per tutto il Paese.
- Promuovere lo sviluppo sostenibile, etico ed inclusivo, attraverso l'innovazione e la digitalizzazione al servizio delle persone, delle comunità e dei territori, nel rispetto della sostenibilità ambientale.
- Contribuire alla diffusione delle nuove tecnologie digitali nel tessuto produttivo italiano, incentivando la standardizzazione, l'innovazione e la sperimentazione nell'ambito dei servizi pubblici.

I principi guida rilevabili nella prima parte del piano sono:

Digital & Mobile First (digitale e mobile come prima opzione): le pubbliche amministrazioni devono realizzare servizi primariamente digitali;

Digital Identity Only (accesso esclusivo mediante identità digitale): le PA devono adottare in via esclusiva sistemi di identità digitale definiti dalla normativa assicurando almeno l'accesso tramite SPID;

Cloud First (cloud come prima opzione): le pubbliche amministrazioni, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano primariamente il paradigma cloud, tenendo conto della necessità di prevenire il rischio di lock-in;

Servizi Inclusivi E Accessibili: le pubbliche amministrazioni devono progettare servizi pubblici digitali che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori;

Dati Pubblici Un Bene Comune: il patrimonio informativo della pubblica amministrazione è un bene fondamentale per lo sviluppo del Paese e deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile;

Interoperabile By Design: i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e senza interruzioni in tutto il mercato unico esponendo le opportune API;

Sicurezza E Privacy By Design: i servizi digitali devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali;

User-Centric, Data Driven E Agile: le amministrazioni sviluppano i servizi digitali, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo.

Once Only: le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite;

Transfrontaliero By Design (concepito come transfrontaliero): le pubbliche amministrazioni devono rendere disponibili a livello transfrontaliero i servizi pubblici digitali rilevanti;

Codice Aperto: le pubbliche amministrazioni devono prediligere l'utilizzo di software con codice aperto e, nel caso di software sviluppato per loro conto, deve essere reso disponibile il codice sorgente.

Si rilevano inoltre almeno due concetti nuovi:

- il dato pubblico come bene comune;
- lo sviluppo di sistemi digitali in linea con le esigenze del lavoro agile.

Non è inoltre possibile fare a meno di tenere conto delle evoluzioni organizzative che sono state imposte o ritenute opportune a seguito della recente pandemia causata dal propagarsi del virus denominato COVID-19. Ci si riferisce in particolare al ricorso all'istituto del così detto Lavoro Agile (o smart working) introdotto con la Legge n. 81/2017 oltre alla recente Legge n. 120/2020 che ha accelerato l'attuazione di alcune attività afferenti alla transazione al digitale.

La Legge n. 120 del 11/09/2020, di conversione, con modifiche, del decreto legge n. 76 del 16/07/2020 (Decreto semplificazioni), accelera di fatto la digitalizzazione dei servizi pubblici e ha stabilito, tra l'altro, la scadenza del 28/02/2021 entro la quale le PA erano tenute a:

- avviare i progetti per portare on-line tutti i servizi erogati in modalità tradizionale (off-line);
- completare il processo di adesione a PagoPA (piattaforma unica per il pagamento elettronico);
- avviare il passaggio alle diverse modalità di autenticazione online (Sistema Pubblico di Identità Digitale - SPID e Carta d'Identità Elettronica – CIE);
- rendere disponibili i propri servizi attraverso delle applicazioni per dispositivi mobili anche attraverso il punto di accesso telematico di cui all'art. n. 64-bis del CAD ("app" IO ideata e sviluppata dal Team per la trasformazione digitale nell'ambito del progetto PagoPA);
- eseguire gli opportuni adeguamenti in modo da rendere accessibili i propri strumenti informatici ai cittadini con disabilità.

Per una corretta applicazione delle disposizioni nazionali non si è ritenuto sufficiente definire il presente piano senza analizzare anche altri aspetti: per questo motivo è stata eseguita una procedura di "Assessment" mirata ad analizzare lo stato di adempimento agli obblighi normativi e del livello di digitalizzazione dell'Ente. Per l'esecuzione di quest'analisi, si è provveduto ad affidare alla ditta Maggioli S.p.a. un servizio di supporto alla transizione al digitale.

OBIETTIVI PREFISSATI DA AGID

Per quanto riguarda i risultati attesi a livello nazionale si rimanda alla lettura del Piano AgID; per gli obiettivi sono così riassumibili suddivisi per Capitoli del Piano AgID

Il Capitolo 1 “Componenti Tecnologiche – Servizi” prevede 3 obiettivi

OB.1.1 Migliorare la capacità di generare ed erogare servizi digitali

OB.1.2 Migliorare l’esperienza d’uso e l’accessibilità dei servizi

OB.1.3 Piena applicazione del Regolamento Europeo EU 2018/1724 (Single Digital Gateway)

Il Capitolo 2 “Componenti Tecnologiche – Dati” prevede 3 obiettivi

OB.2.1 Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese

OB.2.2 Aumentare la qualità dei dati e dei metadati

OB.2.3 Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati

Nel Capitolo 3 “Componenti Tecnologiche – Piattaforme” vengono fissati 3 obiettivi

OB. 3.1 - Favorire l’evoluzione delle piattaforme esistenti

OB. 3.2 - Aumentare il grado di adozione delle piattaforme abilitanti esistenti da parte delle pubbliche amministrazioni

OB. 3.3 - Incrementare il numero di piattaforme per le amministrazioni ed i cittadini

Sono 3 gli obiettivi anche il Capitolo 4 “Componenti Tecnologiche – Infrastrutture”

OB. 4.1- Migliorare la qualità dei servizi digitali erogati dalle amministrazioni locali favorendone l’aggregazione e la migrazione su infrastrutture sicure ed affidabili

OB. 4.2 - Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l’aggregazione e la migrazione su infrastrutture sicure ed affidabili

OB. 4.3 - Migliorare l’offerta di servizi di connettività per le PA

Per il Capitolo 5 “Componenti Tecnologiche - Interoperabilita'” troviamo:

OB. 5.1 Favorire l’applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API

OB. 5.2 Adottare API conformi al Modello di Interoperabilità

OB. 5.3 Modelli e regole per l’erogazione integrata di servizi interoperabili

Il Capitolo 6 “Componenti Tecnologiche - Sicurezza Informatica”

OB. 6.1 - Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA

OB. 6.2 - Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

Per quanto concerne la Governance – Leve per L’innovazione il Capitolo 7 prevede 2 obiettivi

OB. 7.1 Rafforzare le leve per l’innovazione delle PA e dei territori

OB. 7.2 Rafforzare le competenze digitali per la PA e per il Paese e favorire l’inclusione digitale

Al Capitolo 8 “Governare La Trasformazione Digitale” troviamo gli ultimi 3 obiettivi

OB. 8.1 Rafforzare le leve per l’innovazione delle PA e dei territori e Migliorare i processi di trasformazione digitale della PA

OB. 8.2 Rafforzare le competenze digitali per la PA e per il Paese e favorire l’inclusione digitale

OB. 8.3 Migliorare i processi di trasformazione digitale e di innovazione della PA - Il monitoraggio del Piano triennale

LA VERIFICA DELL'ASSESSMENT

L'analisi dello stato di adempimento degli obblighi normativi e del livello di digitalizzazione dell'Ente è stata eseguita con il supporto di uno staff della ditta Maggioli SPA specializzato in materia di esecuzione delle attività in gestione al RTD

Gli scopi dell'analisi sono stati:

- Contestualizzare alle prassi operative adottate le novità normative e giurisprudenziali
- Fornire gli strumenti informativi previsti dalle norme con particolare attenzione alle ricadute pratico/operative
- Permettere l'applicazione di tutte le disposizioni in materia di PA digitale finalizzata alla gestione digitale dei documenti
- Impostare il cambiamento organizzativo necessario

Dall'analisi è stata prodotta una relazione finale che si allega al presente documento (allegato 1)

STATO ATTUALE DELL'ENTE

L'evoluzione digitale dell'Ente è stata sempre caratterizzata da una maggiore attenzione al tema dell'operatività come richiesto anche dall'attuale Piano Triennale.

Questo Piano Triennale vuole nascere sotto il principio di perseguimento di una strategia di progettazione trasversale delle attività ICT che si rifanno anche alle linee guida già identificate nell'Assessment.

In sintesi

- Acquisire consapevolezza digitale
- Pianificare e proseguire il percorso verso il digitale
- Aumentare l'efficienza dei servizi forniti

E' necessario incrementare una sensibilità nelle visioni di lungo periodo che permetta di aprirsi alle nuove tecnologie e scegliere sistemi innovativi e tecnologie utili alla propria attività.

I progetti ipotizzati a questo fine soddisfano i principali obiettivi del Piano Triennale AGID:

- *GOVERNARE LA TRASFORMAZIONE DIGITALE*
    - Formazione - argomenti ipotizzati: Gestione documentale (Norme, gestione operativa e workflow, SI in house); Cybersecurity; Norme e regolamenti della Transizione Digitale, Privacy e GDPR, Piattaforme PA (SPID, PagoPA, aspetti tecnico legali gestionali); Open data, Accessibilità siti web (aspetti tecnici e normativi) e creazione di documenti accessibili/interventi sui documenti).
    - Linea Guida Acquisti: Raccogliere la normativa AGID e aggiornare i contratti
    - Monitoraggio del Piano Triennale oltre a progetti e contratti
- *AUMENTARE LA QUALITÀ DEI DATI E DEI METADATI*
    - Gestione documentale: Adeguamento normativa e redazione manuale di gestione documentale
- *COMPONENTI TECNOLOGICHE - DATI*
    - Open data e interoperabilità:
- *COMPONENTI TECNOLOGICHE - SICUREZZA INFORMATICA*
    - Cyber security: valutare l'affidamento in outsourcing del servizio di cyber security
    - Implementazione misure minime di sicurezza
- *MIGLIORARE L'ESPERIENZA D'USO E L'ACCESSIBILITÀ DEI SERVIZI*
    - Aggiornamento dei Siti Web
        - Dichiarazione di accessibilità siti e verifica conformità alle norme

- Verifica e aggiornamento continuo dei contenuti

Di seguito gli obiettivi e le linee di Azione da portare avanti nel triennio

COMPONENTI TECNOLOGICHE – servizi

Obiettivo 1.1 Migliorare la capacità di generare ed erogare servizi digitali

- *Linea Azione 02 - Continuare ad applicare i principi Cloud First - SaaS First e ad acquisire servizi cloud solo se qualificati da AGID, consultando il Catalogo dei servizi cloud qualificati da AGID per la PA*
- *Linea Azione 04 - Adeguare le proprie procedure di procurement alle linee guida di AGID sull'acquisizione del software e al CAD (artt. 68 e 69)*
- *Linea Azione 05 aderiscono al programma di abilitazione al cloud e trasmettono al Dipartimento per la Trasformazione Digitale gli elaborati previsti dalla fase di assessment dei servizi avviando le fasi successive. Le PAL (Pubblica amministrazione locale) aderiscono al programma di abilitazione al cloud e trasmettono ad AGID gli elaborati previsti dalla fase di assessment dei servizi e avviano le fasi successive*
- *Linea Azione 17 - Le PA avviano il percorso di migrazione verso il cloud consultando il manuale di abilitazione al cloud nell'ambito del relativo programma*

Obiettivo 1.2 Migliorare l'esperienza d'uso e l'accessibilità dei servizi

- *Linea Azione 09 - Nei procedimenti di acquisizione di beni e servizi ICT, fare riferimento alle Linee guida di design*
- *Linea Azione 14 - Comunicare ad AGID, tramite apposito form online, l'uso dei modelli per lo sviluppo web per i propri siti istituzionali*

- *Linea Azione 15 - Pubblicare la dichiarazione di accessibilità per le APP mobili, tramite l'applicazione form.agid.gov.it*
- *Linea Azione 20 - pubblicare, entro il 23 settembre 2022, tramite l'applicazione form.agid.gov.it, una dichiarazione di accessibilità per ciascuno dei loro i siti web e APP mobili"*
- *Linea Azione 21 - adeguare i propri siti web rimuovendo, tra gli altri, gli errori relativi a 2 criteri di successo più frequentemente non soddisfatti, come pubblicato sul sito di AGID*

Obiettivo 1.3 Piena applicazione del Regolamento Europeo EU 2018/1724 (Single Digital Gateway)

Rispetto a questo Obiettivo non ci sono linee d'azione di interesse per l'Ente.

Componenti tecnologiche - Dati

Obiettivo 2.1 Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese

- *Linea Azione 01 - Individuare i dataset di tipo dinamico da rendere disponibili in open data coerenti con il modello di interoperabilità e con i modelli di riferimento di dati nazionali ed europei*
- *Linea Azione 02 - Rendere disponibili i dati territoriali attraverso i servizi di cui alla Direttiva 2007/2/EC (INSPIRE)*
- *Linea Azione 03 - Avviare le procedure di apertura dei dati di tipo dinamico individuati di cui sono titolari in conformità alla Direttiva (UE) 2019/1024; stimolare, anche nella predisposizione di gare d'appalto, i gestori di servizi pubblici da loro controllati per l'apertura dei dati dinamici (es. i dati sulla mobilità in possesso dell'azienda partecipata locale), e agevolare la documentazione degli stessi nei cataloghi nazionali di riferimento (dati, geodati e API)*

- *Linea Azione 04 - Avviare l'adeguamento dei sistemi che si interfacciano alle banche dati di interesse nazionale secondo le linee guida del modello di interoperabilità*
- *Linea Azione 05 - Documentare le API coerenti con il modello di interoperabilità nei relativi cataloghi di riferimento nazionali*
- *Linea Azione 14 - Avviare l'adeguamento al modello di interoperabilità e ai modelli di riferimento di dati nazionali ed europei delle basi di dati della PA e le documentano nel relativo catalogo delle API*

Obiettivo 2.2 Aumentare la qualità dei dati e dei metadati

- *Linea Azione 06 - Uniformare i propri sistemi di metadati relativi ai dati geografici alle specifiche nazionali e documentare i propri dataset nel catalogo nazionale geodati.gov.it*
- *Linea Azione 07 - Uniformare i propri sistemi di metadati relativi ai dati non geografici alle specifiche nazionali e documentare i propri dataset nel catalogo nazionale dati.gov.it*
- *Linea Azione 08 - Fornire indicazioni sul livello di qualità dei dati per le caratteristiche individuate e pubblicare i relativi metadati (per esempio indicando la conformità ai modelli dati standard nazionali ed europei)*
- *Linea Azione 15 - pubblicare i propri dati aperti tramite API nel catalogo PDND e le documentano anche secondo i riferimenti contenuti nel National Data Catalog per l'interoperabilità semantica"*

Obiettivo 2.3 Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati

- *Linea Azione 09 - Adottare la licenza aperta di riferimento nazionale, documentandola esplicitamente come metadato*

- *Linea Azione 10 - Definire al proprio interno una "squadra per i dati" (data team) ovvero identificare tutte le figure, come raccomandato dalle Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico, che possano contribuire alla diffusione della cultura del dato e al recepimento della Strategia nazionale dati su tutto il territorio*
- *Linea Azione 11 - Partecipare a interventi di formazione e sensibilizzazione sulle politiche open data*
- *Linea Azione 16 - attuare le linee guida contenenti regole tecniche per l'attuazione della norma di recepimento della Direttiva (EU) 2019/1024 definite da AGID anche per l'eventuale monitoraggio del riutilizzo dei dati aperti sulla base di quanto previsto nella Direttiva stessa*

COMPONENTI TECNOLOGICHE - PIATTAFORME

Obiettivo 3.1 Favorire l'evoluzione delle piattaforme esistenti

Rispetto a questo Obiettivo non ci sono linee d'azione di interesse per l'Ente.

Obiettivo 3.2 Aumentare il grado di adozione delle piattaforme abilitanti esistenti da parte delle pubbliche amministrazioni

- *Linea Azione 10 – Per i soggetti obbligati all'adesione alla Piattaforma PagoPA, risolvere le residuali problematiche tecnico/organizzative bloccanti per l'adesione alla Piattaforma stessa e completare l'attivazione dei servizi*
- *Linea Azione 12 –cessare il rilascio di credenziali proprietarie a cittadini dotabili di SPID e/o CIE*
- *Linea Azione 13 –adottare lo SPID by default: le nuove applicazioni devono nascere SPID-only a meno che non ci siano vincoli normativi o tecnologici, se dedicate a soggetti dotabili di SPID*
- *Linea Azione 20 – adeguarsi alle evoluzioni previste dall'ecosistema SPID (tra cui OpenID connect, servizi per i minori e gestione degli attributi qualificati)*
- *Linea Azione 21 – Assicurare per entrambe le piattaforme pagoPA e App IO l'attivazione di nuovi servizi in linea con i target sopra descritti e secondo le modalità attuative definite nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR)*

Obiettivo 3.3 Incrementare il numero di piattaforme per le amministrazioni ed i cittadini

- *Linea Azione 09 - definire un piano operativo e temporale per la cessazione del rilascio di credenziali proprietarie e per la predisposizione di un accesso SPID-only nei confronti dei cittadini dotabili di SPID*
- *Linea Azione 18 - Predisporsi per interagire con INAD per l'acquisizione dei domicili digitali dei soggetti in essa presenti*

- *Linea Azione 23 -Secondo la roadmap di attuazione prevista dal Piano Nazionale di Ripresa e Resilienza (PNRR), se PA in perimetro dovrà integrare 90 API nella Piattaforma Digitale Nazionale Dati*

COMPONENTI TECNOLOGICHE - INFRASTRUTTURE

Obiettivo 4.1 Migliorare la qualità dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili

- *Linea Azione 11 (ex Linea Azione 01 PT 2020/22) - Se PA proprietarie di data center di gruppo B, richiedere l'autorizzazione ad AGID per le spese in materia di data center nelle modalità stabilite dalla Circolare AGID 1/2019 (vuoto)*
- *Linea Azione 13 - trasmettere all'Agenzia per la cybersicurezza nazionale l'elenco e la classificazione dei dati e dei servizi digitali come indicato nel Regolamento*
- *Linea Azione 14 - aggiornre l'elenco e la classificazione dei dati e dei servizi digitali in presenza di dati e servizi ulteriori rispetto a quelli già oggetto di conferimento e classificazione come indicato nel Regolamento -*
- *Linea Azione 16 - trasmettere al DTD e all'AGID i piani di migrazione mediante una piattaforma dedicata messa a disposizione dal DTD come indicato nel Regolamento*

OB. 4.2 Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali migrandone gli applicativi on-premise (Data Center Gruppo B) verso infrastrutture e servizi cloud qualificati (incluso PSN)

Rispetto a questo Obiettivo non ci sono linee d'azione di interesse per l'Ente.

OB. 4.3 Migliorare l'offerta di servizi di connettività per le PA

- *Linea Azione 9 - approvvigionarsi sul nuovo catalogo MEPA per le necessità di connettività non riscontrabili nei contratti SPC*
- *Linea Azione 10 - acquistare i nuovi servizi disponibili nel listino SPC*
- *Linea Azione 23 - acquistare i servizi della nuova gara di connettività SPC*

COMPONENTI TECNOLOGICHE – INTEROPERABILITA'

Obiettivo 5.1 Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API

- *Linea Azione 01 - Prendere visione della Linea di indirizzo sull'interoperabilità tecnica per la PA e programmare le azioni per trasformare i servizi per l'interazione con altre PA implementando API conformi -*
- *Linea Azione 02 - Adottare la Linea guida sul Modello di Interoperabilità per la PA realizzando API per l'interazione con altre PA e/o soggetti privati*

Obiettivo 5.2 Adottare API conformi al Modello di Interoperabilità

- *Linea Azione 03 – In caso si decida di progettare API o SW in casa, popolare gli strumenti su developers.italia.it con i servizi che hanno reso conformi alla Linea di indirizzo sull'interoperabilità tecnica*
- *Linea Azione 04 -I n caso si decida di progettare API o SW in casa, popolare il Catalogo con le API conformi alla Linea guida sul Modello di Interoperabilità per la PA*
- *Linea Azione 05 - Utilizzare le API presenti sul Catalogo*
- *Linea Azione 06 - Cittadini e le imprese utilizzano le API presenti sul Catalogo*

- *Linea Azione 07 - "Le PA che hanno riportato su Developers Italia le proprie API provvedono al porting sul Catalogo delle API della Piattaforma Digitale Nazionale Dati"*

Obiettivo 5.3 Modelli e regole per l'erogazione integrata di servizi interoperabili

- *Linea Azione 08 - evidenzire le esigenze che non trovano riscontro nella Linea guida e partecipano alla definizione di pattern e profili di interoperabilità per l'aggiornamento delle stesse*

COMPONENTI TECNOLOGICHE – SICUREZZA INFORMATICA

Obiettivo 6.1 Aumentare la consapevolezza del rischio cyber (*Cyber Security Awareness*) nelle PA

- *Linea Azione 01 - Nei procedimenti di acquisizione di beni e servizi ICT far riferimento alle Linee guida sulla sicurezza nel procurement ICT*
- *Linea Azione 02 - Fare riferimento al documento tecnico "Cipher Suite protocolli TLS minimi per la comunicazione tra le PA e verso i cittadini"*
- *Linea Azione 04 - Valutare l'utilizzo del tool di Cyber Risk Assessment per l'analisi del rischio e la redazione del Piano dei trattamenti*
- *Linea Azione 05 - Definire, sulla base di quanto proposto dal RTD, all'interno dei piani di formazione del personale, interventi sulle tematiche di "Cyber Security Awareness"*
- *Linea Azione 06 - Adeguarsi alle Misure minime di sicurezza ICT per le pubbliche amministrazioni aggiornate*

Obiettivo 6.2 Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

- *Linea Azione 07 - Consultare la piattaforma Infosec aggiornata per rilevare le vulnerabilità (CVE) dei propri asset*
- *Linea Azione 09 - utilizzare il tool di self assessment per il controllo del protocollo HTTPS e la versione del CMS messo a disposizione da AGID"*
- *Linea Azione 12 fare riferimento per la configurazione del protocollo HTTPS all'OWASP Transport Layer Protection Cheat Sheet e alle Raccomandazioni AGID TLS e Cipher Suite e mantenere aggiornate le versioni dei CMS*

GOVERNANCE - LEVE PER L'INNOVAZIONE

Obiettivo 7.1 Rafforzare le leve per l'innovazione delle PA e dei territori - Coinvolgimento attivo delle amministrazioni e dei territori

- *Linea Azione 07 (ex cap. 8 -Linea Azione 12) - Valutare gli strumenti di procurement disponibili*
- *Linea Azione 9 e 10 - Programmare i fabbisogni di innovazione, beni e servizi innovativi per l'anno 2022 e 2023*

Obiettivo 7.2 Rafforzare le competenze digitali per la PA e per il Paese e favorire l'inclusione digitale

- *Linea Azione 07 (ex CAP8. -Linea Azione 21) - partecipare alle iniziative pilota, alle iniziative di sensibilizzazione e a quelle di formazione specialistica previste dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali*
- *Linea Azione 13 - partecipare alle attività di formazione "Monitoraggio dei contratti ICT" secondo le indicazioni fornite da AGID*
- *Linea Azione 14 - partecipare alle iniziative per lo sviluppo delle competenze digitali dei cittadini previste dal PNRR e in linea con il Piano operativo della Strategia Nazionale per le Competenze Digitali*

- *Linea Azione 15 - utilizzare tra i riferimenti per i propri piani di azione quanto previsto nel Piano operativo della strategia nazionale per le competenze digitali aggiornato*

GOVERNARE LA TRASFORMAZIONE DIGITALE

Obiettivo 8.1 Migliorare i processi di trasformazione digitale e di innovazione della PA - Consolidamento del ruolo del Responsabile della transizione al digitale; Rafforzare le leve per l'innovazione delle PA e dei territori - La domanda pubblica come leva per l'innovazione del Paese; Rafforzare le leve per l'innovazione delle PA e dei territori -Modelli e regole per l'erogazione integrata di servizi interoperabili

- *Linea Azione 07 - aderire alla piattaforma di community*
- *Linea Azione 08 - Se PA aderenti alla community, partecipare all'interscambio di esperienze e forniscono contributi per l'individuazione di best practices*
- *Linea Azione 10 - Attraverso i propri RTD, partecipare alle survey periodiche sui fabbisogni di formazione del personale, in tema di trasformazione digitale*
- *Linea Azione 14 - Programmare i fabbisogni di innovazione, beni e servizi innovativi per l'anno 2022*
- *Linea Azione 15 - Programmare i fabbisogni di innovazione, beni e servizi innovativi per l'anno 2023*
- *Linea Azione 32 - partecipare alle iniziative di formazione per RTD e loro uffici proposte da AGID*
- *Linea Azione 33 - partecipare alle iniziative di formazione per RTD e loro uffici proposte da AGID e contribuiscono alla definizione di moduli formativi avanzati da mettere a disposizione di tutti i dipendenti della PA*

Obiettivo 8.2 Rafforzare le competenze digitali per la PA e per il Paese e favorire l'inclusione digitale

- *Linea Azione 22 - Aggiornare i piani di azione secondo quanto previsto nel Piano strategico nazionale per le competenze digitali*
- *Linea Azione 23 - Aggiornare i piani di azione secondo quanto previsto nel Piano strategico nazionale per le competenze digitali*

Obiettivo 8.3 Migliorare i processi di trasformazione digitale e di innovazione della PA - Il monitoraggio del Piano triennale

- *Linea Azione 25 - Avviare l'adozione del Format PT di raccolta dati e informazioni per la verifica di coerenza delle attività con il Piano triennale*
- *Linea Azione 26 - Adottare le modifiche introdotte nella Circolare n. 4/2016 avente come oggetto "Monitoraggio sull'esecuzione dei contratti" e partecipare alle attività di formazione secondo le indicazioni fornite da AGID*
- *Linea Azione 29 - Partecipare alle attività di formazione secondo le indicazioni fornite da AGID*
- *Linea Azione 31 - Partecipare alle attività di monitoraggio per la misurazione dei target2022 dei Risultati Attesi del Piano secondo le modalità definite da AGID e Dipartimento per la Trasformazione Digitale*

SINTESI DEL PIANO E CRONO PROGRAMMA

La presente sezione costituisce un estratto del file in formato xls *(Allegato 2 – Piano Triennale)* e contiene, in formato tabellare, l'elenco delle azioni e delle attività da intraprendere nel periodo di validità del presente piano corredate da una previsione temporale circa la loro esecuzione.

È il risultato dell'unione di quanto previsto nel Piano Triennale AgID, dell'elenco delle attività già in corso e delle attività di assessment eseguite.

Le azioni compaiono nella tabella in ordine cronologico per priorità.

La colonna "Descrizione" contiene una descrizione delle attività da svolgere e si riferisce ad una o più descrizioni delle attività che compare nelle tabelle sopracitate.

Sono riportate le attività prioritarie estrapolate dal cronoprogramma generale valido fino al 2023 a disposizione dell'Ente

Priorità 1: attività in corso

Priorità 2: attività da chiudere nel 2022

Priorità 3: attività da iniziare nel 2022

Priorità 4: attività da iniziare nel 2023

Priorità 5: attività da chiudere nel 2023

PRIORITA' 1:
ATTIVITA IN CORSO

Cod.	Rif. Temp. da PT	OBIETTIVO	STATO	Descrizione	STATO AVANZAMENTO LAVORI ENTE
CAP1.PA.LA02	Da settembre 2020	ACQUISTI	CONTINUATIVA	Le PA continuano ad applicare i principi Cloud First - SaaS First e ad acquisire servizi cloud solo se qualificati da AGID, consultando il Catalogo dei servizi cloud qualificati da AGID per la PA https://cloud.italia.it/it/qualificazioni/	Si aplicheranno i principi di Cloud First - SaaS First e si acquisiranno servizi cloud solo se qualificati da AGID
CAP1.PA.LA05	Da dicembre 2020	DATA CENTER IN CLOUD	DA PIANIFICARE	Le PAC (Pubblica amministrazione centrale) aderiscono al programma di abilitazione al cloud e trasmettono al Dipartimento per la Trasformazione Digitale gli elaborati previsti dalla fase di assessment dei servizi avviando le fasi successive. Le PAL (Pubblica amministrazione locale) aderiscono al programma di abilitazione al cloud e trasmettono ad AGID gli elaborati previsti dalla fase di assessment dei servizi e	L'Ente si adeguerà al Programma nazionale di abilitazione al cloud, anche detto “Cloud Enablement Program”. Il programma si ispira al principio “cloud first”, secondo il quale, come anticipato, le pubbliche amministrazioni in fase di definizione di un nuovo progetto e/o di sviluppo di nuovi servizi, devono, in via prioritaria, valutare la possibilità di adottare il paradigma cloud prima di qualsiasi altra tecnologia.

				avviano le fasi successive -	
CAP1.PA.LA09	Da settembre 2020	ACQUISTI	CONTINUATIVA	Nei procedimenti di acquisizione di beni e servizi ICT, le PA devono far riferimento alle Linee guida di design	Raccogliere le linee guida AGID e valutare il rifacimento del sito istituzionale secondo le linee guida di design AGID.
CAP1.PA.LA14	Da aprile 2021	SITO WEB/APP	DA PIANIFICARE	Le PA comunicano ad AGID, tramite apposito form online, l'uso dei modelli per lo sviluppo web per i propri siti istituzionali	L'Ente richiede al fornitore l'uso dei modelli per lo sviluppo web per i propri siti istituzionali
CAP1.PA.LA15	Entro il 23/06/2021	SITO WEB/APP	DA MONITORARE	Le PA devono pubblicare la dichiarazione di accessibilità per le APP mobili, tramite l'applicazione form.agid.gov.it	Non è stata fatta negli anni passati si procederà in tal senso
CAP2.PA.LA01	Da gennaio 2021	INTEROPERABILITA'	DA MONITORARE	Le PA individuano i dataset di tipo dinamico da rendere disponibili in open data coerenti con il modello di interoperabilità e con i modelli di riferimento di dati nazionali ed europei	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP2.PA.LA02	Da genna	OPEN DATA	DA MONITOR	Le PA rendono disponibili i dati territoriali attraverso i servizi di cui	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione

	io 2021		ARE	alla Direttiva 2007/2/EC (INSPIRE)	Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP2.PA.LA03	Da febbraio 2021	INTEROPERABILITA'	DA MONITORARE	Le PA avviano le procedure di apertura dei dati di tipo dinamico individuati di cui sono titolari in conformità alla Direttiva (UE) 2019/1024; stimolano, anche nella predisposizione di gare d'appalto, i gestori di servizi pubblici da loro controllati per l'apertura dei dati dinamici (es. i dati sulla mobilità in possesso dell'azienda partecipata locale), e agevolano la documentazione degli stessi nei cataloghi nazionali di riferimento (dati, geodati e API)	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP2.PA.LA06	Da gennaio 2021	OPEN DATA	DA MONITORARE	uniformare i propri sistemi di metadati relativi ai dati geografici alle specifiche nazionali e documentano i propri dataset nel	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo

				catalogo nazionale geodati.gov.it	all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP2.PA.LA07	Da gennaio 2021	OPEN DATA	DA MONITORARE	Le PA uniformano i propri sistemi di metadati relativi ai dati non geografici alle specifiche nazionali e documentano i propri dataset nel catalogo nazionale dati.gov.it	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP2.PA.LA08	Da gennaio 2021	OPEN DATA	DA MONITORARE	Le PA forniscono indicazioni sul livello di qualità dei dati per le caratteristiche individuate e pubblicano i relativi metadati (per esempio indicando la conformità ai modelli dati standard nazionali ed europei)	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso.

					https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP2.PA.LA09	Da gennaio 2021	OPEN DATA	DA MONITORARE	Le PA adottano la licenza aperta di riferimento nazionale, documentandola esplicitamente come metadato	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP2.PA.LA10	Da gennaio 2021	OPEN DATA	DA MONITORARE	Le PA definiscono al proprio interno una “squadra per i dati” (data team) ovvero identificano tutte le figure, come raccomandato dalle Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico, che possano contribuire alla diffusione della cultura del dato e al recepimento della Strategia nazionale dati su tutto il territorio	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP2.PA.LA11	Da genna	OPEN DATA	DA MONITOR	Le PA partecipano a interventi di formazione e sensibilizzazione	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione

	io 2021		ARE	sulle politiche *open data*	Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP3.PA.LA01	Da ottobre 2020	PIATTAFORME	DA VALUTARE	Le PA che intendono aderire a NoiPA esprimono manifestazione di interesse e inviano richiesta di adesione	?
CAP3.PA.LA04	Da gennaio 2021	PIATTAFORME	DA VALUTARE	Le PA interessate compilano il questionario per la raccolta delle informazioni di assessment per l'adesione a NoiPA	?
CAP3.PA.LA09	Entro dicembre 2020	PIATTAFORME		Le PA e i gestori di pubblici servizi interessati definiscono un piano operativo e temporale per la cessazione del rilascio di credenziali proprietarie e per la predisposizione di un accesso SPID-only nei confronti dei cittadini dotabili di SPID	il Consiglio ha provveduto all'implementazione delle piattaforme abilitanti SPID e CIE e consente l'accesso ai servizi online che richiedono l'identificazione dell'utente mediante i suddetti strumenti di autenticazione. l'Amministrazione consiliare consente agli utenti di sottoscrivere le istanze presentate telematicamente con la firma SPID. E' necessario assicurarsi che tutti i servizi siano

					fruibili in modalità telematica e accessibili mediante SPID e CIE e valutare la possibilità di erogare online ulteriori servizi oltre a quelli già resi disponibili
CAP3.PA.LA10	Entro dicembre 2020	PIATTAFORME		I soggetti obbligati all'adesione alla Piattaforma pagoPA risolvono le residuali problematiche tecnico/organizzative bloccanti per l'adesione alla Piattaforma stessa e completano l'attivazione dei servizi	Si procederà come attività continuativa
CAP3.PA.LA12	Da ottobre 2021	PIATTAFORME	DA MONITORARE	Le PA e i gestori di pubblici servizi interessati cessano il rilascio di credenziali proprietarie a cittadini dotabili di SPID e/o CIE	il Consiglio ha provveduto all'implementazione delle piattaforme abilitanti SPID e CIE e consente l'accesso ai servizi online che richiedono l'identificazione dell'utente mediante i suddetti strumenti di autenticazione. l'Amministrazione consiliare consente agli utenti di sottoscrivere le istanze presentate telematicamente con la firma SPID. E' necessario assicurarsi che tutti i servizi siano fruibili in modalità telematica e accessibili mediante SPID e CIE e valutare la possibilità di erogare online ulteriori servizi oltre a quelli già resi disponibili
CAP3.PA.LA13	Da ottobre 2021	PIATTAFORME	DA MONITORARE	Le PA e i gestori di pubblici servizi interessati adottano lo SPID by default: le nuove applicazioni devono nascere SPID-only a meno	si procederà in tal senso

				che non ci siano vincoli normativi o tecnologici, se dedicate a soggetti dotabili di SPID	
CAP4.PA.LA11 exCAP4.PA.LA01	Da settembre 2020	DATA CENTER IN CLOUD	DA MONITORARE	Le PA proprietarie di data center di gruppo B richiedono l'autorizzazione ad AGID per le spese in materia di data center nelle modalità stabilite dalla Circolare AGID 1/2019. Le PAL proprietarie di data center di gruppo B richiedono l'autorizzazione ad AGID per le spese in materia di data center nelle modalità stabilite dalla Circolare AGID 1/2019 e prevedono in tali contratti, qualora autorizzati, una durata massima coerente con i tempi strettamente necessari a completare il percorso di migrazione previsti nei propri piani di migrazione	A inizio 2019 è stato aggiornato il datacenter. Si sta procedendo verso l'acquisto delle licenze.
CAP4.PA.LA09	Da ottobre 2020	ACQUISTI	CONTINUATIVA	Le PAL si approvvigionano sul nuovo catalogo MEPA per le necessità di connettività non riscontrabili nei contratti SPC	Non c'è un regolamento specifico sugli acquisti IT ma la normativa AGID è sempre stata applicata e si procederà in tal senso
CAP4.PA.LA10	Da giugno	ACQUISTI	CONTINUATIVA	Le PA possono acquistare i nuovi servizi disponibili nel listino SPC	Non c'è un regolamento specifico sugli acquisti IT ma la normativa AGID è sempre stata applicata e si procederà in tal senso

	2021				
CAP5.PA.LA01	Da settembre 2020	INTEROPERABILITA'	DA MONITORARE	Le PA prendono visione della Linea di indirizzo sull'interoperabilità tecnica per la PA e programmano le azioni per trasformare i servizi per l'interazione con altre PA implementando API conformi	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP5.PA.LA02	Da gennaio 2021	INTEROPERABILITA'	DA MONITORARE	Le PA adottano la Linea guida sul Modello di Interoperabilità per la PA realizzando API per l'interazione con altre PA e/o soggetti privati	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP5.PA.LA03	Da settembre	OPEN DATA	DA MONITORARE	Le PA popolano gli strumenti su developers.italia.it con i servizi che hanno reso conformi alla Linea di	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in

	2020			indirizzo sull'interoperabilità tecnica	merito. Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP6.PA.LA01	Da settembre 2020	ACQUISTI	CONTINUATIVA	Le PA nei procedimenti di acquisizione di beni e servizi ICT devono far riferimento alle Linee guida sulla sicurezza nel *procurement* ICT	Non c'è un regolamento specifico sugli acquisti IT ma la normativa AGID è sempre stata applicata e si procederà in tal senso
CAP6.PA.LA02	Da novembre 2020	ACQUISTI	CONTINUATIVA	Le PA devono fare riferimento al documento tecnico Cipher Suite protocolli TLS minimi per la comunicazione tra le PA e verso i cittadini	Non c'è un regolamento specifico sugli acquisti IT ma la normativa AGID è sempre stata applicata e si procederà in tal senso
CAP6.PA.LA04	Da settembre 2020	SICUREZZA	DA VALUTARE	Le PA valutano l'utilizzo del tool di Cyber Risk Assessment per l'analisi del rischio e la redazione del Piano dei trattamenti	L'Ente ne valuta l'utilizzo
CAP6.PA.LA07	Da dicembre 2021	DATA CENTER IN CLOUD	CONTINUATIVA	Le PA devono consultare la piattaforma Infosec aggiornata per rilevare le vulnerabilità (CVE) dei propri asset	L'Ente provvede a mantenere firewall aggiornati con la struttura HW e Antivirus aggiornati; si procederà col passaggio back up in cloud. L'Ente ha un piano di Business

					continuity
CAP8.PA.LA07	Da gennaio 2021	COMMUNITY	DA MONITORARE	Le PA che hanno nominato il RTD aderiscono alla piattaforma di *community*	Si valuta e si procede in tal senso. Viene inoltre periodicamente consultata la pagina AgID relativa al Responsabile per la transizione al digitale https://www.agid.gov.it/it/agenzia/responsabile-transizione-digitale. Se opportuno si partecipa ai percorsi di formazione per RTD organizzati da AgID.
CAP8.PA.LA08	Da febbraio 2021	COMMUNITY	DA MONITORARE	Le PA aderenti alla community partecipano all'interscambio di esperienze e forniscono contributi per l'individuazione di best practices	Si valuta e si procede in tal senso. Viene inoltre periodicamente consultata la pagina AgID relativa al Responsabile per la transizione al digitale https://www.agid.gov.it/it/agenzia/responsabile-transizione-digitale. Se opportuno si partecipa ai percorsi di formazione per RTD organizzati da AgID.
CAP7.PA.LA07 exCAP8.PA.LA12	Da dicembre 2020	ACQUISTI	CONTINUATIVA	Le PA, nell'ambito della pianificazione per l'attuazione della propria strategia digitale, valutano gli strumenti di procurement disponibili	Non c'è un regolamento specifico sugli acquisti IT ma la normativa AGID è sempre stata applicata e si procederà in tal senso
CAP8.PA.LA14	Entro ottobre 2021	FABBISOGNI INNOVAZIONE	CONTINUATIVA	Le PA programmano i fabbisogni di innovazione, beni e servizi innovativi per l'anno 2022	La partita del procurement è complessa e il settore degli approvvigionamenti IT è strategico .si lavora per ottenere approvvigionamenti pianificati che puntino sull'innovazione

CAP8.PA.LA19	Da novembre 2021	COMMUNITY	DA MONITORARE	Le PA partecipano ai tavoli di coordinamento per domini specifici	Si valuta e si procede in tal senso. Viene inoltre periodicamente consultata la pagina AgID relativa al Responsabile per la transizione al digitale https://www.agid.gov.it/it/agenzia/responsabile-transizione-digitale. Se opportuno si partecipa ai TAVOLI DI COORDINAMENTO
CAP7.PA.LA12 exCAP8.PA.LA21	da gennaio 2021	FORMAZIONE	ANNUALE DA PIANIFICARE	Le PA partecipano alle iniziative pilota, alle iniziative di sensibilizzazione e a quelle di formazione specialistica previste dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali	E' utile, indispensabile e necessario per il personale e per l'RTD partecipare alle iniziative di formazione specialistica previste dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali
CAP8.PA.LA22	Da febbraio 2021	FORMAZIONE	ANNUALE DA PIANIFICARE	Le PA aggiornano i piani di azione secondo quanto previsto nel Piano strategico nazionale per le competenze digitali	E' utile, indispensabile e necessario per il personale e per l'RTD partecipare alle iniziative di formazione specialistica previste dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali
CAP8.PA.LA26	Da febbraio 2021	ACQUISTI	CONTINUATIVA	Le PA adottano le modifiche introdotte nella Circolare n. 4/2016 avente come oggetto “Monitoraggio sull’esecuzione dei contratti” e partecipano alle attività di formazione secondo le indicazioni fornite da AGID	Non c'è un regolamento specifico sugli acquisti IT ma la normativa AGID è sempre stata applicata e si procederà in tal senso

CAP1.PA.LA17	Da ottobre 2021	DATA CENTER IN CLOUD	DA PIANIFICARE	Le PA avviano il percorso di migrazione verso il cloud consultando il manuale di abilitazione al cloud nell'ambito del relativo programma	L'Ente può indagare tra le diverse soluzioni e iniziare a predisporre il piano
CAP2.PA.LA14	da dicembre 2021	OPEN DATA	DA PIANIFICARE	Le PA titolari di banche di dati di interesse nazionale avviano l'adeguamento al modello di interoperabilità e ai modelli di riferimento di dati nazionali ed europei delle basi di dati della PA e le documentano nel relativo catalogo delle API	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP6.PA.LA09	Da dicembre 2021	SITO WEB/APP	DA PIANIFICARE	Le PA, in funzione delle proprie necessità, possono utilizzare il tool di self assessment per il controllo del protocollo HTTPS e la versione del CMS messo a disposizione da AGID	si valuterà lo strumento con il fornitore
CAP7.PA.LA13	da settembre 2021	MONITORAGGIO	CONTINUATIVA	Le PA, in funzione delle proprie necessità, partecipano alle attività di formazione "Monitoraggio dei contratti ICT" secondo le indicazioni fornite da AGID	si procederà il prossimo anno con la scadenza

PRIORITA' 2:

ATTIVITA' DA CHIUDERE NEL 2022

Cod.	Rif. Temp. da PT	OBIETTIVO	STATO	Descrizione	STATO AVANZAMENTO LAVORI ENTE
CAP1.PA.LA04	Entro ottobre 2022	ACQUISTI	CONTINUATIVA	Le PA adeguano le proprie procedure di procurement alle linee guida di AGID sull'acquisizione del software e al CAD (artt. 68 e 69)	Non c'è un regolamento specifico sugli acquisti IT ma la normativa AGID è sempre stata applicata e si procederà in tal senso
CAP6.PA.LA05	Entro dicembre 2022	FORMAZIONE	ANNUALE DA PIANIFICARE	Le PA definiscono, sulla base di quanto proposto dal RTD, all'interno dei piani di formazione del personale, interventi sulle tematiche di Cyber Security Awareness	E' utile, indispensabile e necessario per il personale e per l'RTD partecipare alle iniziative di formazione specialistica previste dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali
CAP8.PA.LA15	Entro ottobre 2022	FABBISOGNI INNOVAZIONE	CONTINUATIVA	Le PA programmano i fabbisogni di innovazione, beni e servizi innovativi per l'anno 2023	La partita del procurement è complessa e il settore degli approvvigionamenti IT è strategico .si lavora per ottenere approvvigionamenti pianificati che puntino sull'innovazione
CAP1.PA.LA20	Entro settembre	SITO WEB/APP	DA FINALIZZARE	Le PA pubblicano, entro il 23 settembre 2022, tramite l'applicazione form.agid.gov.it, una	Non è stata fatta negli anni passati si procederà in tal senso

	2022			dichiarazione di accessibilità per ciascuno dei loro i siti web e APP mobili	
CAP1.PA.LA21	Entro dicembre 2022	SITO WEB/APP	DA FINALIZZARE	Le Amministrazioni adeguano i propri siti web rimuovendo, tra gli altri, gli errori relativi a 2 criteri di successo più frequentemente non soddisfatti, come pubblicato sul sito di AGID	Tra gli errori si provvederà ad aggiornare il TLS 1.3 e word press
CAP4.PA.LA13	Entro giugno 2022	SICUREZZA	DA FINALIZZARE	Le PAL trasmettono all'Agenzia per la cybersicurezza nazionale l'elenco e la classificazione dei dati e dei servizi digitali come indicato nel Regolamento	L'Ente valuta un piccolo progetto a riguardo considerando che le attività di migrazione al cloud devono essere precedute dal necessario censimento e classificazione dei dati e dei servizi digitali dell'Ente, in osservanza del Modello definito dall'ACN d'intesa con il Dipartimento per la Trasformazione Digitale. Particolare attenzione, dunque, dovrà essere prestata ai dati classificati come critici e strategici, i quali non potranno essere ospitati su infrastrutture pubbliche munite di requisiti minimi adeguati alla classe di dati e servizi.
CAP6.PA.LA12	Entro giugno 2022	SITO WEB/APP	DA FINALIZZARE	Le ASL e le restanti Pubbliche Amministrazioni, relativamente ai propri portali istituzionali, devono fare	L'Ente si confronta con il fornitore ma indica che Https a posto mentre TLS da aggiornare

				riferimento per la configurazione del protocollo HTTPS all'OWASP Transport Layer Protection Cheat Sheet e alle Raccomandazioni AGID TLS e Cipher Suite e mantenere aggiornate le versioni dei CMS	
CAP7.PA.LA09	Entro ottobre 2022	FABBISOGNI INNOVAZIONE	CONTINUATIVA	Le PA, che ne hanno necessità, programmano i fabbisogni di innovazione, beni e servizi innovativi per l'anno 2023	La partita del procurement è complessa e il settore degli approvvigionamenti IT è strategico .si lavora per ottenere approvvigionamenti pianificati che puntino sull'innovazione

PRIORITA' 3:

ATTIVITA' DA INIZIARE NEL 2022

Cod.	Rif. Temp. da PT	OBIETTIVO	STATO	Descrizione	STATO AVANZAMENTO LAVORI ENTE
CAP2.PA.LA04	Da gennaio 2022	INTEROPERABILITA'	DA PIANIFICARE	Le PA avviano l'adeguamento dei sistemi che si interfacciano alle banche dati di interesse nazionale secondo le linee guida del modello di interoperabilità	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP2.PA.LA05	da gennaio 2022	INTEROPERABILITA'	DA PIANIFICARE	Le PA documentano le API coerenti con il modello di interoperabilità nei relativi cataloghi di riferimento nazionali	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire

					creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP3.PA.LA18	Da febbraio 2022	PIATTAFORME	DA VERIFICARE	Le PA si predispongono per interagire con INAD per l'acquisizione dei domicili digitali dei soggetti in essa presenti Le PA si integrano con le API INAD per l'acquisizione dei domicili digitali dei soggetti in essa presenti	da verificare
CAP5.PA.LA06	Da gennaio 2022	INTEROPERABILITA'	DA PIANIFICARE	I cittadini e le imprese utilizzano le API presenti sul Catalogo	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale

CAP8.PA.LA10	Da gennaio 2022	FORMAZIONE	ANNUALE DA PIANIFICARE	Le PA, attraverso i propri RTD, partecipano alle *survey* periodiche sui fabbisogni di formazione del personale, in tema di trasformazione digitale	E' utile, indispensabile e necessario per il personale e per l'RTD partecipare alle iniziative di formazione specialistica previste dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali
CAP8.PA.LA23	Da febbraio 2022	FORMAZIONE	ANNUALE DA PIANIFICARE	Le PA aggiornano i piani di azione secondo quanto previsto nel Piano strategico nazionale per le competenze digitali	E' utile, indispensabile e necessario per il personale e per l'RTD partecipare alle iniziative di formazione specialistica previste dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali
CAP8.PA.LA25	Da gennaio 2022	MONITORAGGIO	CONTINUATIVA	Le PA coinvolte avviano l'adozione del Format PT di raccolta dati e informazioni per la verifica di coerenza delle attività con il Piano triennale Le PA possono avviare l'adozione del "Format PT" di raccolta dati e informazioni per la verifica di coerenza delle attività con il Piano triennale	si procederà il prossimo anno con la scadenza
CAP8.PA.LA29	Da marzo	FORMAZIONE	ANNUALE DA PIANIFICARE	Le PA partecipano alle attività di formazione secondo le	E' utile, indispensabile e necessario per il personale e per l'RTD

	2022			indicazioni fornite da AGID	partecipare alle iniziative di formazione specialistica previste dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali
CAP2.PA.LA15	da dicembre 2022	OPEN DATA	DA PIANIFICARE	Le PA pubblicano i loro dati aperti tramite API nel catalogo PDND e le documentano anche secondo i riferimenti contenuti nel National Data Catalog per l'interoperabilità semantica	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP3.PA.LA20	Da gennaio 2022	PIATTAFORME	DA PIANIFICARE	Le PA devono adeguarsi alle evoluzioni previste dall'ecosistema SPID (tra cui OpenID connect, servizi per i minori e gestione degli attributi qualificati)	si procederà in tal senso
CAP4.PA.LA14	da luglio 2022	OPEN DATA	DA PIANIFICARE	Le PAL aggiornano l'elenco e la classificazione dei dati e dei servizi digitali in presenza di	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle

				dati e servizi ulteriori rispetto a quelli già oggetto di conferimento e classificazione come indicato nel Regolamento -	Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP5.PA.LA07	Da dicembre 2022	INTEROPERABILITA'	DA PIANIFICARE	Le PA che hanno riportato su Developers Italia le proprie API provvedono al porting sul Catalogo delle API della Piattaforma Digitale Nazionale Dati	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP5.PA.LA08	Da febbraio 2022	INTEROPERABILITA'	DA PIANIFICARE	Le PA evidenziano le esigenze che non trovano riscontro nella Linea guida e partecipano alla definizione di	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di

				pattern e profili di interoperabilità per l'aggiornamento delle stesse	conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP7.PA.LA14	da aprile 2022	FORMAZIONE	ANNUALE DA PIANIFICARE	Le PA, in funzione delle proprie necessità, partecipano alle iniziative per lo sviluppo delle competenze digitali dei cittadini previste dal PNRR e in linea con il Piano operativo della Strategia Nazionale per le Competenze Digitali	E' utile, indispensabile e necessario per il personale e per l'RTD partecipare alle iniziative di formazione specialistica previste dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali
CAP7.PA.LA15	da aprile 2022	FORMAZIONE	ANNUALE DA PIANIFICARE	Le PA, in funzione delle proprie necessità, utilizzano tra i riferimenti per i propri piani di azione quanto previsto nel Piano operativo della strategia nazionale per le competenze digitali	E' utile, indispensabile e necessario per il personale e per l'RTD partecipare alle iniziative di formazione specialistica previste dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali

				aggiornato	
CAP8.PA.LA32	Da gennaio 2022	FORMAZIONE	ANNUALE DA PIANIFICARE	Le PA in base alle proprie esigenze, partecipano alle iniziative di formazione per RTD e loro uffici proposte da AGID	E' utile, indispensabile e necessario per il personale e per l'RTD partecipare alle iniziative di formazione specialistica previste dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali

PRIORITA' 4:
ATTIVITA' DA INIZIARE NEL 2023

Cod.	Rif. Temp. da PT	OBIETTIVO	STATO	Descrizione	STATO AVANZAMENTO LAVORI ENTE
CAP5.PA.LA04	Da gennaio 2023	INTEROPERABILITA'	DA MONITORARE	Le PA popolano il Catalogo con le API conformi alla Linea guida sul Modello di Interoperabilità per la PA	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP5.PA.LA05	Da gennaio 2023	INTEROPERABILITA'	DA MONITORARE	Le PA utilizzano le API presenti sul Catalogo	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere

					condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP2.PA.LA16	Da gennaio 2023	OPEN DATA	DA PIANIFICARE	Le PA attuano le linee guida contenenti regole tecniche per l'attuazione della norma di recepimento della Direttiva (EU) 2019/1024 definite da AGID anche per l'eventuale monitoraggio del riutilizzo dei dati aperti sulla base di quanto previsto nella Direttiva stessa	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP4.PA.LA23	Da Maggio 2023	ACQUISTI	CONTINUATIVA	Le PA possono acquistare i servizi della nuova gara di connettività SPC	Non c'è un regolamento specifico sugli acquisti IT ma la normativa AGID è sempre stata applicata e si procederà in tal senso
CAP7.PA.LA16	da aprile 2023	FORMAZIONE	ANNUALE DA PIANIFICARE	Le PA, in funzione delle proprie necessità, utilizzano tra i riferimenti per i propri piani di azione quanto previsto nel Piano operativo della strategia nazionale per le competenze digitali aggiornato	E' utile, indispensabile e necessario per il personale e per l'RTD partecipare alle iniziative di formazione specialistica previste dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali

CAP8.PA.LA33	Da gennaio 2023	FORMAZIONE	ANNUALE DA PIANIFICARE	Le PA, in base alle proprie esigenze, partecipano alle iniziative di formazione per RTD e loro uffici proposte da AGID e contribuiscono alla definizione di moduli formativi avanzati da mettere a disposizione di tutti i dipendenti della PA	E' utile, indispensabile e necessario per il personale e per l'RTD partecipare alle iniziative di formazione specialistica previste dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali

PRIORITA' 5:

ATTIVITA' DA CHIUDERE NEL 2023

Cod.	Rif. Temp. da PT	OBIETTIVO	STATO	Descrizione	STATO AVANZAMENTO LAVORI ENTE
CAP6.PA.LA06	Entro dicembre 2023	SICUREZZA	DA PIANIFICARE	Le PA si adeguano alle Misure minime di sicurezza ICT per le pubbliche amministrazioni aggiornate	L'Ente procede con l'aggiornamento
CAP8.PA.LA31	Entro dicembre 2023	MONITORAGGIO	CONTINUATIVA	Le PA partecipano alle attività di monitoraggio per la misurazione dei target 2022 degli Risultati Attesi del Piano secondo le modalità definite da AGID e Dipartimento per la Trasformazione Digitale - Le PA panel partecipano alle attività di monitoraggio del Piano triennale secondo le modalità definite da AGID	si procederà il prossimo anno con la scadenza
CAP1.PA.LA22	Entro dicembre 2023	SITO WEB/APP	DA PIANIFICARE	Le Amministrazioni adeguano i propri siti web rimuovendo, tra gli altri, gli errori relativi a 2 criteri di successo più frequentemente non soddisfatti, come pubblicato	si procederà il prossimo anno con la scadenza

				sul sito di AGID	
CAP1.PA.LA25	Entro dicembre 2023	REGOLAMENTO UE 2018/1724	DA VERIFICARE	Le Pubbliche Amministrazioni competenti per i dati necessari all'esecuzione dei procedimenti amministrativi ricompresi nelle procedure di cui all'Allegato 16 II del Regolamento UE 2018/1724, mettono a disposizione dati strutturati ovvero dati non strutturati in formato elettronico secondo ontologie e accessibili tramite API nel rispetto delle specifiche tecniche del Single Digital Gateway. Nel caso di Pubbliche Amministrazioni che rendono disponibili i dati non strutturati, le stesse amministrazioni predispongono la pianificazione di messa a disposizione degli stessi dati in formato strutturato prevedendo il completamento dell'attività entro Dicembre 2025	si verifica e si procede in tal senso

CAP3.PA.LA21	Entro dicembre 2023	PIATTAFORME	DA PIANIFICARE	Le PA aderenti a pagoPA e App IO assicurano per entrambe le piattaforme l'attivazione di nuovi servizi in linea con i target sopra descritti e secondo le modalità attuative definite nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR)	deve procedere ad aderire a IO
CAP3.PA.LA23	Entro dicembre 2023	OPEN DATA	DA PIANIFICARE	Le PA in perimetro, secondo la roadmap di attuazione prevista dal Piano Nazionale di Ripresa e Resilienza (PNRR), dovranno integrare 90 API nella Piattaforma Digitale Nazionale Dati	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'Ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale
CAP4.PA.LA16	Entro febbraio 2023	DATA CENTER IN CLOUD	DA PIANIFICARE	Le PAL con obbligo di migrazione verso il cloud trasmettono al DTD e all'AGID i piani di migrazione mediante una	L'Ente vuole indagare tra le diverse soluzioni e iniziare a predisporre il piano

				piattaforma dedicata messa a disposizione dal DTD come indicato nel Regolamento	
CAP7.PA.LA10	Entro ottobre 2023	FABBISOGNI INNOVAZIONE	CONTINUATIVA	Le PA, che ne hanno necessità, programmano i fabbisogni di innovazione, beni e servizi innovativi per l'anno 2024	La partita del procurement è complessa e il settore degli approvvigionamenti IT è strategico .si lavora per ottenere approvvigionamenti pianificati che puntino sull'innovazione

Spett.le

RTD

CONSIGLIO REGIONALE DELLA SARDEGNA

SERVIZIO DI CHECK ON SITE
AL RESPONSABILE DELLA TRANSIZIONE DIGITALE
DELLA PUBBLICA AMMINISTRAZIONE

- Relazione di assessment relativa agli obblighi ed allo stato di digitalizzazione dell'ente alla luce del D. LGS. N. 82/2005 e disposizioni attuative -

INDICE

PREMESSA METODOLOGICA

Il Consiglio regionale della Sardegna è incluso tra gli organi della Regione ai sensi dell'art. 15 dello Statuto speciale per la Sardegna (approvato con legge cost. 26 febbraio 1948, n.3) e svolge funzioni legislative e regolamentari della Regione.

Il Consiglio regionale ha autonomia organizzativa, funzionale, finanziaria e contabile, in conformità a quanto previsto al Regolamento interno. Sul punto, l'art. 5 del Regolamento dei Servizi stabilisce che l'Amministrazione del Consiglio regionale assicura il perseguimento degli obiettivi stabili, nell'esercizio delle rispettive competenze statutarie e regolamentari, dagli organi istituzionali, secondo quanto disposto dallo stesso Regolamento dei servizi e dal Regolamento del personale. A tal riguardo, la legge regionale della Sardegna 13 novembre 1998, n. 31 – che detta la disciplina sul personale e sull'organizzazione degli uffici della Regione – stabilisce che l'Amministrazione e gli enti pubblici regionali non aventi natura economica «*assumono ogni determinazione per l'organizzazione degli uffici al fine di assicurare l'economicità, la speditezza e la rispondenza dell'azione amministrativa al pubblico interesse*» (art. 3).

Al fine di valutare la concreta applicabilità, dal punto di vista sia soggettivo che oggettivo, delle disposizioni in materia di digitalizzazione delle pubbliche amministrazioni all'attività svolta dall'Amministrazione del Consiglio regionale della Sardegna, appare opportuno iniziare l'analisi con alcuni cenni introduttivi in materia di adeguamento alla normativa in materia di digitalizzazione (in primis, il Codice dell'Amministrazione Digitale e il Piano Triennale per l'informatica nella PA 2021 - 2023).

L'analisi delle attività dell'Amministrazione consiliare e dei suoi processi sono state condotte con le seguenti modalità operative:

a) elaborazione di un questionario indirizzato alla struttura incaricata di gestire la transizione al digitale;

b) incontri tenutisi presso la Vostra sede con i referenti designati dall'amministrazione;

c) analisi delle informazioni acquisite mediante le risposte al questionario, della documentazione fornita a supporto e delle informazioni apprese durante i colloqui di chiarimento intercorsi;

d) individuazione degli strumenti informatici e delle soluzioni organizzative in uso presso il Consiglio regionale della Sardegna.

Con il presente documento si riscontra la Vostra richiesta sopra indicata, evidenziando - partendo da una breve ricostruzione della normativa applicabile - i profili risultati maggiormente critici in seguito all'interlocuzione con i Vostri uffici, con l'indicazione delle principali priorità d'intervento.

Data la complessità della materia, per comodità di trattazione, le questioni saranno affrontate suddividendo il parere in sette sezioni:

I. ambito di applicazione del Codice dell'amministrazione digitale e del piano triennale per l'informatica nella PA;

II. organizzazione per la transizione al digitale;

III. dematerializzazione dei documenti e degli archivi;

IV. erogazione di servizi *on line* a favore di cittadini e imprese*;*

V. sicurezza informatica e privacy;

VI. acquisto di beni e servizi ICT;

VII. valorizzazione del patrimonio informativo della PA.

Per ciascuno di tali profili, l'esposizione è divisa in due parti: la prima relativa alla descrizione degli obblighi normativi, la seconda contenente l'elencazione delle attività che la Vostra amministrazione deve porre in essere.

1. AMBITO DI APPLICAZIONE DEL CODICE DELL'AMMINISTRAZIONE DIGITALE E DEL PIANO TRIENNALE PER L'INFORMATICA NELLA PA

Appare opportuno iniziare l'analisi con alcuni cenni introduttivi alla normativa vigente in materia di digitalizzazione e, in particolare, al Codice dell'Amministrazione Digitale.

Il Decreto Legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale, d'ora in poi anche "CAD") è stato adottato in modo da definire il quadro normativo in materia di informatizzazione della pubblica amministrazione, dettando un triplice ordine di norme:

a) disposizioni sul valore giuridico - probatorio del documento informatico;

b) obblighi a contenuto informatico per le pubbliche amministrazioni;

c) diritti digitali degli utenti.

Il Codice, entrato in vigore il 1° gennaio 2006, è stato oggetto di ripetuti interventi di riforma da parte del Legislatore.

I vari interventi di modifica hanno riguardato – oltre alle singole previsioni – lo stesso impianto del testo normativo, con specifico riferimento ai soggetti destinatari delle previsioni (e quindi degli obblighi) in esso contenuti.

Se la versione originaria del CAD, infatti, prevedeva che lo stesso fosse destinato solo alle pubbliche amministrazioni di cui all'art. 1, comma 2, D.lgs. n. 165/2001 (tra cui figurano le Regioni e gli enti pubblici non economici regionali) e alle società ed enti inseriti nel conto economico consolidato dello stato (redatto da Istat), a seguito dei D.lgs. n. 179/2016 e n. 217/2017, è stato novellato l'art. 2, comma 2 del Codice prevedendo che le disposizioni ivi contenute si applichino anche:

- ai gestori di servizi pubblici in relazione ai servizi di pubblico interesse;

- alle società a controllo pubblico così come individuate in base al D. lgs. n. 175/2016.

Per quando riguarda, invece, l'ambito oggettivo di applicazione del Codice, le materie escluse sono disciplinate sempre dall'art. 2 ai commi 6 e 6-*bis*.

Con riferimento alle modifiche introdotte dal D.lgs. n. 217/2017 (secondo correttivo al CAD), l'intervento di modifica ha comportato importanti novità, come si vedrà nel prosieguo, soprattutto con riferimento alla parte del Codice relativa ai diritti digitali degli utenti che sono stati ampliati grazie all'introduzione della Carta della cittadinanza digitale (artt. 3 – 9 CAD) e all'istituzione del difensore civico per il digitale (art. 17, comma 1-quater CAD). È chiaro che quest'ultima circostanza ha considerevoli riflessi, dal lato della pubblica amministrazione, sui servizi che devono essere resi da parte della stessa agli utenti.

L'ultimo intervento di modifica organica al CAD, avvenuto ad opera del c.d. "Decreto Semplificazioni" (Decreto-legge 16 luglio 2020, n. 76, conv. con mod. dalla L. 11 settembre 2020, n. 120), invece, si è posto l'obiettivo di accelerare il processo di digitalizzazione dei rapporti tra cittadini e pubblica amministrazione, in particolare rendendo effettivo il diritto di accedere ai servizi in rete mediante le identità digitali (attraverso l'individuazione delle date di *switch off*, come si dirà meglio *infra*) e privilegiando l'utilizzo della comunicazione telematica. Sono state introdotte, inoltre, disposizioni che ridisegnano la *governance* del digitale e danno impulso ai processi di razionalizzazione delle infrastrutture, condivisione del patrimonio informativo pubblico e messa in sicurezza dei sistemi informativi (di cui si darà conto *infra*).

Appare opportuno ricordare come le disposizioni contenute nel Codice (e, più in generale, nella normativa applicabile) possono, per comodità, essere aggregate in cinque macro-aree tematiche:

- la dematerializzazione dei documenti e la gestione degli archivi;
- l'erogazione dei servizi in rete a cittadini e imprese;
- la sicurezza informatica e la tutela dei dati personali;
- la razionalizzazione della spesa per acquisti *ICT*;
- valorizzazione del patrimonio informativo delle pubbliche amministrazioni.

A ciascuna di queste macro-aree sarà dedicata un'apposita sezione del presente documento.

Oltre a quanto detto, segnatamente sul Codice dell'amministrazione digitale, va ricordato, inoltre, che l'art. 14-*bis* del CAD, alla lettera b), attribuisce all'AgID il compito di redigere e verificare l'attuazione del Piano Triennale per l'informatica nella PA, contenente la fissazione degli obiettivi e l'individuazione dei principali interventi di sviluppo e gestione dei sistemi informativi delle amministrazioni pubbliche.

Il Piano triennale 2021 – 2023[1], che rappresenta l'ultima versione delle linee strategiche definite dal Governo, detta indirizzi specifici per le amministrazioni. Il documento si compone di tre parti: la

[1] Il testo del Piano triennale per l'informatica nella PA 2021 – 2023 è consultabile all'indirizzo: https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_linformatica_nella_pubblica_amministrazione_2021-2023.pdf.

prima fornisce un quadro di riferimento e indica i principi e gli obiettivi strategici del Piano; la seconda è dedicata alle componenti tecnologiche: servizi, dati, piattaforme, infrastrutture, interoperabilità, sicurezza informatica; nella terza parte sono riportati gli strumenti di *governance* della trasformazione digitale. Ogni capitolo si articola in una parte introduttiva, che funge da raccordo con la precedente edizione del Piano e con le azioni già realizzate, un sommario del contesto normativo e strategico di riferimento, una sezione recante gli obiettivi e i risultati attesi – suddivisi in *target* scanditi nel tempo, due sezioni in cui si esplicitano le azioni che devo porre in essere AgID, il Dipartimento per la Trasformazione Digitale e le singole Amministrazioni. L'attuale edizione del Piano, che ha mantenuto la stessa organizzazione in capitoli dell'edizione 2020-2022, inoltre presenta in ogni capitolo previsioni di coordinamento con gli obiettivi e le linee di azione del Piano Nazionale di Ripresa e Resilienza[2].

2. ORGANIZZAZIONE PER LA TRANSIZIONE AL DIGITALE

Prima di procedere nell'analisi di dettaglio, va ricordato che – per consentire una più efficace e organica applicazione della normativa – il CAD impone a ciascuna pubblica amministrazione di dotarsi di un'adeguata organizzazione, nominando un "*responsabile per la transizione alla modalità digitale*" la cui figura è descritta nell'art. 17 del D.lgs. n. 82/2005, così come modificato dal D.lgs. n. 217/2017.

L'art. 17, comma 1 del CAD, infatti, prevede che all'ufficio a cui è preposto un soggetto – che può essere un dirigente o una posizione apicale - debba essere affidata: *"la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità".* La norma dispone, anzitutto, di dare attuazione al Piano Triennale per l'informatica nella PA il quale – all'interno del capitolo 8 sul governo della trasformazione digitale[3] – dedica uno specifico spazio al responsabile della transizione al digitale facendo specificamente riferimento all'obiettivo di costituire una rete di RTD, vale a dire un gruppo di lavoro permanente diffuso sul territorio per supportare le amministrazioni nella transizione al digitale. Nella sua ultima edizione, inoltre, il Piano affida alla rete di RTD il compito di definire un modello di maturità (*maturity model*) delle amministrazioni che individui i cambiamenti organizzativi e gli adeguamenti tecnologici necessari alla diffusione dello *smartworking*.

Dalla summenzionata disposizione del codice si evince altresì che il responsabile, come si approfondirà nel prosieguo, ha un importante ruolo non solo in tema di digitalizzazione ma anche in materia di dati e trasparenza.

Al medesimo ufficio sono attribuiti "*i compiti relativi a:*

[2] Il testo della Strategia per l'innovazione tecnologica e la digitalizzazione del Paese 2025 è consultabile al seguente link: https://innovazione.gov.it/assets/docs/MID_Book_2025.pdf

[3] L'idea di costituire una rete di RTD è presente già a partire dall'edizione del Piano triennale 2019-2021, consultabile al seguente link: https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2019-2021/index.html

a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;

b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;

c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;

d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;

e) analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;

f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);

g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;

h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;

i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;

j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità, nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'art. 64 – bis;

j-bis) pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b)".

L'elenco che precede è stato significativamente aggiornato dall'ultima riforma del CAD con i riferimenti al domicilio digitale, all'identità digitale e al ruolo del responsabile rispetto all'interoperabilità e agli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione (v. lett. j – *bis* introdotta dal D.lgs. n. 217/2017).

È espressamente previsto, inoltre, che il responsabile "*è dotato di adeguate competenze tecnologiche, di informatica giuridica e manageriali e risponde, con riferimento ai compiti relativi alla transizione, alla modalità digitale direttamente all'organo di vertice politico*" (art. 17, comma 1-

ter). In assenza del vertice politico, il responsabile dell'ufficio per il digitale è nominato dal vertice amministrativo al quale poi risponde (art. 17, comma 1-*sexies*).

Una volta nominato, spetta al responsabile per la transizione digitale l'impulso e il coordinamento di tutte le attività legate al rispetto delle norme in materia di digitalizzazione (di cui si parlerà nel prosieguo del presente documento).

Si aggiunge, per completezza, che la scadenza per la nomina della figura in oggetto era fissata al 31 dicembre 2017 e che i riferimenti del RTD devono essere indicati nell'Indice delle Pubbliche Amministrazioni (IPA)[4].

Tuttavia, a seguito della presa d'atto del fatto che soltanto un numero limitato di amministrazioni aveva (e, in alcuni casi, ha) provveduto ad individuare il proprio RTD, il Ministero per la Pubblica Amministrazione ha adottato la circolare n. 3/2018[5] con l'obiettivo di sollecitare, con urgenza, le pubbliche amministrazioni a provvedere alla nomina dello stesso. All'interno della suddetta Circolare viene evidenziato come l'urgenza di provvedere alla nomina sia data dalla centralità del ruolo del Responsabile per la Transizione al Digitale ai fini della trasformazione digitale dell'amministrazione e dalla necessità di garantire il pieno adempimento delle norme in materia di innovazione della pubblica amministrazione.

La circolare specifica, al fine di garantire la piena operatività dell'ufficio del RTD, che nell'atto di conferimento dell'incarico o di nomina, oltre ai compiti espressamente previsti dal CAD, possono essere previste anche una serie di altre funzioni in ragione della trasversalità della figura. In particolare: *a) il potere del RTD di costituire tavoli di coordinamento con gli altri dirigenti dell'amministrazione e/o referenti nominati da questi ultimi; b) il potere del RTD di costituire gruppi tematici per singole attività e/o adempimenti (ad esempio: pagamenti informatici, piena implementazione di SPID, gestione documentale, apertura e pubblicazione dei dati, accessibilità, sicurezza, ecc.); c) il potere del RTD di proporre l'adozione di circolari e atti di indirizzo sulle materie di propria competenza (ad esempio, in materia di approvvigionamento di beni e servizi ICT); d) l'adozione dei più opportuni strumenti di raccordo e consultazione del RTD con le altre figure coinvolte nel processo di digitalizzazione della pubblica amministrazione (responsabili per la gestione, responsabile per la conservazione documentale, responsabile per la prevenzione della corruzione e della trasparenza, responsabile per la protezione dei dati personali); e) la competenza del RTD in materia di predisposizione del Piano triennale per l'informatica della singola amministrazione, nelle forme e secondo le modalità definite dall'Agenzia per l'Italia digitale; f) la predisposizione di una relazione annuale sull'attività svolta dall'Ufficio da trasmettere al vertice politico o amministrativo che ha nominato il RTD.*

Ulteriori funzioni, poi, sono attribuite al responsabile per la transizione al digitale dalla Circolare n. 1 del 2019 recante "*Attuazione delle norme sull'accesso civico generalizzato (c.d. FOIA)*[6]" che, all'articolo 3, specifica che le indicazioni relative all'utilizzo di soluzioni tecnologiche per la gestione

[4] L'Indice è consultabile all'indirizzo https://indicepa.gov.it/
[5] Il testo completo della Circolare è consultabile all'indirizzo http://www.funzionepubblica.gov.it/articolo/dipartimento/01-10-2018/circolare-n3-del-2018
[6] Il testo integrale della circolare FOIA è disponibile all'indirizzo: http://www.funzionepubblica.gov.it/sites/funzionepubblica.gov.it/files/Circolare_FOIA_n_1_2019.pdf

delle istanze FOIA attengono ai compiti del responsabile della transizione digitale, individuati dall'art. 17 del D.lgs. 7 marzo 2005, n. 82 (Codice per l'amministrazione digitale).

L'ufficio per la transizione al digitale svolge, infine, il ruolo di "punto di contatto" sia all'interno che all'esterno dell'amministrazione di appartenenza, relazionandosi e confrontandosi con vari soggetti quali, ad esempio:

- gli organi di governo coinvolti nell'attuazione dell'Agenda digitale italiana, tra cui l'Agenzia per l'Italia Digitale e il Dipartimento per la Trasformazione Digitale, in particolare per le attività di attuazione della Strategia per la crescita digitale, del Piano Triennale e della *governance* dei processi di cooperazione istituzionale;
- l'Ufficio del difensore civico per il digitale relativamente alle segnalazioni di cui sarà destinataria l'amministrazione coinvolta;
- il *Data Protection Officer* (DPO) di riferimento per l'amministrazione, previsto dal GDPR;
- altre pubbliche amministrazioni, società partecipate e concessionari di servizi pubblici, con specifico riguardo all'interoperabilità e all'integrazione di sistemi e servizi;
- cittadini, imprese e stakeholder rispetto ai servizi *online* e agli altri temi di sua competenza.

Tra le attività trasversali del RTD, ci si sofferma su quattro profili ritenuti di particolare rilevanza:

a) formazione del personale;

b) attività di informazione per gli utenti;

c) accessibilità;

d) reingegnerizzazione dei processi.

a) Formazione del personale

L'art. 13 del CAD prevede che i soggetti tenuti all'applicazione del Codice, nell'ambito delle risorse finanziarie disponibili, debbano attuare "*anche politiche di reclutamento e formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione, nonché dei temi relativi all'accessibilità e alle tecnologie assistive*". Nell'ambito dei programmi di formazione che ciascuna amministrazione è tenuta a porre in essere, particolare attenzione deve essere dedicata agli interventi destinati ai dirigenti, in considerazione della centralità del loro ruolo nel processo di transizione digitale (così come sottolineato dal comma 1-*bis* del citato art. 13).

I programmi di formazione, inoltre, andranno adeguati al Syllabus delle competenze digitali adottato dal Dipartimento della funzione pubblica[7] e progressivamente integrati con le attività necessarie a garantire il rispetto del *codice di condotta tecnologica* (v. *infra*, Sez. 6) recentemente introdotto dal

[7] Il Syllabus "Competenze digitali per la PA" è reperibile al seguente url: https://www.competenzedigitali.gov.it/syllabus.html

D.L. 16 luglio 2020, n. 76 (c.d. Decreto "Semplificazioni", convertito con modificazioni dalla L. 11 settembre 2020, n. 120).

Il Piano Triennale 2021-2023, inoltre, pone particolare attenzione al tema della sicurezza informatica (cfr. capitolo 6), individuando linee di azione volte ad incrementare la consapevolezza degli enti sui rischi di sicurezza informatica (*Cyber Security Awareness*), a partire dalla somministrazione di questionari di *self-assessment* ai RTD, ai quali poi è affidato il compito – entro dicembre 2022 – di definire all'interno dei piani di formazione del personale gli interventi sulle tematiche di *Cyber Security Awareness*.

Sempre con riferimento ai contenuti introdotti dall'ultima edizione Piano, si rileva altresì che lo stesso prevede che, a partire dal gennaio 2022, le amministrazioni attraverso i propri RTD saranno chiamate a partecipare alle *survey* periodiche avviate da AGID, Dipartimento per la Trasformazione Digitale e Dipartimento della Funzione Pubblica, sui fabbisogni di formazione del personale in tema di trasformazione digitale.

Una volta delineato il quadro strategico degli interventi previsti per l'adeguamento alla normativa, quindi, vanno prioritariamente definite attività formative che consolidino le competenze del personale in materia tecnico-informatica, anche con riferimento alla *privacy* e all'accessibilità.

b) Attività di informazione per gli utenti

Com'è noto, l'erogazione di servizi *online* da parte dei soggetti pubblici, che verrà approfondita nell'ambito della sezione 4 del documento, è uno dei principali obiettivi delle politiche di digitalizzazione amministrativa, sia nazionali che dell'Unione Europea.

Con riferimento al ruolo dell'utenza rispetto ai servizi resi, l'art. 7, comma 1 del CAD, come modificato dal Correttivo, prevede che: "*i soggetti di cui all'articolo 2, comma 2, provvedono alla riorganizzazione e all'aggiornamento dei servizi resi, sulla base di una preventiva analisi delle reali esigenze degli utenti e rendono disponibili on line i propri servizi nel rispetto delle disposizioni del presente Codice e degli standard e dei livelli di qualità individuati e periodicamente aggiornati dall'AgID con le proprie linee guida tenuto anche conto dell'evoluzione tecnologica anche in termini di fruibilità, accessibilità, usabilità e tempestività, stabiliti con le regole tecniche di cui all'articolo 71*". In relazione a tali servizi, l'art. 7, comma 3 del CAD rende obbligatoria la rilevazione del giudizio degli utenti sulla qualità del servizio reso e la pubblicazione dei relativi dati sul sito istituzionale dell'organizzazione insieme alle relative statistiche di utilizzo.

Così come previsto dall'art. 7, comma 1, del CAD, poi, gli *standard* e i livelli di qualità sono definiti e aggiornati dall'Agenzia per l'Italia Digitale che ha pubblicato numerosi provvedimenti attuativi (ad es. in materia di accessibilità, nonché di *design* dei siti[8] e dei progetti digitali[9]).

[8] Le Linee Guida per il design dei siti Web e dei servizi *online* sono disponibili all'url: https://designers.italia.it/

[9] Le indicazioni per lo sviluppo dei progetti digitali sono contenute nel Piano Triennale per l'Informatica nella Pubblica Amministrazione 2021-2023, disponibile all'url: https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_linformatica_nella_pubblica_amministrazione_2021-2023.pdf.

c) Accessibilità

Il tema dell'accessibilità interessa in modo trasversale la pubblica amministrazione e, nella recente evoluzione normativa, ha assunto i lineamenti di una vera e propria linea strategica di attività, la cui attuazione richiede il coinvolgimento di tutti i soggetti che erogano servizi di rilievo pubblico. Al centro di questa strategia si collocano gli strumenti informatici delle amministrazioni, rispetto ai quali l'accessibilità si atteggia a requisito tecnico il cui rispetto deve essere assicurato in sede di acquisto o sviluppo.

L'accessibilità, però, è opportuno precisare sin da subito, non è solo un profilo di carattere tecnico-informatico, ma rappresenta anche un obiettivo organizzativo, il cui perseguimento deve essere considerato a monte, cioè in fase di pianificazione e programmazione dell'attività amministrativa o di servizio.

Il quadro normativo interno trova il suo punto di riferimento nella c.d. Legge "Stanca" – l. 9 gennaio 2004, n. 4, recante "*Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici*", da ultimo modificata ad opera del d. lgs. del 10 agosto 2018, n. 106, con cui è stata recepita la Direttiva (UE) 2016/2102 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici.

In attuazione dell'art. 3 della Costituzione, l'art. 1 della Legge "Stanca" sancisce il diritto delle persone con disabilità di accedere ai servizi informatici e telematici della pubblica amministrazione e ai servizi di pubblica utilità erogati da altri soggetti. Il tema dell'accessibilità, infatti, è strettamente collegato alla parità di trattamento delle persone con disabilità e alla loro tutela contro forme di discriminazione, diretta o indiretta (cfr. art. 2, l. n. 67 del 2006), che possono realizzarsi, tra l'altro, in presenza di barriere di accessibilità negli strumenti informatici.

Come anticipato, ai sensi dell'art. 17, comma 1, lett. d) del CAD, l'ufficio RTD è competente anche in materia di accessibilità. Nel CAD, come vedremo, diverse norme rinviano al tema dell'accessibilità, il quale non si esaurisce nella predisposizione di siti web o applicativi mobili di tipo accessibile, giacché lo stesso deve trovare adeguata considerazione nella riorganizzazione dei processi dell'amministrazione. Il 26 novembre 2019 l'AgID, ai sensi dell'art. 11 della Legge "Stanca", ha approvato le *Linee guida sull'accessibilità degli strumenti informatici*[10], le quali sono destinate ad avere un ruolo decisivo nell'attuazione della strategia sull'accessibilità. Questa, in estrema sintesi, si muove in una triplice direzione, cui corrispondono altrettanti obiettivi di accessibilità. Il RTD, infatti, deve assicurare l'accessibilità:

a) per quanto concerne i documenti informatici, attraverso la formazione di originali accessibili (cfr. art. 23-*ter*, del CAD);

[10] Le Linee guida sull'accessibilità degli strumenti informatici, come di recente rettificate dalla det. D.G. dell'AgID dell'8 settembre 2020, n. 396, sono consultabili al seguente link: https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/202531636210O__OLinee+Guida+Accessibilit%E0+versione+rettifica+del+23+luglio+2020+%28002%29.pdf

b) per quanto riguarda strumenti e servizi informatici, esigendo il rispetto dei requisiti tecnici di accessibilità in sede di approvvigionamento di hardware, software ed applicativi quali siti *web* e applicazioni mobili (cfr. art. 4, l. n. 4/2004);

c) più in generale, con riguardo all'intera attività dell'amministrazione di appartenenza, organizzando attività di formazione del personale che abbiano specifico riguardo al tema (cfr. art. 13, CAD e art. 8, l. n. 4/2004).

Con riferimento al punto a), si deve segnalare che, in ossequio a quanto disposto dal comma 5-*bis* dell'art. 23-*ter* del CAD, i documenti informatici dell'amministrazione devono essere fruibili indipendentemente dalla condizione di disabilità del personale. Detto obbligo si traduce in un duplice onere in capo al RTD, il quale, da una parte, deve esigere che i documenti prodotti dall'amministrazione siano conformi allo standard di accessibilità documentale richiesto dalla normativa e definito dalle Linee guida, dall'altra, deve occuparsi di censire la documentazione esistente, al fine di individuare i documenti non accessibili di cui disporre l'adeguamento. A tal proposito, si invita alla consultazione della "*Guida pratica per la creazione di un documento accessibile*" elaborata dall'AgID, anche al fine di rendere accessibili le copie informatiche di originali analogici[11]. La declinazione operativa di tali indicazioni nella realtà di ogni singola organizzazione dovrà avvenire – sotto il coordinamento del RTD – a cura del responsabile per la gestione documentale.

Con riferimento al punto b), le Linee guida individuano le diverse tipologie di strumento informatico di cui deve essere garantita l'accessibilità: hardware, pagine web[12], documenti non web, software, applicazioni mobili, documentazione e servizi di supporto. Per ciascuna tipologia di strumento sono individuate le norme tecniche di riferimento. Nelle Linee guida, inoltre, sono fornite indicazioni per l'identificazione delle tecnologie assistive da impiegare sulle postazioni di lavoro a disposizione del dipendente con disabilità e sono rese, inoltre, raccomandazioni e precisazioni sull'accessibilità digitale dei servizi pubblici erogati a sportello dalle amministrazioni.

Un'altra importante novità contenuta nelle Linee guida è l'individuazione delle modalità per la redazione della **Dichiarazione di accessibilità** di cui all'art. 3 *quater* della Legge "Stanca", che consentirà ad AgID il monitoraggio sul rispetto degli obblighi di legge in materia di accessibilità dei siti web e delle applicazioni mobili (si segnala che, come previsto dalle Linee guida, il primo monitoraggio di AgID è già iniziato a gennaio 2020 e si concluderà a dicembre 2021). In particolare, con l'all. 1 è fornito il Modello di dichiarazione di accessibilità[13], che le amministrazioni sono tenute a compilare e rilasciare nel rispetto delle tempistiche che le stesse Linee guida impongono al par.

[11] Link: https://www.agid.gov.it/sites/default/files/repository_files/linee_guida/guida_pratica_creazione_word_accessibile_2.pdf

[12] Con riferimento ai servizi, si veda anche la Circolare AgID n. 3/2017, disponibile al link https://www.agid.gov.it/sites/default/files/repository_files/uploads/193/circolare_agid_03-2017_servizi_a_sportello_accessibili.pdf), nonché le Linee Guida per il design dei siti Web e dei servizi *online,* reperibili al seguente link: https://designers.italia.it/

[13] Il Modello di dichiarazione di accessibilità, All. 1 alle Linee guida sull'accessibilità degli strumenti informatici, è disponibile al seguente url: https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/193569075700__OAllegato+1+-+Modello+di+Dichiarazione+di+Accessibilit%E0.pdf

4.1. Le informazioni rese nella Dichiarazione, si precisa, potranno essere ricavate da una delle seguenti analisi: un'autovalutazione effettuata direttamente dal soggetto erogatore, una valutazione effettuata da terzi, oppure una valutazione effettuata con il "Modello di autovalutazione" di cui all'all. 2 delle medesime Linee guida[14]. Le dichiarazioni compliate, poi, devono essere pubblicate tramite il sito form.agid.gov.it.

Si sottolinea, infine, che al par. 4.2 delle Linee Guida – che ha sostituito la circolare AgID n. 1 del 2016 – è ribadito l'obbligo per le pubbliche amministrazioni (ai sensi del d.l. n. 179/2012, articolo 1, comma 2) di pubblicare sul proprio sito web entro il 31 di marzo di ogni anno gli **obiettivi di accessibilità** per l'anno corrente e lo stato di attuazione del piano per l'utilizzo del telelavoro. Si tratta di documenti strategici di cui il RTD deve curare la redazione e l'aggiornamento.

Le Linee guida, infine, hanno esplicitato il concetto di "onere sproporzionato" di cui all'art. 3-*ter*, comma 2 della Legge "Stanca", il cui riscontro in concreto, se debitamente motivato, può consentire la deroga degli obblighi previsti dalla legge. Compete ad AgID la verifica, sia sulla conformità della Dichiarazione, sia sulla concreta applicabilità della fattispecie di onere sproporzionato.

È opportuno segnalare che da eventuali contestazioni di AgID posso scaturire misure correttive indirizzate all'amministrazione.

d) Reingegnerizzazione dei processi

Come esposto, al RTD viene affidata la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità.

Attività preliminari per procedere alla trasformazione digitale dell'amministrazione sono la mappatura dei processi dell'amministrazione e la loro successiva reingegnerizzazione. Quest'ultima, d'altra parte, è alla base di ciascun compito assegnato dalla normativa al RTD.

Ci si sofferma segnatamente sulla riorganizzazione e reingegnerizzazione di due ambiti di attività che meritano attenzione poiché di particolare rilievo per l'amministrazione.

d.1) L'attività degli organi collegiali

La trasformazione digitale non investe solo l'attività strettamente amministrativa degli enti ma riguarda anche quella politica.

In mancanza di una normativa generale in materia, le amministrazioni fin qui hanno scelto se prevedere nei rispettivi atti organizzativi la modalità telematica per lo svolgimento delle riunioni degli organi collegiali, disciplinandone strumenti e modalità.

[14]Il Modello di autovalutazione, All. 2 alle Linee guida sull'accessibilità degli strumenti informatici, è disponibile al seguente url:
https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/193569081100__OAllegato+2+-+Modello+di+autovalutazione.pdf

A tale proposito, peraltro, si segnala che, in seguito all'aggravarsi dell'emergenza epidemiologica da covid-19, il Governo ha adottato provvedimenti urgenti che incidono in modo significativo sull'organizzazione delle pubbliche amministrazioni. La necessità di mitigare il rischio di contagio e al tempo stesso garantire la continuità dell'azione amministrativa ha richiesto, infatti, una netta accelerazione della transizione al digitale degli enti.

In particolare, con riferimento al profilo in oggetto, le disposizioni introdotte con il D.L. 17 marzo 2020, n. 18 (c.d. Decreto-Legge "Cura Italia", convertito in legge con modificazioni dalla L. 24 aprile 2020, n. 27) hanno interessato l'organizzazione dell'attività delle amministrazioni anche con riferimento all'attività degli organi collegiali. È stato disposto, infatti, che gli organi collegiali degli enti locali (Consiglio e Giunta) possono svolgere le proprie sedute in videoconferenza anche in assenza di uno specifico regolamento dell'ente (cfr. art. 73 D.L. Cura Italia). Affinché gli enti possano beneficiare di tale deroga, la norma richiede:

- che siano rispettati criteri di trasparenza e tracciabilità previamente fissati dalla presidenza dell'organo o dal sindaco;

- che durante la seduta sia garantito l'esercizio delle funzioni del Segretario dell'ente;

- che siano adottati sistemi che consentano di identificare con certezza i partecipanti alla seduta;

- che sia data adeguata pubblicità alla seduta (ad es., mediante trasmissione in diretta *streaming* o successiva pubblicazione della registrazione della seduta sul sito istituzionale).

d.2) L'organizzazione del lavoro dei dipendenti

I processi di riorganizzazione finalizzati alla transizione digitale riguardano anche le modalità di svolgimento dell'attività lavorativa da parte dei dipendenti, con conseguente possibilità di evoluzione verso il c.d. "*smart working*" (o lavoro agile).

Lo *smart working* non va confuso con il telelavoro[15]. Il telelavoro, infatti, prevede lo spostamento (in tutto o in parte) della sede di lavoro dagli uffici ad altra sede ma il dipendente è vincolato, comunque, a lavorare da una postazione fissa e prestabilita, con gli stessi limiti di orario che avrebbe in ufficio. Il 23 marzo 2000 è stato stipulato l'Accordo quadro nazionale per l'applicazione del telelavoro ai rapporti di lavoro del personale dipendente delle pubbliche amministrazioni. Con la circolare INPS n. 52 del 27 febbraio 2015 ("Disposizioni attuative dell'Accordo Nazionale sul progetto di telelavoro domiciliare") vengono illustrate le attività interessate e le modalità di attivazione del telelavoro, con particolare riferimento alle misure di prevenzione e protezione.

Con riferimento allo *smart working*, la Legge 22 maggio 2017 n. 81 disciplina il lavoro agile, che viene definito all'articolo 18 come: "*modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza*

[15] V. legge n. 191 del 1998. Le concrete modalità attuative sono poi state dettate dal D.P.R. n. 70 del 1999 "Regolamento recante disciplina del telelavoro nelle pubbliche amministrazioni, a norma dell'articolo 4, comma 3, della legge 16 giugno 1998, n. 191". Il telelavoro viene definito come quella forma di lavoro svolto a distanza, ovvero al di fuori dell'azienda e degli altri luoghi in cui tradizionalmente viene prestata l'attività lavorativa ma, al contempo, funzionalmente e strutturalmente collegato ad essa grazie all'ausilio di strumenti di comunicazione informatici e telematici.

precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa. La prestazione lavorativa viene eseguita, in parte all'interno di locali aziendali e in parte all'esterno senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva". Obiettivo dichiarato è promuovere il lavoro agile per "*incrementare la competitività e agevolare la conciliazione dei tempi di vita e di lavoro".* Il comma 3 precisa che le disposizioni normative si applicano anche ai "*rapporti di lavoro alle dipendenze delle amministrazioni pubbliche".*

La Direttiva n. 3 del 2017 del Presidente del Consiglio dei Ministri e della Ministra Madia contiene le linee guida per la nuova organizzazione del lavoro, finalizzate a promuovere la conciliazione dei tempi di vita e di lavoro dei dipendenti in attuazione dei commi 1 e 2 dell'articolo 14 della Legge delega 7 agosto 2015, n. 124.

Come noto, in seguito al verificarsi dell'emergenza sanitaria da Covid-19, il processo di transizione verso forme di lavoro agile nelle amministrazioni ha visto una notevole accelerazione, resa possibile anche dalla previsione di semplificazioni normative volte a garantire nel contesto emergenziale la continuità dell'attività amministrativa e l'erogazione dei servizi.

In particolare, in una prima fase, il Decreto "Cura Italia" ha previsto che, fino alla cessazione dello stato di emergenza sanitaria, il lavoro agile rappresenta la modalità ordinaria di svolgimento della prestazione lavorativa nelle pubbliche amministrazioni (cfr. art. 87, comma 1, D.L. Cura Italia – nella versione al tempo vigente – e Decreto del Ministro per la PA del 19 ottobre 2020)[16], in particolare prevedendo la possibilità di ricorrere allo *smart working* anche a prescindere dalla stipula di accordi individuali con il lavoratore[17].

In seguito, il "Decreto Semplificazioni 2020" è intervenuto direttamente sul Codice dell'amministrazione digitale che, all'art. 12, già conteneva norme volte a favorire l'utilizzo da parte dei lavoratori di **dispositivi elettronici personali o personalizzabili.** A tale ultimo proposito, ha

[16] Si segnala che le misure straordinarie per le PA contenute nel D.L. Cura Italia erano state in parte anticipate dal Ministero della Pubblica Amministrazione, con i provvedimenti di indirizzo reperibili ai link indicati:
- circolare MPA n. 1 del 4 marzo 2020, recante "Misure incentivanti per il ricorso a modalità flessibili di svolgimento della prestazione lavorativa":
http://www.funzionepubblica.gov.it/sites/funzionepubblica.gov.it/files/Circolare_n_1_2020.pdf;
- direttiva MPA n. 2 del 12 marzo 2020, recante "indicazioni in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19 nelle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165" (che sostituisce integralmente la direttiva n. 1 del 25 febbraio 2020):
http://www.funzionepubblica.gov.it/sites/funzionepubblica.gov.it/files/Direttiva_2_20.pdf;
- Circolare MPA n. 3 del 2020 recante "Modalità di svolgimento della prestazione lavorativa nell'evolversi della situazione epidemiologica da parte delle pubbliche amministrazioni":
http://www.funzionepubblica.gov.it/sites/funzionepubblica.gov.it/files/DIR_3_2020.pdf.

[17] Tale disposizione, si segnala fin da subito, si deve ritenere ormai superata, sia per l'approssimarsi della scadenza del termine dello stato emergenziale – che, al momento in cui si scrive, non è stato ancora oggetto di proroga – che per effetto della recente adozione del Decreto del Ministro per la PA dell'8 ottobre 2021, recante "Modalità organizzative per il rientro in presenza dei lavoratori delle pubbliche amministrazioni"). Tale ultimo decreto, a firma del Ministro Brunetta, infatti ha stabilito misure per il superamento dell'utilizzo del lavoro agile emergenziale come una delle modalità ordinarie dello svolgimento della prestazione lavorativa nella PA. Ciò non esclude, tuttavia, la possibilità di ricorrere al lavoro agile secondo le regole ordinarie.

previsto che ai lavoratori sia data **un'adeguata informazione sull'uso sicuro degli strumenti impiegati, in particolare i servizi in cloud** e, inoltre, che le pubbliche amministrazioni adottino ogni misura atta a garantire la **sicurezza informatica e la protezione dei dati**, compresa la diffusione di **linee guida** presso i lavoratori o la regolamentazione delle attività che possono essere svolte, **previa informazione delle organizzazioni sindacali** nel caso di utilizzo di dispositivi personali dei lavoratori.

Al fine di agevolare la diffusione del lavoro agile, poi, è stata inserita, sempre nell'ambito dell'art. 12 CAD, una disposizione specificamente rivolta alle pubbliche amministrazioni in senso stretto. Queste ultime, quando **acquistano beni o progettano e sviluppano i sistemi informativi e i servizi informatici, devono farlo assicurando che siano previste modalità idonee a consentire ai lavoratori di accedere da remoto ad applicativi, dati e informazioni necessari allo svolgimento della prestazione lavorativa,** assicurando un adeguato livello di **sicurezza informatica**.

Tra le novità introdotte nella fase emergenziale, ma destinate a produrre effetti anche a emergenza conclusa, si segnalano anche le disposizioni concernenti il **Piano organizzativo del lavoro agile** (**POLA**).

L'articolo 14 della Legge 7 agosto 2015, n. 124, come recentemente modificato ad opera dell'art. 263 del D.L. n. 34/2020 (c.d. Decreto "Rilancio", conv. con mod. dalla L. n. 77/2020) nonché del D.L. 56/2021, prevede che **entro il 31 gennaio di ciascun anno**, le PA, sentite le organizzazioni sindacali, redigono il POLA quale sezione del Piano delle performance di cui al D.lgs. n. 150/2009. Il POLA deve individuare le modalità attuative del lavoro agile, e in particolare:

1. le misure organizzative;

2. i requisiti tecnologici;

3. i percorsi formativi del personale, anche dirigenziale;

4. gli strumenti di rilevazione e di verifica periodica dei risultati conseguiti, anche in termini di miglioramento dell'efficacia e dell'efficienza dell'azione amministrativa, della digitalizzazione dei processi, nonché della qualità dei servizi erogati.

Ai sensi di legge il POLA deve prevedere, per le attività che possono essere svolte in modalità agile, che almeno il 15 per cento dei dipendenti possa avvalersene[18].

[18] La legge prevede, inoltre, che le economie derivanti dall'applicazione del POLA restano acquisite al bilancio di ciascuna amministrazione pubblica, mentre in caso di mancata adozione del POLA, è previsto che il lavoro agile deve essere applicato ad almeno il 15 per cento dei dipendenti dell'ente, ove lo richiedano.
Si segnala, inoltre, che il Ministro per la Pubblica Amministrazione, con D.M. del 9 dicembre 2020, ha approvato le "***Linee guida sul piano organizzativo del lavoro agile (POLA) e indicatori di performance***", al fine di fornire alcune indicazioni metodologiche per supportare le amministrazioni nel passaggio della modalità di lavoro agile dalla fase emergenziale a quella ordinaria, in linea con quanto richiesto dall'art. 14, co. 1, della L. 7 agosto 2015, n. 124, come modificato dall'art. 263, co. 4-*bis*, del D.L. n. 34/2020.
Da ultimo, si segnala che, a norma dell'art. 1, co. 1, D.L. 56/2021 (Disposizioni urgenti in materia di termini legislativi), i termini di cui all'art. 263, comma 1, D.L. n. 34/2020 – disposizione concernete semplificazioni in materia di lavoro agile nella PA, tra cui, in particolare, la possibilità di ricorrere allo *smart working* a prescindere dagli accordi individuali e dagli obblighi informativi di cui agli artt. 18 e 23 della L. n. 81/2017 – sono prorogati fino alla data di cessazione dello stato di emergenza epidemiologica da COVID-19 e comunque non oltre il 31 dicembre 2021.

Da ultimo, preme segnalare che ai sensi dell'art. 6 del D.L. n. 9 giugno 2021, n. 80 (conv. con mod. dalla L. 6 agosto 2021, n. 113), per le pubbliche amministrazioni con più di cinquanta dipendenti è prevista l'adozione, entro il 31 gennaio di ogni anno, del **Piano integrato di attività e organizzazione delle amministrazioni pubbliche**, il quale deve prevedere, tra l'altro, anche la strategia di gestione del capitale umano e di sviluppo organizzativo, anche mediante il lavoro agile[19] (il termine per l'adozione del PIAO per l'anno 2022, si segnala, è stato prorogato al 30 aprile).

Organizzazione per la transizione al digitale del Consiglio regionale della Sardegna – Stato dell'arte e adempimenti

Una volta delineato il quadro normativo vigente in materia di transizione alla modalità operativa digitale delle pubbliche amministrazioni, si segnalano gli adempimenti che si ritengono di prioritaria rilevanza per l'Amministrazione consiliare.

I. Nomina ufficio RTD

Con riguardo all'organizzazione predisposta per la transizione al digitale, il Consiglio regionale, con delibera dell'Ufficio di Presidenza n. 157 del 30 novembre 2021, ha nominato il Responsabile per la transizione alla modalità operativa digitale (RTD) ai sensi dell'art. 17 del d. lgs. n. 82 del 2005, individuandolo nella persona della Dott.ssa Maria Rita Gatto, già Vice Segretario Generale. L'atto di nomina, inoltre, affida al Segretario Generale del Consiglio regionale il compito di adottare gli appositi atti organizzativi interni finalizzati all'istituzione di un gruppo di lavoro permanente costituito dalle professionalità necessarie a supportare il RTD nello svolgimento delle proprie funzioni.

Con riferimento alla forma della nomina, pertanto, si ritiene che, in conformità alle disposizioni richiamate, l'Amministrazione consiliare abbia correttamente inquadrato il RTD come un ufficio – con a capo un dirigente o una figura apicale – dotato di competenze giuridiche, manageriali e tecniche.

Con riferimento ai contenuti dell'atto di nomina, nel quale sono individuati i poteri e i compiti del RTD, si segnala che lo stesso potrebbe essere utilmente aggiornato con il riferimento alle più recenti novità in materia, sia normative, sia di indirizzo amministrativo. Ci si riferisce, in particolare:

- alla Circolare MPA n. 3 del 2018;

- alla Circolare del Dipartimento della Funzione Pubblica n. 1 del 2019;

- al nuovo Piano triennale per l'informatica nella pubblica amministrazione 2021-2023 dell'AgID.

[19] Si segnala che il nuovo Piano integrato, secondo quanto previsto dalla norma citata, presumibilmente integrerà e sostituirà i contenuti già previsti nel Piano della performance, nel Piano del fabbisogno del personale, nonché nel POLA. A tal fine, tuttavia, sarà necessaria l'adozione di un apposito D.P.R., che individuerà con precisione i documenti pianificatori che saranno integrati e sostituiti dal nuovo Piano.

Com'è noto, in base alla norma, il RTD deve essere interno all'amministrazione e non è richiesto – come per altre figure (tra cui il RPD previsto dalla normativa *privacy* e il RPCT previsto dalla normativa anticorruzione) – che non si trovi in conflitto di interesse. Al contrario, il Responsabile per la transizione alla modalità operativa digitale deve essere il soggetto che all'interno delle amministrazioni – per funzione e competenze – sia meglio in condizione di svolgere le attività di stimolo e coordinamento che la norma gli assegna. In particolare, con riferimento alle funzioni attribuite all'ufficio dalla circolare MPA n. 3 del 2018, quest'ultima si sofferma sulla possibilità del responsabile di convocare tavoli di lavoro e di promuovere atti di indirizzo. Si tratta di elementi che è importante inserire nella nomina per rafforzare il ruolo dell'ufficio RTD quale punto di riferimento interno all'amministrazione per altre figure con cui deve necessariamente interfacciarsi (es. RPCT, RPD ecc.).

Si ricorda, inoltre, che l'ufficio dovrebbe intrattenere anche diversi rapporti con l'esterno (perlomeno con l'AgID e con il Dipartimento per la Trasformazione Digitale), oltre che con le altre amministrazioni. Pertanto, la nomina dovrebbe far riferimento anche a tali rapporti.

Si rileva, infine, che i dati di contatto del RTD nominato, già pubblicati in IPA, dovrebbero essere pubblicati anche sul sito istituzionale del Consiglio regionale, dando evidenza dell'incarico conferito.

II. Risorse assegnate all'ufficio RTD

Con riferimento segnatamente all'organizzazione dell'ufficio, si deve rilevare che il pieno svolgimento delle funzioni a esso affidate presuppone necessariamente la possibilità di disporre, oltre che di risorse umane, di un *budget* e che la nomina dovrebbe recare previsioni anche in tal senso.

III. Adempimenti

Secondo quanto rappresentato nel questionario, l'Amministrazione consiliare non ha adotta il piano triennale per l'informatica. Tra gli adempimenti cui dare priorità si raccomanda, pertanto, si di procedere alla redazione del piano, adeguato ai contenuti del Piano Triennale dell'AgID 2021-2023, in cui devono confluire tutte le attività relative all'attuazione della transizione digitale dell'amministrazione che richiedono programmazione (adempimenti, acquisti informatici, migrazione dei servizi, formazione del personale, etc.). Si ricorda che, una volta predisposto, il piano deve essere condiviso con l'organo politico competente a deliberarne l'approvazione (nel Vostro caso, l'Ufficio di Presidenza).

Una volta adottato, il piano deve essere pubblicato sul sito istituzionale dell'amministrazione nella sezione "Amministrazione trasparente", sottosezione "Atti generali".

L'Amministrazione consiliare, secondo quanto rappresentato, ha implementato le misure minime di sicurezza di cui alla Circolare dell'AgID n. 2 del 2017. Si ricorda che il modulo di implementazione delle misure minime, una volta compilato dal RTD, deve essere periodicamente aggiornato. Si ricorda altresì che dopo la compilazione il modulo deve essere firmato digitalmente, marcato temporalmente e versato in conservazione. Andranno previsti

altresì piani di emergenza in grado di assicurare la continuità operativa ai sensi dell'art. 51 CAD.

Inoltre, d'intesa con l'area risorse umane, il RTD dovrebbe pianificare le seguenti attività:

• pianificazione delle sessioni di formazione del personale in materia informatica (sia dal punto di vista tecnologico che giuridico). Secondo quanto rappresentato, l'amministrazione già organizza tali attività. Si raccomanda di coordinare le attività di formazione in materia informatica (in modo da razionalizzare la spesa e l'impiego delle risorse) anche con quelle di formazione in materia di protezione dei dati personali (di cui al Regolamento (UE) n. 2016/679);

• organizzazione di attività informative per gli utenti, ad esempio, sui servizi *online* e sulle modalità di interazione telematica con l'amministrazione consiliare.

Si raccomanda, altresì, che il Responsabile pianifichi la redazione di una relazione periodica sull'attività svolta da inviare all'organo che lo ha nominato.

IV. Lavoro agile

Secondo quanto da Voi rappresentato, il Consiglio consente ai lavoratori di svolgere la prestazione lavorativa in modalità agile e le relative modalità sono disciplinate in un apposito atto regolamentare.

Secondo quanto rappresentato, inoltre, il Consiglio ha adottato una politica sull'uso delle risorse informatiche, che tuttavia non è stata trasposta in un apposito disciplinare da distribuire ai dipendenti. Si raccomanda, pertanto, di provvedere in tal senso. Si ricorda che la politica d'uso dovrebbe consentire ai dipendenti l'utilizzo di risorse informatiche anche personali, dettando misure per garantire la protezione dei dati personali trattati e la sicurezza informatica, nel rispetto del Reg. (UE) 2016/679.

L'Amministrazione consiliare, inoltre, dovrebbe adottare il Piano organizzativo del lavoro agile (POLA). Come previsto dall'articolo 14, comma 1, della L. n. 124/2015, (come recentemente modificato ad opera dell'art. 263 del D.L. n. 34/2020, conv. con mod. dalla L. n. 77/2020), entro il 31 gennaio di ciascun anno le amministrazioni pubbliche, sentite le organizzazioni sindacali, individuano le modalità attuative del lavoro agile nell'ambito del POLA, redatto quale sezione del Piano della performance di cui al D.lgs. n. 150/2009. A tal proposito si rammenta che, secondo quanto previsto dal recente D.L. n. 80/2021, i contenuti del POLA presumibilmente confluiranno nel nuovo Piano integrato di attività e organizzazione delle amministrazioni pubbliche (PIAO), alla cui adozione sono tenute le amministrazioni con almeno 50 dipendenti.

V. Accessibilità

Secondo quanto rappresentato, il Consiglio regionale non ha provveduto alla pubblicazione degli obiettivi di accessibilità per l'anno 2021. Si rammenta che l'obbligo, in accordo con

quanto ribadito al par. 4.2 dalle Linee guida AgID sull'accessibilità degli strumenti informatici, deve essere ottemperato entro il 31 marzo di ogni anno.

È compito del RTD redigere il documento che individua gli obiettivi di accessibilità. A tal fine, in vista della prossima pubblicazione (31 marzo 2022), si suggerisce di procedere alla redazione di tale documento partendo da una ricognizione dello stato di attuazione della disciplina sull'accessibilità nell'Amministrazione consiliare, tenendo conto poi, in sede di individuazione degli obiettivi, delle tre direttrici strategiche sull'accessibilità di cui si è detto *supra*.

Si ricorda che per la redazione e la pubblicazione annuale degli obiettivi l'AgID ha messo a disposizione degli enti un'apposita applicazione, raggiungibile all'indirizzo https://form.agid.gov.it.

L'Amministrazione consiliare, inoltre, non ha provveduto a pubblicare la Dichiarazione di Accessibilità del proprio sito web istituzionale. Si ricorda che il RTD deve provvedere a rilasciare la dichiarazione di accessibilità, oltre che per i siti web, anche per le applicazioni mobili in uso presso la Vostra Amministrazione.

Infine, si ricorda che, in accordo a quanto stabilito nelle Linee Guida in materia, entro il 23 settembre di ogni anno, l'amministrazione è tenuta a riesaminare e validare l'esattezza delle affermazioni contenute nella dichiarazione di accessibilità, avvalendosi esclusivamente della piattaforma predisposta dall'AgID.

VI. Mappatura dei procedimenti e reingegnerizzazione dei processi

Fermo restando tutto quanto appena esposto, occorre specificare, infine, che l'aspetto organizzativo fondamentale e preliminare alla stessa transizione al digitale è rappresentato dalla mappatura di tutti i procedimenti amministrativi con eventuale conseguente aggregazione in processi. D'altra parte, si ricorda è compito dell'RTD provvedere alla reingegnerizzazione dei processi (art. 17 CAD), previa mappatura di tutti i procedimenti amministrativi dell'Amministrazione consiliare, con eventuale conseguente aggregazione in processi, aspetto organizzativo fondamentale e preliminare alla stessa transizione al digitale.

Oltre alla reingegnerizzazione di tutti i processi relativi all'attività amministrativa, si invita il l'Amministrazione a favorire lo svolgimento delle attività in via telematica. Secondo quanto rappresentato, tali attività sono già consentite, sebbene non disciplinate da un apposito regolamento. A tal riguardo, si rileva che gli organi collegiali dell'Amministrazione consiliare non sembrano rientrare nell'ambito di applicazione dell'art. 73 del Decreto "Cura Italia" (D.l. n. 18/2020), norma recante "Semplificazioni in materia di organi collegiali". Pertanto, al fine di garantire regolarità, tracciabilità, trasparenza e sicurezza delle sedute in videoconferenza, i requisiti delle soluzioni tecnologiche e criteri di svolgimento delle sedute devono trovare compiuta definizione in un apposito atto regolamentare. Peraltro, si ricorda che la deroga prevista nel richiamato art. 73 è condizionata al perdurare dello stato di emergenza sanitaria (la cui durata, al momento in cui si scrive, è prevista fino al 31 marzo 2022).

3. LA DEMATERIALIZZAZIONE DEI DOCUMENTI E DEGLI ARCHIVI

Una cospicua parte di disposizioni del CAD è dedicata alla dematerializzazione dei documenti e degli archivi. Il presupposto da cui muove il Legislatore, infatti, è quello di ritenere che, grazie ai documenti informatici, possano essere conseguiti importanti vantaggi sotto il profilo del risparmio di spesa e dell'efficientamento organizzativo.

Com'è noto, in effetti, per il principio di documentalità, nel procedimento amministrativo, ogni passaggio – dalla fase dell'iniziativa a quella deliberativa – e lo stesso provvedimento finale devono avere evidenza documentale.

Le norme contenute nel CAD hanno, quindi, la duplice finalità di imporre, dove possibile, l'abbandono dei documenti analogici (cioè cartacei) e di adottare tutte le cautele che consentano al digitale di soddisfare gli stessi crismi di affidabilità, certezza e sicurezza del cartaceo.

Sotto questo profilo, le disposizioni contenute nel CAD sono riferite a tre distinti aspetti del ciclo di vita del documento informatico:

a) la gestione;

b) la formazione;

c) la conservazione nel tempo.

Si farà cenno, nell'ambito della successiva sezione 3.A relativa alla gestione documentale, ad un'ulteriore fase fondamentale del ciclo di vita del documento informatico, ossia quella della trasmissione (comunicazioni con altre amministrazioni, imprese, professionisti e altri cittadini).

È importante sin da subito sottolineare che la disciplina del ciclo di vita del documento informatico ha subito di recente un importante intervento normativo.

Il 10 settembre 2020, infatti, AgID ha pubblicato le *Linee guida sulla formazione, gestione e conservazione dei documenti informatici*[20]. Obiettivo delle Linee Guida è quello di raccogliere in un unico provvedimento normativo materie prima disciplinate separatamente. Esse recano una disciplina coordinata e omogenea che regola l'intero ciclo di vita del documento informatico, dalla formazione fino alla conservazione, passando per la fase di gestione.

Gli allegati alle Linee Guida sono da considerarsi parte integrante delle stesse e contengono:

1. Glossario dei termini e degli acronimi;

[20] Le *Linee guida sulla formazione, gestione e conservazione dei documenti informatici* e i relativi allegati, nella versione approvata dall'AgID con det. D.G. del 9 settembre 2020, n. 407, sono reperibili al seguente link: https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/2025314490100__O407+DT+DG+n.+407+-+9+sett+2020+-Determinazione+adozione+linee+guida+formazione+gestione+e+conservazione+dei+documenti+informatici.pdf.
L'ultima versione del testo Linee guida e degli allegati n. 5 e 6, come modificati con det. D.G. del 17 maggio 2021, sono reperibili al seguente link: https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/2113616591900__O371+dt+dg+n.+371+modifiche+allegati+e+proproga+termini+di+adozione_1+002.pdf.

2. Formati di File e Riversamento;
3. Certificazione di processo;
4. Standard e specifiche tecniche;
5. Metadati;
6. Comunicazione tra AOO di Documenti Amministrativi Protocollati.

Con riferimento alla portata applicativa, è opportuno sottolineare che - come precisato dal Consiglio di Stato nell'ambito del parere reso sullo schema di decreto legislativo del correttivo al CAD, n. 2122/2017 - le Linee guida, adottate da AGID ai sensi dell'art. 71 del CAD, assumono natura di **atto regolamentare** (recante regole tecniche), avente **carattere vincolante** e valenza ***erga omnes***. Con la conseguenza che esse sono pienamente azionabili davanti al giudice amministrativo in caso di violazione delle prescrizioni ivi contenute. Inoltre, nelle ipotesi in cui la violazione sia posta in essere da parte dei soggetti di cui all'art. 2, comma 2 del CAD, è altresì possibile presentare apposita segnalazione al difensore civico, ai sensi dell'art. 17 del CAD.

Le Linee guida, entrate in vigore dal giorno successivo alla pubblicazione, sono pienamente applicabili a partire dal **1° gennaio 2022**. A partire da tale data, quindi, esse sostituiscono e abrogano:

- il DPCM 13 novembre 2014, recante "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici";
- il DPCM 3 dicembre 2013, recante "Regole tecniche in materia di sistema di conservazione";
- il DPCM 3 dicembre 2013, recante "Regole tecniche per il protocollo informatico" (eccetto le disposizioni di cui ai seguenti articoli: 2, comma 1; 6; 9; 18, commi 1 e 5; 20; 21);
- la Circolare AgID n. 60 del 23 gennaio 2013 in materia di "Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni" (sostituita dall'allegato 6 "Comunicazione tra AOO di documenti amministrativi protocollati").

3. A - La gestione documentale

La gestione documentale è un processo che può essere suddiviso in tre fasi principali: formazione, gestione e conservazione. Nell'ambito di ognuna delle suddette fasi si svolgono una serie di attività che si distinguono per complessità, impatto, natura, finalità e/o effetto, anche giuridico, alle quali corrispondono approcci metodologici e prassi operative distinte.

Tale processo – che è essenziale per ogni struttura organizzata – tradizionalmente è stato realizzato basandosi sulla produzione e gestione di documentazione cartacea per la quale si sono venute definendo regole e prassi di gestione spesso inconsapevolmente applicate in modo più o meno corretto.

L'introduzione dei documenti informatici ha reso necessario ripensare alle modalità di gestione dei documenti, spesso condizionate da strumenti e regole disegnati per il cartaceo, per adeguarle a

questo nuovo scenario. Inoltre, con l'applicazione dell'informatica alla gestione documentale, quest'ultima ha acquisito una nuova centralità e maggiore visibilità all'interno delle organizzazioni, mettendone in luce la fondamentale rilevanza e le grandi potenzialità in termini di maggiore e più facile utilizzo delle risorse informative.

Negli ultimi quindici anni tale ritrovata centralità si è manifestata anche in una rinnovata attenzione normativa, sfociata nell'approvazione del D. Lgs. n. 82/2005 e dei suoi decreti attuativi che contengono le regole tecniche (in particolare, il DPCM 3 dicembre 2013[21]) e, da ultimo, nella pubblicazione delle citate Linee guida AgID del 10 settembre 2020. I provvedimenti normativi in questione impongono alle amministrazioni di abbandonare gli strumenti analogici tradizionalmente usati per la gestione dei processi di propria competenza in favore dell'uso degli strumenti informatici (documento informatico, firma digitale, fascicoli informatici, comunicazioni telematiche, ecc.). L'obbligatorietà dell'uso degli strumenti informatici, quindi, rende imprescindibile ricorrere a sistemi informatici di gestione documentale (c.d. "*software gestionali*").

Il CAD, nella sua formulazione previgente alle modifiche operate dal D. Lgs. n. 179/2016, conteneva la seguente definizione di "*gestione informatica dei documenti*": l'*"insieme delle attività finalizzate alla registrazione e segnatura di protocollo nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema d'archivio adottato, effettuate mediante sistemi informatici"* (art. 1, comma 1, lettera U)[22].

In questa definizione sono ricomprese tutte le attività tradizionali della gestione documentale, già definite e descritte dalla disciplina archivistica, ma declinate nell'applicazione a esse di sistemi di trattamento informatico. Il sistema di gestione documentale, quindi, non si esaurisce nel servizio di protocollo informatico ma comprende anche gli archivi dei documenti e dei fascicoli[23] (intesi come insieme dei documenti relativi al procedimento) oltre a tutti i registri in uso.

[21] Il testo delle Regole tecniche è disponibile al seguente link:
http://www.agid.gov.it/sites/default/files/repository_files/leggi_decreti_direttive/dpcm_3-12-2013_protocollo.pdf

[22] Tale definizione è stata abrogata dal D. Lgs. n. 179/2016, ma si ritiene possa comunque essere considerata valida ai fini della perimetrazione delle attività del sistema di gestione documentale.

[23] Per l'individuazione delle tipologie di fascicoli, si può ricorrere alle definizioni tradizionali di fascicolo archivistico:

- *fascicolo per procedimento:* comprende i documenti, recanti tutti la medesima classifica, prodotti da uno o più uffici per la trattazione di un procedimento. Ogni fascicolo si riferisce ad un procedimento amministrativo specifico e concreto e si chiude con la conclusione del procedimento stesso. Ha quindi una data di apertura, una durata circoscritta ed una data di chiusura.
- *fascicolo per affare*: comprende i documenti, recanti tutti la medesima classifica, prodotti da uno o più uffici per la trattazione di un affare. Ha le medesime caratteristiche del fascicolo per procedimento, ma essendo relativo ad un affare non si chiude mai con un atto finale, né con in tempi predeterminati.
- *fascicolo per attività*: comprende i documenti prodotti nello svolgimento di un'attività amministrativa semplice, non discrezionale e ripetitiva, che si esaurisce in risposte obbligate o meri adempimenti. La sua chiusura è periodica, tendenzialmente annuale, salvo diverse esigenze gestionali.
- *fascicolo nominativo* (per persona fisica o giuridica): comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona fisica o giuridica. Si tratta di fascicolo permanente, attivo fino quando è "attivo" il soggetto a cui è intestato.

Le norme, inoltre, prevedono che i sistemi di gestione documentale informatica, dal punto di vista tecnologico e organizzativo, debbano assicurare:

- la sicurezza e l'integrità del sistema;
- la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Il sistema di gestione informatica, peraltro, deve consentire:

- il reperimento delle informazioni riguardanti i documenti registrati;
- l'accesso, in condizioni di sicurezza, alle informazioni da parte dei soggetti interessati nel rispetto delle norme sulla tutela dei dati personali;
- il rapido reperimento delle informazioni riguardanti i fascicoli, il procedimento e il relativo responsabile;
- lo scambio di informazioni con sistemi per la gestione dei flussi documentali di altre amministrazioni/soggetti al fine di determinare lo stato e l'iter dei procedimenti complessi.

Ricapitolando, è possibile affermare che un sistema di gestione informatica dei documenti debba garantire:

- attendibilità del sistema e dei documenti nella fase di formazione, garantendo un'organizzazione stabile dei documenti, un controllo sulle responsabilità, certezza dei dati sulla formazione/acquisizione dei documenti;
- autenticità dei documenti gestiti, mantenendo l'integrità dei documenti e delle informazioni per l'accesso dei documenti nello spazio (trasmissione, assegnazione, reperimento) e nel tempo (conservazione);
- accessibilità nel tempo, mantenendo leggibili e comprensibili i documenti e il contesto di produzione degli stessi.

Un sistema informatico di gestione documentale, correttamente sviluppato e gestito, deve offrire, inoltre, avanzate funzionalità di ricerca e reperimento dei documenti e dei fascicoli, garantendo così un fondamentale supporto all'efficienza e alla trasparenza dell'attività dell'organizzazione.

Il Legislatore, oltre all'adeguata dotazione informatica, richiede a ciascuna organizzazione:

- di provvedere alla nomina di un Responsabile per la gestione documentale, e di un suo vicario, per casi di vacanza, assenza o impedimento del primo;
- di adottare il Manuale di gestione dei documenti informatici, su proposta del responsabile della gestione documentale.

Il Responsabile della Gestione Documentale

Tale soggetto esegue i seguenti compiti:

a) predispone lo schema del Manuale di gestione;

b) predispone il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza prevista dalla normativa vigente in materia di protezione dei dati.

In generale, inoltre, al Responsabile per la gestione documentale, spetta la vigilanza e il controllo sul rispetto da parte del personale delle prescrizioni di legge e di regolamento nonché delle istruzioni operative previste nel Manuale di gestione.

Il Responsabile può avvalersi dello strumento della delega nei confronti di altri soggetti; tale delega deve essere conferita con apposito atto all'interno del quale siano specificamente indicate le funzioni e attribuzioni di ciascun soggetto all'interno del servizio di gestione documentale.

Il Manuale della Gestione Documentale

Il Manuale della Gestione Documentale, invece, rappresenta un atto fondamentale che deve essere adottato dall'amministrazione e tenuto costantemente aggiornato.

Il Manuale di gestione deve descrivere il sistema di gestione, anche ai fini della conservazione dei documenti informatici, e fornire le istruzioni per il corretto funzionamento del servizio per la gestione dei flussi documentali e degli archivi.

In osservanza di quanto previsto nelle Linee Guida (par. 3.5), il Manuale di gestione, una volta redatto, deve essere adottato dall'ente con provvedimento formale e pubblicato sul proprio sito istituzionale in una parte chiaramente identificabile dell'area "Amministrazione trasparente".

In fase di redazione del Manuale devono essere riportati, in particolare:

1. relativamente agli **aspetti organizzativi**:

a) le modalità di utilizzo degli strumenti informatici per la formazione dei documenti informatici e per lo scambio degli stessi all'interno ed all'esterno dell'AOO, applicando le modalità di trasmissione conformi alle indicazioni contenute nell'allegato 6 alle Linee guida ("Comunicazione tra AOO di Documenti Amministrativi Protocollati");

b) l'indicazione delle unità organizzative responsabili (UOR) delle attività di registrazione di protocollo, di archiviazione dei documenti all'interno dell'AOO;

c) l'indicazione delle regole di assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso aree organizzative omogenee della stessa amministrazione o verso altre amministrazioni;

d) i criteri e le modalità per il rilascio delle abilitazioni di accesso, interno ed esterno all'Amministrazione, al sistema di gestione informatica dei documenti;

2. relativamente ai **formati** dei documenti:

a) l'individuazione dei formati utilizzati per la formazione del documento informatico tra quelli indicati nell'Allegato 2 alle Linee guida ("Formati di file e riversamento");

b) la descrizione di eventuali ulteriori formati utilizzati per la formazione di documenti in relazione a specifici contesti operativi che non sono individuati nell'Allegato;

c) le procedure per la valutazione periodica di interoperabilità dei formati e per le procedure di riversamento previste come indicato al paragrafo 3.7 delle Linee guida e nell'Allegato 2;

3. relativamente al **protocollo informatico** e alle registrazioni particolari:

a) le modalità di registrazione delle informazioni annullate o modificate nell'ambito delle attività di registrazione;

b) la descrizione completa e puntuale delle modalità di utilizzo della componente «sistema di protocollo informatico» del sistema di gestione informatica dei documenti;

c) le modalità di utilizzo del registro di emergenza, inclusa la funzione di recupero dei dati protocollati manualmente;

d) l'elenco dei documenti esclusi dalla registrazione di protocollo per cui è prevista registrazione particolare;

e) determinazione dei metadati da associare ai documenti soggetti a registrazione particolare individuati, assicurando almeno quelli obbligatori previsti per il documento informatico dall'Allegato 5 alle Linee guida;

f) i registri particolari individuati per la gestione del trattamento delle registrazioni particolari informatiche, gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti, riconosciuti da una norma;

4. relativamente alle **azioni di classificazione e selezione**:

a) il piano di classificazione adottato dall'Amministrazione, con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, con riferimento alle procedure di scarto;

5. relativamente alla **formazione delle aggregazioni documentali**:

a) le modalità di formazione, gestione e archiviazione dei fascicoli informatici e delle aggregazioni documentali informatiche con l'insieme minimo dei metadati ad essi associati;

6. relativamente ai **flussi di lavorazione dei documenti in uso**:

a) la descrizione dei flussi di lavorazione interni all'Amministrazione, anche mediante la rappresentazione formale dei processi attraverso l'uso dei linguaggi indicati da AgID, applicati per la gestione dei documenti ricevuti, inviati o ad uso interno;

7. relativamente alla organizzazione dei documenti informatici, dei fascicoli informatici e delle serie informatiche:

a) la definizione della struttura dell'archivio all'interno del sistema di gestione informatica dei documenti. L'archivio informatico - formato ai sensi del capo IV "Sistema di gestione informatica dei documenti" del DPR 445/2000 - deve essere progettato in modo da assicurare certezza e trasparenza all'attività giuridico amministrativa;

8. relativamente alle **misure di sicurezza e protezione dei dati personali** adottate:

a) le opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio anche in materia di protezione dei dati personali;

9. relativamente alla **conservazione**:

a) il piano di conservazione, da allegare al manuale di gestione documentale, con l'indicazione dei tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate.

All'interno del Manuale di gestione documentale, infine, devono essere disciplinate le modalità di trasmissione dei documenti tenendo conto del fatto che la normativa vigente contiene precise disposizioni che sanciscono modalità differenti a seconda della categoria di destinatari della comunicazione.

In particolare:

- comunicazioni con le altre pubbliche amministrazioni: l'art. 47 CAD prescrive tassativamente che tali comunicazioni debbano avvenire esclusivamente attraverso la cooperazione applicativa, la posta elettronica o la posta elettronica certificata (senza possibilità di ricorrere a modalità analogiche), pena la responsabilità dirigenziale, disciplinare ed erariale. Le PA e i gestori di pubblici servizi devono pubblicare nell'Indice dei domicili digitali almeno una casella di posta elettronica per protocollo;
- comunicazioni con professionisti e imprese: l'art. 5-*bis* CAD (attuato dal DPCM 22 luglio 2011) e art. 6-*bis*, comma 2, CAD prevedono che tali comunicazioni debbano avvenire in modalità esclusivamente telematica (PEC), pena l'impossibilità di produrre effetti per i destinatari. La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando gli strumenti telematici di trasmissione. In particolare, per le comunicazioni e le notifiche destinati alle imprese e ai professionisti, le amministrazioni utilizzano esclusivamente i recapiti di posta elettronica certificata presenti nel pubblico elenco di INI-PEC[24], che a seguito della recente modifica apportata dal D.L. n. 76/2020 (c.d. Decreto "Semplificazioni"), conterrà anche i domicilii digitali dei professionisti iscritti in elenchi o registri detenuti dalle pubbliche amministrazioni e istituiti con legge dello Stato, oltre a quelli dei professionisti iscritti presso gli ordini o i collegi professionali;
- comunicazioni con le persone fisiche: nel caso in cui l'utente abbia un domicilio digitale, ai sensi degli artt. 3-*bis*, 6 *quater*, 6 *quinquies* del CAD, tale indirizzo dovrebbe essere

[24] https://www.inipec.gov.it

prioritariamente utilizzato. Tanto anche alla luce della recente istituzione dell'Indice nazionale dei domicili digitali delle persone fisiche (INAD) di cui all'art. 6-***quater*** CAD (che diventerà operativo a breve) che è destinato a contenere i recapiti telematici che le amministrazioni saranno tenute ad utilizzare nei rapporti con le persone fisiche. Peraltro, alla luce delle recenti modifiche apportate dal citato D.L. n. 76/2020, l'INAD conterrà anche i domicili digitali professionali dei professionisti non presenti in INI-PEC poiché non iscritti presso ordini professionali, albi o elenchi detenuti da pubbliche amministrazioni. Da ultimo, si segnala che l'AgID ha adottato e pubblicato le Linee Guida in cui sono stabilite le modalità di realizzazione e gestione operativa dell'INAD[25].

Si aggiunge che, ai sensi dell'art. 3-***bis***, l'utente ha facoltà di eleggere domicilio speciale anche su posta elettronica ordinaria ma, in questo caso, non può eccepire la mancata ricezione da parte dell'amministrazione. Inoltre, con le recenti disposizioni introdotte dal D.L. n. 76/2020 (c.d. Decreto "Semplificazioni"), sono state disciplinate in via generale le modalità di funzionamento della ***Piattaforma per la notificazione digitale degli atti della pubblica amministrazione***, di cui le pubbliche amministrazioni e i soggetti incaricati delle attività di riscossione dei tributi (quest'ultimi solo limitatamente a tale attività) potranno avvalersi ai fini della notifica a persone fisiche di atti, provvedimenti, comunicazioni e avvisi. Tramite la piattaforma l'atto o la comunicazione oggetto di notificazione potrà essere messo a disposizione del destinatario, cui sarà trasmesso un avviso mediante posta elettronica certificata o altro servizio elettronico di recapito certificato qualificato, con l'indicazione delle modalità per prendere visione del documento. Ai destinatari privi di domicilio digitale, invece, il gestore della piattaforma trasmetterà l'avviso in via analogica con l'indicazione delle modalità per identificarsi e accedere ***online*** o, in alternativa, ritirare il documento oggetto di notifica in formato cartaceo.
Affinché la piattaforma diventi operativa, tuttavia, si dovrà attendere la disciplina di dettaglio che sarà definita con futuro decreto attuativo della Presidenza del Consiglio dei Ministri.

Gestione documentale del Consiglio regionale della Sardegna – Stato dell'arte e adempimenti

Dopo aver illustrato il quadro normativo in materia di gestione documentale, si indicano le principali priorità da affrontare nell'ottica di assicurare un pieno adempimento degli obblighi innanzi citati.

È stata correttamente individuata un'unica AOO del Consiglio regionale.

Con decreto del Segretario Generale n. 3/2022 è stato nominato il Responsabile per la gestione documentale dell'Amministrazione consiliare. Non è stato adottato, invece, il Manuale di gestione documentale dell'ente.

Con riguardo al sistema di protocollo informatico, è in fase di avvio il passaggio all'utilizzo del software J-Iride.

[25] Le Linee guida sull'INAD sono reperibili al seguente url: https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/212581610420O_OLinee+guida+INAD+art.+6-quater+CAD.pdf

Secondo quanto rappresentato, l'amministrazione non provvede alla fascicolazione informatica dei documenti, ma tale attività è in fase di implementazione.

Secondo quanto rappresentato, l'ente comunica telematicamente con le altre pubbliche amministrazioni, mentre le comunicazioni con le imprese, i professionisti e i cittadini muniti di domicilio digitale non sempre avvengono tramite tale modalità.

Alla luce dello stato dell'arte descritto, si rilevano i principali ambiti di intervento futuro:

- si ricorda, innanzitutto, che – laddove non si fosse già proceduto in tal senso – deve essere nominato il Vicario del Responsabile della gestione documentale, nonché devono essere individuati i soggetti delegati alle attività di protocollazione;
- si ricorda, inoltre, che il Responsabile per la gestione documentale – anche in vista dell'adeguamento alle Linee Guida AgID, che sono divenute pienamente efficaci dal 1° gennaio 2022 – deve provvedere alla redazione ed al costante aggiornamento del Manuale di gestione documentale. A tal fine, è auspicabile che il Responsabile sia coadiuvato da un gruppo di lavoro dotato di competenze informatiche, giuridiche e archivistiche. Una volta predisposto, il Manuale deve essere approvato con delibera dell'Ufficio di Presidenza, organo competente all'adozione degli atti di organizzazione dell'Amministrazione consiliare (cfr art. 131 del Regolamento interno). Si ricorda altresì che il Manuale e i relativi allegati, oltre a essere comunicati a tutti i dipendenti interessati, dovranno essere pubblicati sul sito istituzionale dell'Amministrazione nella Sezione "*Amministrazione Trasparente*", preferibilmente nella sottosezione "*Atti generali*";
- si ricorda che è compito del Responsabile verificare la conformità delle piattaforme in uso alle nuove Linee Guida AgID e valutare gli interventi evolutivi, specialmente con riferimento all'informatizzazione dei flussi documentali interni; inoltre, bisognerà progressivamente prevedere che tutte le comunicazioni interne siano gestite in modalità informatica (possibilmente nell'ambito di una procedura di *workflow* associata a ciascun procedimento). Alla medesima conclusione si può pervenire per tutte le comunicazioni relative alla gestione del personale;
- bisognerà provvedere alla formazione dei fascicoli informatici, secondo il piano di fascicolazione definito dall'ente;
- andranno pianificati gli interventi per adeguare progressivamente il sistema di gestione dei documenti al modello di interoperabilità definito dall'Agenzia per l'Italia Digitale ai sensi del Piano triennale per l'informatica;
- con riferimento ai flussi documentali verso l'esterno, inoltre, bisognerà assicurare il rispetto delle norme in materia di domicilio digitale e valutare eventuali interventi evolutivi (es. integrazione anagrafiche con il domicilio digitale, possibilità di acquisizione in cooperazione applicativa dei domicili digitali presenti nelle banche dati di cui agli Indici PEC di cui agli artt. 6-*bis*, 6-*ter* e 6-*quater* CAD). Inoltre, si ricorda di assicurarsi che tutte le comunicazioni con i soggetti dotati di un domicilio digitale avvengano esclusivamente in

via telematica. Non ci si riferisce solo alle comunicazioni con le altre amministrazioni, ma anche con imprese e professionisti, nonché con i cittadini che ne sono provvisti.

3. B - La formazione dei documenti informatici e dei fascicoli informatici

Il Codice dell'amministrazione digitale, all'art. 40, rubricato "*Formazione di documenti informatici*", introduce un fondamentale precetto: "*Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71*". La norma richiamata stabilisce un preciso obbligo: i documenti dei soggetti che rientrano nell'ambito di applicazione del CAD devono essere prodotti esclusivamente in modalità informatica.

La dematerializzazione dei flussi documentali non rappresenta, dunque, solo un'opportunità o un percorso volto al raggiungimento di livelli di maggior efficienza, efficacia, trasparenza, semplificazione e partecipazione, ma un preciso e improrogabile precetto normativo.

Ciò che contraddistingue il documento informatico è la sua forma elettronica (rappresentazione informatica) che – per avere valore giuridico e probatorio – deve essere conforme alle disposizioni contenute agli artt. 20 e ss. CAD e alle relative regole tecniche, ossia le citate Linee guida AgID sul documento informatico.

La formazione del documento informatico è regolata dal Capitolo 2 delle Linee guida AgID.

Il momento di formazione dei documenti informatici è fondamentale poiché solo una corretta formazione del documento è in grado di garantirne un'efficace gestione e una valida conservazione a lungo termine. In ambito digitale, infatti, la conservazione dei documenti informatici non può essere considerata un'attività *ex-post* ma deve necessariamente costituire una componente irrinunciabile della fase di formazione dei documenti stessi. Nella fase di formazione dei documenti si dovranno adottare, pertanto, tutti gli accorgimenti e gli strumenti opportuni per la loro corretta produzione, anche in ragione delle diverse tipologie documentali, della loro differente natura e contenuto o della loro destinazione. Dovrà essere garantita l'integrità, immodificabilità, identificazione, classificazione, fascicolazione, leggibilità, memorizzazione e conservazione dei documenti in conformità alle norme e alle regole tecniche che presidiano la corretta tenuta e gestione degli stessi. Dal punto di vista giuridico, il rispetto della norma è importante perché – in difetto – l'amministrazione non sarà in grado di assicurare l'efficacia e la validità dei propri documenti.

In particolare, com'è noto, il documento amministrativo è ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa. Il documento informatico viene definito dal CAD come "*il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*" (art. 1, comma 1, lett. p)).

In tema di validità ed efficacia probatoria dei documenti informatici, il D. Lgs. n. 217 del 2017 ha introdotto l'importante comma 1 *bis* all'interno dell'art. 20 del CAD.

Tale norma dispone che: "*Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una* firma *digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID, ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida".*

Il Codice fissa, altresì, per quali atti è richiesta la firma elettronica qualificata o firma digitale, pena nullità (art. 21, comma 2 *bis*).

Per quanto riguarda le richiamate regole tecniche, le Linee Guida AgID dettano le regole per la formazione e conservazione dei documenti informatici delle pubbliche amministrazioni che si applicano anche ai soggetti cui è eventualmente affidata la gestione o la conservazione dei documenti informatici.

Ai sensi del capitolo 2.1.1. delle Linee Guida, il documento informatico può essere formato mediante una delle seguenti quattro modalità: creazione, acquisizione, memorizzazione informatica di informazioni o dati e generazione o raggruppamento di un insieme di dati o registrazioni.

Si tratta, come ampiamente esposto, di una fase fondamentale del ciclo di vita del documento, poiché è in questo momento che vanno adottati una serie di accorgimenti in vista della futura conservazione.

a) Creazione

La creazione del documento informatico mediante la sua redazione tramite l'utilizzo di appositi strumenti *software* (o servizi *cloud* qualificati[26]) rappresenta la principale modalità di produzione di documenti informatici; si tratta della più tradizionale modalità di formazione di un documento che interviene utilizzando applicazioni di *office automation* deputate, il più delle volte, alla redazione di documenti contenenti testo. Una volta memorizzato nel suo formato originale di produzione, il documento informatico potrà essere consolidato in una o più versioni, sino ad arrivare alla sua versione definitiva, ossia la versione che non subirà alcuna ulteriore modifica di contenuto da parte del suo autore. Solo dopo questa fase, il documento assumerà anche una forma definitiva o meglio un formato definitivo in grado di rendere immodificabile il suo contenuto e, ove necessario, predisposto per una eventuale sottoscrizione digitale. Immodificabilità e staticità sono, quindi, due caratteristiche essenziali che devono essere obbligatoriamente garantite.

Secondo quanto previsto dalle Linee guida AgID, inoltre, affinché un documento sia conforme alla normativa deve essere creato nel rispetto delle regole di interoperabilità dei formati indicate nell'Allegato 2. In particolare, l'Allegato 2, al par. 2, indica un **elenco di formati** idonei a garantire

[26] Sul tema della qualificazione dei servizi *cloud* si veda *infra*, cap. 6.C.

l'interoperabilità, mentre al par. 3 prevede che l'utilizzo di formati diversi da quelli elencati, o il discostamento dalle regole relative a uno specifico formato, debba essere preceduto da una **valutazione di interoperabilità**, che l'ente è tenuto a redigere con cadenza annuale.

A seconda del tipo di documento, poi, si renderà necessaria la sottoscrizione elettronica (di norma, in caso di provvedimenti che impegnano l'organizzazione all'esterno, dovrà procedersi con lo strumento della firma digitale).

b) Acquisizione

Con questa modalità il documento è formato mediante acquisizione:

- di un documento informatico per via telematica o su supporto informatico;
- della copia per immagine su supporto informatico di un documento analogico;
- della copia informatica di un documento analogico.

c) Memorizzazione informatica di informazioni o dati

Fra le diverse modalità di formazione dei documenti informatici vi è anche quella di cui alla lett. c) del par. 2.1.1. delle Linee guida, che si realizza attraverso la "*memorizzazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente*".

Le istanze, le dichiarazioni e le comunicazioni, se pervenute all'organizzazione per mezzo di moduli o formulari (ad esempio *form* compilati sul sito *Web*), devono poter essere identificate e trattate nel sistema di gestione informatica dei documenti come i documenti informatici ovvero, se soggette a norme specifiche che prevedono la sola tenuta di estratti per riassunto, memorizzate in specifici archivi informatici dettagliatamente descritti nel Manuale di gestione.

d) Generazione o raggruppamento di un insieme di dati o registrazioni

Il documento informatico, infine, può essere prodotto tramite la generazione o il raggruppamento, anche in via automatica, di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica (Linee guida AgID, par. 2.1.1., lett. d).

Tale modalità fa espresso riferimento all'interoperabilità e alla c.d. "*cooperazione applicativa*", vale a dire ai documenti informatici formati mediante acquisizione di dati e informazioni dai sistemi informatici di altri soggetti pubblici.

Il documento informatico, formato con una delle modalità sopra esposte, dovrà essere identificato in modo univoco e persistente e dovrà essere memorizzato in un sistema di gestione informatica dei documenti.

Le Linee guida, poi, precisano quali sono le metodologie – specifiche per ciascuna modalità di formazione del documento – da applicare per rendere un documento informatico **immodificabile**, condizione che si può ritenere realizzata quando la memorizzazione del documento su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.

Al momento della formazione del documento informatico immodificabile, inoltre, devono essere generati e associati permanentemente ad esso i relativi **metadati**.

I metadati sono un insieme di dati (informazioni) associati a un determinato documento informatico o a un fascicolo informatico o a un'aggregazione documentale informatica che hanno il fine di identificarlo e descriverne: contesto, contenuto e struttura, nonché di permetterne la gestione nel tempo nel sistema di conservazione.

L'insieme dei **metadati obbligatori** del documento informatico è definito nell'Allegato 5 alle Linee guida, che indica altresì i metadati obbligatori da associare al documento amministrativo informatico e alle aggregazioni documentali informatiche (fascicoli, serie, etc.).

Nel Manuale di gestione possono essere individuati ulteriori metadati da associare a particolari tipologie di documenti informatici o di aggregazioni. In ogni caso nel Manuale di gestione devono essere riportati i metadati definiti per ogni tipologia di documento.

L'obbligo di formazione degli originali informatici contenuto all'art. 40, comma 1 CAD è norma generale che si applica a tutti i "documenti" (ivi compresi gli albi, i registri e gli elenchi dell'amministrazione). In base ad altre norme settoriali, vigenti già da tempo, l'ente ha l'obbligo giuridico di formare come documenti informatici – sottoscritti digitalmente – i contratti per lavori, servizi e forniture (a partire dal 1° gennaio 2015) nonché gli accordi con altre pubbliche amministrazioni, stipulati ai sensi dell'art. 15 Legge n. 241/1990 (a partire dal 30 giugno 2014).

La stipula di tali accordi deve avvenire in modalità informatica a pena di nullità, prevista espressamente dalla normativa vigente. Naturalmente, dato che questi documenti vengono formati (e quindi devono essere fascicolati e conservati) in modalità informatica, è necessario che vengano anche repertoriati e gestiti con le medesime modalità (ad esempio prevedendo il pagamento dell'imposta di bollo in modalità virtuale).

Per quanto riguarda i fascicoli informatici, questi, ai sensi dell'art. 41 del CAD, devono recare una serie di informazioni: a) l'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo; b) le altre amministrazioni partecipanti; c) il responsabile del procedimento; d) l'oggetto del procedimento; e) l'elenco dei documenti contenuti, salvo quanto disposto dal comma 2-*quater*; e-*bis*) l'identificativo del fascicolo medesimo. L'allegato 5 alle Linee guida, inoltre, indica anche i metadati obbligatori per le aggregazioni documentali, tra cui i fascicoli informatici.

Per espressa previsione del citato art. 41, il fascicolo informatico può contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati. Il fascicolo è formato, però, in modo tale da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti. Il fascicolo informatico, inoltre, è costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla legge n. 241 del 1990 e dall'articolo 5, comma 2, del decreto legislativo 14 marzo 2013, n. 33, nonché l'immediata

conoscibilità, anche attraverso i servizi di cui agli articoli 40-*ter* e 64-*bis*, sempre per via telematica, dello stato di avanzamento del procedimento, del nominativo e del recapito elettronico del responsabile del procedimento.

Formazione dei documenti informatici da parte del Consiglio regionale della Sardegna – Stato dell'arte e adempimenti

Dopo aver illustrato il quadro normativo in materia di formazione dei documenti informatici, si indicano le principali criticità da affrontare nell'ottica di assicurare un pieno adempimento degli obblighi innanzi citati.

In base a quanto rappresentato, presso la Vostra Amministrazione non tutti i documenti sono formati in originale con mezzi informatici. Inoltre, i documenti che richiedono la sottoscrizione non sempre sono firmati digitalmente.

Secondo quanto rappresentato, inoltre, l'amministrazione provvede alla formazione di documenti accessibili alle persone con disabilità.

Si rendono necessari, quindi, i seguenti rilievi:

- come esposto, occorrerà procedere all'adozione del Manuale di gestione documentale (di cui al precedente punto 3.A), che disponga sulla digitalizzazione di tutti gli originali formati dall'Amministrazione consiliare, indicando le modalità di redazione tramite *software* (almeno gli indirizzi generali) e sottoscrizione digitale dei documenti, nel rispetto della normativa vigente, al fine di garantirne l'efficacia giuridico-probatoria. In particolare, si dovranno dare precise disposizioni circa i seguenti elementi:
    - formati (con osservanza delle indicazioni contenute nell'Allegato 2 alle Linee guida AgID);
    - la descrizione di eventuali ulteriori formati utilizzati per la formazione di documenti in relazione a specifici contesti operativi che non sono individuati nell'Allegato 2 e le relative procedure di valutazione periodica di interoperabilità;
    - *font* (è preferibile che ne sia adottato uno unico e *standard* per tutti i documenti, individuato tra i font interoperabili indicati nell'allegato 2 alle Linee guida);
    - accessibilità, con indicazioni sulla formazione dei documenti nel rispetto della Legge n. 4/2004 e dei relativi provvedimenti attuativi. A tale proposito, si consiglia la consultazione della "*Guida pratica per la creazione di un documento accessibile*" elaborata dall'AgID, anche al fine di rendere accessibili le copie informatiche di originali analogici[27];

[27] Link: https://www.agid.gov.it/sites/default/files/repository_files/linee_guida/guida_pratica_creazione_word_accessibile_2.pdf.

- metadati (obbligatori e facoltativi), aggiornati in conformità all'allegato 5 delle Linee guida;
- tipologia di firma con cui sottoscrivere il documento (ad es. Cades, Pades, Xades);
- gestione degli eventuali allegati al documento principale;

- in futuro, dopo aver provveduto alle attività sopraelencate, si potrebbe procedere all'acquisito di certificati di firma digitale automatica. Si ricorda, a tale proposito, che, in effetti, la firma digitale automatica risulta utile per sottoscrivere documenti informatici dello stesso genere: l'utente, infatti, può specificare le tipologie di documenti informatici per i quali automatizzare l'applicazione della firma, senza che il PIN sia richiesto per ogni sottoscrizione del singolo documento informatico. Il firmatario non ha l'onere di presenziare durante l'operazione e gli vengono notificati l'apposizione della firma con sistemi automatici e i certificati di notifica. L'art. 35 del D. Lgs. n. 82/2005 rubricato "*Dispositivi sicuri e procedure per la generazione della firma qualificata*", al comma 3, dispone che la firma con procedura automatica è valida se apposta previo consenso del titolare all'adozione della "*procedura medesima*". Si rileva che in questa, come nelle altre norme, non si parla mai di "atti" ma di "procedure". D'altra parte, l'art. 5 del dpcm 22 febbraio del 2013 (Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali), ai commi 2 e 3 recita: "*2. Se il soggetto appone la sua firma elettronica qualificata o firma digitale per mezzo di una procedura automatica ai sensi dell'art. 35, comma 3 del Codice, deve utilizzare una coppia di chiavi destinata a tale scopo, diversa da tutte le altre in suo possesso. L'utilizzo di tale procedura deve essere indicato esplicitamente nel certificato qualificato. 3. Se la procedura automatica di cui al comma 2 fa uso di un insieme di dispositivi sicuri per la generazione della firma elettronica qualificata o firma digitale del medesimo soggetto, deve essere utilizzata una coppia di chiavi diversa per ciascun dispositivo utilizzato dalla procedura automatica*";
- bisognerà assicurarsi che tutti i soggetti che sottoscrivono documenti siano dotati di dispositivi di firma elettronica e che li utilizzino per la sottoscrizione;
- bisognerà prevedere che i documenti sottoscritti digitalmente siano versati in conservazione possibilmente prima della scadenza del certificato di firma digitale con cui sono sottoscritti, per conservarne l'integrità;
- ferma restando la necessità di formare in modalità digitale gli originali, le comunicazioni potranno essere trasmesse in via cartacea solo nel caso in cui non sia possibile utilizzare un recapito telematico (ad es. per gli individui sprovvisti di domicilio digitale).

3.C - La conservazione dei documenti informatici

Come esposto, la conservazione rappresenta un'attività indispensabile per tutti quei documenti che nascono come informatici. I soggetti tenuti all'applicazione del CAD, infatti, devono, per obbligo di

legge, preservare digitalmente i propri documenti informatici di cui sia prescritta la conservazione nel tempo.

L'art. 42 del CAD prevede che le pubbliche amministrazioni valutino in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedano alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche[28].

La produzione di documenti informatici, pertanto, implica anche la loro conservazione in modalità informatica e pone in evidenza la necessità di far evolvere la tradizionale funzione conservativa dei documenti in modalità idonee a conservare i documenti informatici con sistemi informatici. La conservazione costituisce un fattore fondamentale per la sostenibilità del processo di dematerializzazione, a garanzia che documenti e informazioni in formato digitale siano conservati nel lungo periodo, in modo autentico e accessibile, come avviene per i documenti cartacei. Se non ci fosse la garanzia che i documenti digitali prodotti possono essere conservati e resi accessibili nel lungo termine, infatti, non sarebbe ipotizzabile una reale diffusione del processo di dematerializzazione.

La conservazione dei documenti e dei fascicoli informatici è, dunque, l'attività volta a proteggere e mantenere, cioè custodire nel tempo, gli archivi di documenti e dati informatici. Il tempo di conservazione può essere permanente, cioè indefinito nel futuro, o, come spesso avviene, indicato a lungo termine, cioè un arco temporale sufficientemente ampio da essere interessato da cambiamenti tecnologici. Il suo obiettivo primario è di impedire la perdita o la distruzione non autorizzata dei documenti e di mantenere nel tempo le loro caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità.

Per riassumere, in breve, si può dire che:

- autenticità: è la caratteristica di un documento informatico che fornisce la garanzia che il documento sia ciò che dichiara di essere, senza avere subito alterazioni o modifiche. Insieme di identità (identificazione e provenienza) e integrità;
- integrità: è la qualità di un documento di essere completo e inalterato, cioè non avere subito modifiche non autorizzate;
- affidabilità: esprime il livello di fiducia che l'utente, cioè colui che legge il documento, ripone, o può riporre, nel documento informatico, in particolare nella sua visualizzazione leggibile allo stesso;
- leggibilità: è la caratteristica che definisce il mantenimento della fruibilità delle informazioni contenute nel documento durante l'intero ciclo di gestione dei documenti, cioè al momento della sua formazione o produzione, nelle sue forme di diffusione, nella sua memorizzazione e archiviazione e nella sua conservazione; in certi casi si può

[28] Le regole tecniche in materia di conservazione dei documenti informatici, in attesa del 1° gennaio 2022, data in cui diverranno pienamente applicabili le richiamate Linee Guida AgID, attualmente sono contenute nel DPCM 3 dicembre 2013, disponibile al seguente link: http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/dpcm_3-12-2013_conservazione.pdf

distinguere tra leggibilità da parte di sistemi informatici o leggibilità da parte di un essere umano;

- reperibilità: esprime la capacità di reperire ed esibire il documento con le caratteristiche sopra riportate.

Il problema conservativo non era risolvibile con il solo mantenimento dell'immodificabilità dei singoli documenti ma doveva allargarsi al mantenimento delle aggregazioni documentali e delle informazioni di contesto di produzione dei documenti. Tale consapevolezza ha trovato la sua prima definizione nell'art. 44 del CAD che è stato di recente modificato dal summenzionato Correttivo al CAD e che ha introdotto il concetto di "*sistema di conservazione*" dei documenti informatici definendolo come il sistema che deve assicurare autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti.

Il sistema di conservazione, inoltre, deve essere opportunamente collegato con il sistema di gestione dei documenti informatici (descritto nella Sezione 3. A del presente documento), definendo tutti i più opportuni accorgimenti per il versamento di documenti e aggregazioni. Com'è noto, infatti, il processo di conservazione si basa su una logica di conservazione caratterizzata dal versamento da parte dei produttori degli oggetti da conservare (documenti informatici e aggregazioni documentali informatiche) su due fasi:

1) versamento in archivio: si tratta del versamento nel sistema di conservazione dei pacchetti che contengono le aggregazioni documentali informatiche nella loro forma stabile e definitiva; secondo la dottrina archivistica, è attività assimilabile al versamento dall'archivio corrente all'archivio di deposito;
2) versamento anticipato: si tratta, di norma, del versamento di singoli documenti informatici che possono trovarsi ancora nella fase attiva del loro ciclo di vita. Tale versamento – che avviene in un momento il più possibile prossimo a quello di effettiva produzione del documento - ha la finalità di mettere in sicurezza l'oggetto, ponendo in essere le misure necessarie alla sua conservazione a lungo termine.

In proposito, vale la pena rilevare che – per tutti quei casi in cui la normativa vigente non preveda già l'obbligo di versamento entro determinate scadenze (come nel caso della documentazione fiscale e contabile o del registro giornaliero di protocollo) – la nuova versione dell'art. 44, comma 1-*bis* CAD (così come novellata da. D. Lgs. n. 179/2016) prevede che "*almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi*".

I principali adempimenti in materia di gestione documentale possono esser così definiti:

a) dotarsi di un sistema di conservazione dei documenti informatici che rispetti i requisiti previsti dalle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici;
b) nominare il Responsabile della conservazione documentale;

c) adottare il Manuale di conservazione, da parte del Responsabile della conservazione documentale.

Il sistema di conservazione dei documenti informatici

La conservazione può essere realizzata all'interno della struttura organizzativa propria che produce i documenti informatici da conservare (modello interno) ovvero affidandola (modello esterno), in tutto o in parte, ai sensi dell'art. 34, comma 1-*bis*, lett. b), a soggetti pubblici e privati presenti nell'elenco dei conservatori tenuto dall'AgID che offrono idonee garanzie organizzative e tecnologiche e di protezione dei dati personali.

Il Responsabile della Conservazione Documentale

Dal punto di vista organizzativo, inoltre, è necessario nominare formalmente un Responsabile della conservazione documentale.

Come previsto al par. 4.5 delle Linee guida AgID, il Responsabile della conservazione:

a) è un ruolo previsto dall'organigramma dell'amministrazione;

b) è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche ed archivistiche;

c) può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato.

I compiti specifici attribuiti al Responsabile della conservazione sono puntualmente indicati al citato par. 4.5. delle Linee guida e si possono sintetizzare come segue:

- gestione, monitoraggio e verifica periodica della conformità normativa e del corretto funzionamento del sistema di conservazione;
- cura del processo di conservazione e, in particolare, generazione e sottoscrizione degli oggetti della conservazione e successivo versamento al sistema di conservazione;
- redazione e costante aggiornamento del Manuale della conservazione.

Come precisano le Linee Guida AgID, nel caso in cui il servizio di conservazione venga affidato ad un conservatore, i compiti del Responsabile della conservazione – ad esclusione della redazione e dell'aggiornamento del manuale – possono essere affidati, anche solo in parte, al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sul servizi affidati in outsourcing dalle PA. I compiti eventualmente affidati al responsabile del servizio di conservazione, nonché il nome del Responsabile interno all'amministrazione, dovranno risultare nel contratto o nella convenzione con cui si affida il servizio al conservatore.

Il Responsabile della conservazione, inoltre, può delegare, sotto la propria responsabilità, lo svolgimento delle proprie attività o parte di esse a uno o più soggetti interni all'amministrazione che abbiano specifiche competenze ed esperienze. Tale delega, riportata nel manuale di conservazione, deve individuare le specifiche funzioni e competenze delegate.

Il Manuale della conservazione

Il manuale della conservazione è il documento di riferimento in cui vengono descritte in modo dettagliato fasi di lavoro, strumenti e responsabilità che caratterizzano tutta l'attività di conservazione.

Lo scopo del manuale è quello di condividere il metodo tra produttore e conservatore e renderlo noto anche a chi ne abbia interesse.

Le Linee guida AgID sulla formazione, gestione e conservazione del documento informatico, al par. 4.6 precisano che il Manuale deve, innanzitutto, illustrare dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Inoltre, il manuale di conservazione deve:

a) mantenere traccia dei soggetti che hanno assunto, nel tempo, la responsabilità del sistema di conservazione;

b) descrivere la struttura organizzativa, in cui sono chiari funzioni responsabilità e obblighi di chi interviene nel processo di conservazione sia nel ruolo di produttore che di conservatore;

c) descrivere gli oggetti che vengono conservati in termini di:

   - tipologia: registro di protocollo giornaliero, determinazioni di spesa, fattura elettronica[..];
   - formato: indicare in quale formato vengono conservati i documenti per singola tipologia: *pdf*, *jpg*, *xml* e altri. In proposito, è bene tener presenti le indicazioni contenute nell'allegato 2 alle Linee guida AgID;
   - metadati: elencare cioè le informazioni che ne caratterizzano l'identificazione certa. Tali informazioni (metadati) sono organizzate in file *xml*, associate ai documenti e ai fascicoli informatici, e devono includere tutti i metadati previsti come obbligatori dall'allegato 5 alle Linee guida AgID, a seconda della tipologia di oggetto di conservazione;

d) descrivere il metodo di versamento in conservazione da parte del produttore, che, si ricorda, deve avvenire per gruppi di documenti - c.d. pacchetti – e che deve terminare con un rapporto di esito emesso dal conservatore;

e) descrivere il processo di conservazione e il trattamento dei documenti nel sistema di conservazione; in tale sezione del manuale è necessario descrivere almeno quanto previsto dal par. 4.7 delle Linee guida AgID, ossia:

- l'acquisizione da parte del sistema di conservazione del pacchetto di versamento (PdV) per la sua presa in carico;
- la verifica che il PdV e gli oggetti digitali contenuti siano coerenti con le modalità previste dal manuale di conservazione e con quanto indicato nell'allegato 2 "Formati di file e riversamento" delle Linee guida AgID;
- il rifiuto del PdV, nel caso in cui le verifiche di cui al punto precedente abbiano evidenziato delle anomalie. Il numero massimo di rifiuti è stabilito nell'ambito di un contratto o convenzione;
- la generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione;
- la sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica qualificata o avanzata apposta dal responsabile della conservazione o dal responsabile del servizio di conservazione, ove prevista nel manuale di conservazione;
- la preparazione, la sottoscrizione con firma digitale o firma elettronica qualificata o avanzata del responsabile della conservazione o dal responsabile del servizio di conservazione con il sigillo elettronico qualificato o avanzato del titolare dell'oggetto di conservazione o del conservatore e la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati indicate dallo standard UNI 11386:2010 e secondo le modalità riportate nel manuale di conservazione;
- la preparazione e la sottoscrizione con firma digitale o firma elettronica qualificata o avanzata del responsabile della conservazione o del responsabile del servizio di conservazione, oppure l'apposizione del sigillo elettronico qualificato o avanzato, secondo le modalità indicate nel manuale di conservazione, del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente;
- ai fini della interoperabilità tra sistemi di conservazione, i pacchetti di distribuzione possono contenere parte, uno o più i pacchetti di archiviazione;
- la produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli utenti in conformità a quanto previsto dalle Linee Guida AgID;
- la produzione di copie informatiche tramite attività di riversamento al fine di adeguare il formato alle esigenze conservative di leggibilità nel tempo in base alle indicazioni previste dall'allegato 2 alle Linee Guida AgID ("Formati di file e riversamento");
- l'eventuale scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma o secondo quanto indicato

dal piano di conservazione del Titolare dell'oggetto di conservazione e le procedure descritte nelle Linee Guida AgID;

- nel caso degli archivi pubblici o privati, che rivestono interesse storico particolarmente importante, l'eventuale scarto del pacchetto di archiviazione avviene previa autorizzazione del MIBACT rilasciata al Titolare dell'oggetto della conservazione secondo quanto previsto dalla normativa vigente in materia e dalle Linee Guida AgID;

f) descrivere il processo di esibizione e la relativa produzione del pacchetto di distribuzione, quando cioè il produttore richiede al conservatore di recuperare ed esibire un documento precedentemente affidatogli per la conservazione;

g) descrivere il sistema di conservazione negli aspetti prettamente tecnici: quali sono le componenti tecnologiche, fisiche e logiche utilizzate, quali le misure di sicurezza e come le stesse vengono gestite ed evolute nel tempo;

h) descrivere come viene svolto il monitoraggio sul corretto funzionamento del sistema di conservazione e sull'integrità dei documenti conservati. In questo ambito va evidenziato il comportamento che andrebbe ad adottarsi in caso anomalie;

i) descrivere le procedure per la produzione di duplicati e copie;

j) riportare, per tipologia, i tempi entro i quali i documenti debbano essere proposti allo scarto oppure avviati in conservazione facendo riferimento in tal senso al proprio manuale di gestione documentale;

k) indicare i procedimenti ed i casi in cui interviene il pubblico ufficiale;

l) indicare le normative in vigore nei luoghi in cui vengono conservati i documenti.

Si specifica che l'utente deve poter consultare quanto versato in conservazione.

Si precisa, inoltre, che in ossequio alle Linee guida AgID le amministrazioni sono tenute a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di conservazione. La pubblicazione deve essere effettuata in una parte chiaramente identificabile dell'area "Amministrazione trasparente" del sito istituzionale dell'ente.

Conservazione documentale del Consiglio regionale della Sardegna – Stato dell'arte e adempimenti

Dopo aver illustrato il quadro normativo in materia di conservazione documentale, si indicano le principali criticità da affrontare nell'ottica di assicurare un pieno adempimento degli obblighi innanzi citati.

In base a quanto emerge dalle risposte al questionario somministratoVi, la Vostra Amministrazione ha provveduto parzialmente agli adempimenti in materia di conservazione documentale.

Con decreto del Segretario Generale n. 4/2022 è stato nominato il Responsabile per la conservazione dei documenti informatici dell'Amministrazione consiliare. Secondo quanto rappresentato, però, non è stato adottato il Manuale di conservazione dei documenti informatici dell'amministrazione.

Il Consiglio ha delegato la conservazione al conservatore Maggioli S.p.A.

In base a quanto da Voi rappresentato, ad oggi l'ente non provvede a conservare digitalmente i propri atti, sebbene tale attività sia in fase di implementazione.

Di conseguenza, parallelamente alla redazione del Manuale di Gestione di cui al punto 3.A, si raccomanda di:

- adottare il Manuale di conservazione dei documenti informatici. Si ricorda che nell'ambito di tale documento, che deve essere personalizzato per l'amministrazione, devono essere specificate le modalità di formazione dei pacchetti di versamento (e quindi i rapporti con il sistema di gestione documentale) e di distribuzione (e quindi le modalità di ricerca dei documenti da parte del personale in servizio). In alternativa all'adozione del Manuale di conservazione, è possibile inserire all'interno del Manuale di gestione, nella sezione relativa alle modalità di conservazione dei documenti informatici, le disposizioni relative alla conservazione dei documenti, anche eventualmente facendo rinvio al manuale del conservatore. In ogni caso, come previsto dalle Linee guida (cfr. par. 4.6), nel Manuale dell'amministrazione devono essere individuati (in modo che siano pubblicati) i tempi di versamento, le tipologie documentali trattate, i metadati, le modalità di trasmissione dei pacchetti di versamento e le tempistiche di selezione e scarto dei propri documenti informatici;
- assicurarsi che sia previsto il versamento almeno annuale di tutti i documenti, anche a fascicolo aperto, secondo le indicazioni che dovrebbero essere riportate nel Piano di conservazione adottato dall'amministrazione;
- assicurarsi che siano conservati digitalmente non soltanto i documenti formati in originale digitale, ma anche – quando possibile – le copie digitali dei documenti originali analogici di cui è richiesta la conservazione nel tempo.

4. L'EROGAZIONE DI SERVIZI *ONLINE* A FAVORE DI CITTADINI ED IMPRESE

La sezione II (artt. 3-9) del Capo I del Codice dell'amministrazione digitale dal titolo "*Carta della cittadinanza digitale*" elenca una serie di diritti digitali che sono riconosciuti ai cittadini e alle imprese, specificando, all'articolo 3, che chiunque ha il diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti previsti dal Codice nei rapporti con i soggetti di cui all'articolo 2, comma 2 dello stesso.

Oltre quindi a sancire il generale diritto all'uso delle tecnologie dell'utenza nei rapporti con la pubblica amministrazione, il Codice prevede una serie di nuovi diritti digitali.

Con riferimento a tre particolari profili, al diritto dell'utenza corrisponde evidentemente un obbligo dell'amministrazione di implementare i relativi servizi *online*.

Si tratta, in particolare, di:

a) L'identificazione degli utenti;

b) l'accessibilità ai servizi mediante l'app IO;

c) I pagamenti elettronici;

Per completare il quadro in materia di servizi, poi, ci si soffermerà su:

d) la connettività alla rete internet negli uffici e luoghi pubblici;

a) L'identificazione degli utenti

Al fine di evitare il moltiplicarsi di differenti sistemi di autenticazione, il Legislatore ha istituito il Sistema pubblico di identità digitale (c.d. "SPID"), definito come il sistema di autenticazione che permette a cittadini e imprese di accedere ai servizi *online* della pubblica amministrazione e dei privati aderenti con un'identità digitale unica. L'identità SPID è costituita da credenziali (nome utente e *password*) che vengono rilasciate all'utente e che permettono l'accesso a tutti i servizi *online* delle pubbliche amministrazioni e dei soggetti privati che intendono aderire.

Qualora richiedano identificazione, tutte le organizzazioni pubbliche devono rendere i propri servizi *online* accessibili tramite SPID in modo da favorire e semplificare l'utilizzo dei servizi digitali da parte di tutti i cittadini (la scadenza dell'adempimento era fissata al 31 marzo 2018).

Per adeguare i sistemi informativi alle regole tecniche e alle regole di *design* dedicate a SPID, è necessario completare due procedure: una tecnica e l'altra amministrativa (che si conclude con la stipula di una convenzione con l'Agenzia per l'Italia Digitale)[29].

Con particolare riferimento a SPID, poi, è fondamentale ricordare anche che esso non è soltanto una modalità di autenticazione informatica che assicura l'identificazione dell'utente, ma che l'utilizzo di questo strumento viene espressamente equiparato ad una forma di sottoscrizione ai fini dell'inoltro di domande a una amministrazione. In proposito, infatti, l'art. 65 CAD, nella formulazione attualmente vigente quale risulta a seguito delle modifiche introdotte dal D.L. n. 76/2020 prevede che le istanze e le dichiarazioni presentate per via telematica alle pubbliche amministrazioni e ai gestori dei servizi pubblici ai sensi dell'articolo 38, commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sono valide:

"a) se sottoscritte mediante una delle forme di cui all'articolo 20;

b) ovvero, quando l'istante o il dichiarante è identificato attraverso il sistema pubblico di identità digitale (SPID), la carta di identità elettronica o la carta nazionale dei servizi;

[29] Le procedure per l'adesione dei soggetti pubblici e privati a SPID sono descritte dettagliatamente sul sito dedicato https://www.spid.gov.it/

b-bis) ovvero formate tramite il punto di accesso telematico per i dispositivi mobili di cui all'articolo 64-bis (4);

c) ovvero sono sottoscritte e presentate unitamente alla copia del documento d'identità.

c-bis) ovvero se trasmesse dall'istante o dal dichiarante dal proprio domicilio digitale iscritto in uno degli elenchi di cui all'articolo 6-bis, 6-ter o 6-quater ovvero, in assenza di un domicilio digitale iscritto, da un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento eIDAS. In tale ultimo caso, di assenza di un domicilio digitale iscritto, la trasmissione costituisce elezione di domicilio digitale ai sensi e per gli effetti dell'articolo 3-bis, comma 1-ter. Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario".

La norma specifica che siffatte istanze e dichiarazioni sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento.

A quanto fin qui evidenziato, si aggiunge che il D. Lgs. n. 217/2017, correttivo al CAD, ha introdotto una nuova fattispecie di formazione del documento informatico nell'ambito dell'articolo 20, comma 1-*bis*, D. Lgs. n. 82/2005.

Infatti, come già esposto nell'ambito della sezione dedicata alla gestione documentale, la disposizione citata prevede che: "*1-bis. Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida".*

Le Linee guida in questione sono state adottate dall'Agenzia per l'Italia Digitale in data 23 marzo 2020[30]. A seguito dell'adozione delle Linee Guida dell'AgID l'identificazione con SPID è diventata, a tutti gli effetti, un'ulteriore modalità di sottoscrizione elettronica, a patto che le amministrazioni (nella loro qualità di service provider) si adeguino alle modalità tecniche di implementazione dei servizi definite dal provvedimento AgID.

Deve essere sottolineato, però, che il Codice, all'art. 66, comma 3, prevede che anche la carta d'identità elettronica (CIE)[31] e la carta nazionale dei servizi (CNS) possano essere utilizzate quali strumenti di autenticazione telematica per l'effettuazione di pagamenti tra soggetti privati e

[30] Le Linee guida per la sottoscrizione elettronica dei documenti ai sensi dell'art. 20 CAD sono disponibili al seguente link: https://trasparenza.agid.gov.it/archivio28_provvedimenti-amministrativi_0_122208_725_1.html

[31] Il portale istituzionale dedicato alla Carta d'identità elettronica (CIE) è disponibile al seguente indirizzo: https://www.cartaidentita.interno.gov.it.

pubbliche amministrazioni. Le modalità tecniche[32] di emissione della CIE, da parte dei Comuni, sono state definite con decreto dal Ministero dell'Interno. Sempre con riferimento alla CIE, si segnala che, dal 6 aprile 2020, con l'obiettivo di agevolare l'accesso da casa a numerosi servizi pubblici, è stata rilasciata dal Ministero dell'Interno e dall'Istituto Poligrafico e Zecca dello Stato la nuova modalità di identificazione ai servizi *online* attraverso la CIE (Carta d'Identità Elettronica 3.0): l'utente può identificarsi tramite "Entra con CIE", senza dovere più utilizzare un dispositivo di lettura contactless collegato al computer, ma attraverso il proprio smartphone con l'applicazione "CIE ID".

Infine, in tema di sistemi di identificazione degli utenti, si deve segnalare che, in seguito alla recente modifica dell'art. 64, commi 2-quater e 2-quinquies, del CAD per opera del D.L. n. 76/2020 (c.d. Decreto "Semplificazioni"), le modalità di identificazione SPID e CIE sono state pienamente equiparate, essendo stato previsto che gli utenti, per accedere ai servizi *online* delle amministrazioni pubbliche, hanno diritto ad autenticarsi – oltre che con SPID – anche tramite CIE. Pertanto, le amministrazioni sono tenute a garantire anche tale ulteriore modalità di identificazione, per l'accesso a tutti i servizi *online*.

Lo stesso Decreto "Semplificazioni" è intervenuto altresì sull'art. 64 del CAD, individuando il **28 febbraio 2021** come termine ultimo per lo *switch off* delle modalità di autenticazione diverse da SPID e CIE. A partire da tale data, dunque, è fatto divieto alle amministrazioni di rilasciare o rinnovare credenziali per l'identificazione e l'accesso dei cittadini ai propri servizi in rete diverse da SPID, CIE o CNS, fermo restando l'utilizzo di quelle già rilasciate fino alla loro naturale scadenza e, comunque, non oltre il **30 settembre 2021**.
Sempre con riguardo alle modifiche al citato art. 64, occorre segnalare l'introduzione del comma 2-*duodecies*, ai sensi del quale il riconoscimento dell'utente tramite identità digitale (con livello di garanzia almeno significativo ai sensi dell'articolo 8, paragrafo 2, del Regolamento (UE) n. 910/2014) ha lo stesso effetto dell'esibizione di un documento di riconoscimento. La stessa norma prevede che l'invio di istanze, comunicazioni e documenti mediante un indirizzo PEC iscritto nei registri INI-PEC, IPA o INAD è considerato equivalente a identificazione del mittente e che, inoltre, costituisce elezione di domicilio digitale ai sensi dell'art. 3-*bis*, comma 1-*ter* del CAD.

b) l'accessibilità ai servizi mediante l'app IO

L'art. 64-*bis* del CAD, al comma 1, ha previsto l'attivazione di un "*punto di accesso telematico*" presso la Presidenza del Consiglio dei Ministri, attraverso cui le pubbliche amministrazioni sono tenute a rendere fruibili i propri servizi in rete.

A tale fine, il successivo comma 1-*bis* (nella formulazione risultante a seguito delle modifiche di cui al D.L. n. 76/2020 – c.d. Decreto "Semplificazioni") prevede che i soggetti coinvolti nella *governance* digitale (pubbliche amministrazioni, concessionari di pubblici servizi, società a controllo pubblico e prestatori di servizi fiduciari qualificati) "*progettano e sviluppano i propri sistemi e servizi in modo da garantire l'integrazione e l'interoperabilità tra i diversi sistemi e servizi e con il servizio di cui ai*

[32] Il testo del Decreto del Ministero dell'Interno del 23 dicembre 2015 recante le modalità tecniche di emissione della Carta d'identità elettronica sono disponibili al seguente indirizzo: https://www.gazzettaufficiale.it/eli/id/2015/12/30/15A09809/sg

commi 1 e 1-ter, espongono per ogni servizio le relative interfacce applicative e, al fine di consentire la verifica del rispetto degli standard e livelli di qualità di cui all'articolo 7, comma 1, adottano gli strumenti di analisi individuati dall'AgID con le Linee guida".

Gli obblighi previsti dalle norme citate sono posti al fine di consentire la concreta attuazione del diritto degli utenti, sancito dall'art. 7, comma 01 del CAD, di fruire dei servizi digitali "*anche attraverso dispositivi mobili*".

In attuazione delle norme citate, dunque, è stata sviluppata e resa disponibile agli utenti "*IO*", l'applicazione dei servizi pubblici che consentirà a tutti gli enti comunicare con i propri utenti attraverso un unico canale, integrato con i sistemi di identificazione SPID e CIE, permettendo così l'erogazione dei servizi *online* tramite dispositivi mobili.

IO è un canale che qualsiasi ente pubblico può utilizzare per inviare comunicazioni ai propri utenti: fornire aggiornamenti, ricordare scadenze o richiedere pagamenti relativi a un determinato servizio.

Dopo un primo periodo di sperimentazione presso alcuni enti, l'applicazione è attualmente disponibile sugli *store* e liberamente scaricabile da tutti i cittadini.

Il Team per la trasformazione digitale istituito presso la Presidenza del Consiglio dei Ministri ha pubblicato una guida rivolta agli enti pubblici per accompagnarli nel processo di integrazione dei propri servizi sulla piattaforma IO[33]. Il processo si articola in quattro passaggi:

1. identificare quali servizi possono essere erogati tramite IO;
2. predisporre l'integrazione tecnologica attraverso il *back office* messo a disposizione all'url: https://developers.italia.it/it/io/.
3. sottoscrivere l'accordo di adesione ad IO e definire le modalità di gestione di sicurezza e privacy;
4. comunicare ai cittadini la presenza dei servizi sulla piattaforma IO.

Da ultimo si segnala che il D.L. n. 76/2020 ha novellato l'art. 64-*bis* del CAD, prevedendo che le amministrazioni devono consentire l'accesso telematico ai servizi mediante applicazione mobile IO, che diviene l'unico sistema mobile di accesso ai servizi della PA. È stato previsto, inoltre, che le PA devono avviare i progetti di trasformazione digitale entro il **28 febbraio 2021** (art. 64, comma 1-*quater*), fatti salvi impedimenti di natura tecnologica (art. 64, comma 1-*ter*). Lo stesso Decreto, poi, introducendo la lettera b-*bis*) all'art. 65, comma 1 del CAD, ha previsto che mediante l'app IO sarà possibile, inoltre, formare istanze, dichiarazioni e autocertificazioni. Lo stesso decreto, inoltre, ha introdotto modifiche all'art. 8 della Legge n. 241/1990, prevedendo che la comunicazione di avvio del procedimento deve indicare le modalità di accesso tramite l'app IO o altre modalità telematiche per accedere al fascicolo informatico del procedimento.

[33] La guida del Team per la trasformazione digitale è disponibile al seguente link: https://medium.com/team-per-la-trasformazione-digitale/progetto-io-guida-per-gli-enti-pubblici-integrazione-servizi-pubblica-amministrazione-smartphone-cittadini-f290306a611a

c) I pagamenti elettronici

L'art. 5 del CAD prevede che i soggetti di cui all'articolo 2, comma 2, sono obbligati ad accettare i pagamenti spettanti a qualsiasi titolo attraverso sistemi di pagamento elettronico, ivi inclusi, per i micro-pagamenti, quelli basati sull'uso del credito telefonico.

Con riferimento alle modalità, oltre ad accettare anche eventuali altre forme di pagamento, tutti i soggetti pubblici devono consentire che tali pagamenti avvengano attraverso la piattaforma abilitante denominata pagoPA nel rispetto delle Linee Guida definite dall'Agenzia per l'Italia Digitale[34]. Come precisato nelle Linee Guida dell'AgID (cfr. punto 5, "Strumenti di pagamento"), infatti, per effettuare i pagamenti elettronici possono essere utilizzati tutti gli strumenti di pagamento messi a disposizione dai Prestatori di Servizi di Pagamento (PSP), purché siano connessi con la piattaforma pagoPA (bonifico, bollettino postale, carte di credito o di debito e ogni altro servizio di pagamento integrato con la piattaforma). Fanno eccezione i metodi di pagamento con modello F24, Sepa Direct Debit (SDD), nonché altri eventuali servizi di pagamento non ancora integrati e che non risultino sostituibili con quelli integrati con pagoPA perché specifica disposizione di legge ne prevede la messa a disposizione all'utente.

Si segnala che la scadenza per l'adesione al sistema pagoPA[35] e il relativo piano di implementazione, nonché l'obbligo per i prestatori di servizi di pagamento abilitati di utilizzare esclusivamente la piattaforma pagoPA per i pagamenti verso le pubbliche amministrazioni, che in precedenza era stato differito al 30 giugno 2020 dal D.L. n. 162/2019, oggi è stato ulteriormente differito al 28 febbraio 2021 a seguito delle modifiche all'art. 65 del d. lgs. 217/2017 previste dal D.L. n. 76/2020 (c.d. Decreto "Semplificazioni"). In proposito si segnala inoltre che, per effetto di quest'ultima disposizione – già modificata dall'art. 8, co. 4 del d.l n. 135 del 2018 – è stato stabilito che le amministrazioni sono tenute, entro la medesima data, a integrare i loro sistemi di incasso con la piattaforma pagoPA, ovvero ad avvalersi, a tal fine, di servizi forniti da altri soggetti già abilitati. Il mancato adempimento di tale obbligo rileva ai fini della misurazione e della valutazione della performance individuale dei dirigenti responsabili e comporta responsabilità dirigenziale e disciplinare ai sensi degli articoli 21 e 55 del d. lgs. n. 165/2001.

Infine, con riguardo ai comuni si deve segnalare l'**art. 24-bis** del **D.L. "Semplificazioni"**, introdotto in sede di conversione in legge, il quale dispone che i comuni devono assicurare l'interoperabilità degli strumenti di pagamento elettronico dei titoli di viaggio all'interno dei rispettivi territori e a tal fine hanno facoltà di sottoscrivere, anche per il tramite delle aziende di trasporto locali, appositi accordi o convenzioni con soggetti privati al fine di realizzare specifiche piattaforme digitali. La relativa normativa di dettaglio sarà adottata, entro sei mesi dall'entrata in vigore della legge di conversione, con decreto del Ministro delle infrastrutture e dei trasporti adottato d'intesa con la Conferenza unificata e sentita la Conferenza Stato-città ed autonomie locali.

[34] Le Linee Guida per i pagamenti informatici e la descrizione della Piattaforma PagoPA sono consultabili al seguente link: https://www.agid.gov.it/sites/default/files/repository_files/lineeguidapagamenti_v_1.2.pdf.

[35] Le procedure per l'adesione a PagoPA e la relativa modulistica sono pubblicate alla url: https://www.pagopa.gov.it/it/pubbliche-amministrazioni/come-aderire/

d) connettività alla rete internet negli uffici e luoghi pubblici

Sempre in tema di servizi, infine, va ricordato che, in attuazione dell'art. 8-*bis* del CAD, ai sensi del quale le amministrazioni favorisco la disponibilità di connettività alla rete internet presso gli uffici pubblici e altri luoghi pubblici, è necessario uniformare e aumentare la diffusione della connettività wireless nei luoghi pubblici e negli uffici della Pubblica Amministrazione accessibili al pubblico. In tal senso, l'AgID ha adottato le linee guida per l'erogazione del servizio pubblico *wi-fi free* (ancora in via di pubblicazione definitiva).

Servizi *online* – Stato dell'arte e adempimenti del Consiglio regionale della Sardegna

Dopo aver illustrato il quadro normativo in materia servizi in rete, si ritiene che gli adempimenti da curare siano i seguenti:

a) secondo quanto da Voi rappresentato, il Consiglio ha provveduto all'implementazione delle piattaforme abilitanti SPID e CIE e consente l'accesso ai servizi online che richiedono l'identificazione dell'utente mediante i suddetti strumenti di autenticazione. Secondo quanto rappresentato, inoltre, l'Amministrazione consiliare consente agli utenti di sottoscrivere le istanze presentate telematicamente con la firma SPID. La Vostra amministrazione, dunque, deve assicurarsi che tutti i servizi siano fruibili in modalità telematica e accessibili mediante SPID e CIE e valutare la possibilità di erogare online ulteriori servizi oltre a quelli già resi disponibili;

b) la Vostra amministrazione deve procedere ad aderire a IO, seguendo i passaggi sopra indicati, considerato anche l'obbligo di avviare i relativi progetti di trasformazione digitale entro il 28 febbraio 2021 (cfr. disposizioni del Decreto "Semplificazioni" 2020). Si raccomanda, inoltre, di consentire progressivamente agli utenti la possibilità di accedere tramite l'app IO a tutti i servizi online erogati dall'ente che risultino compatibili con tale modalità di erogazione;

c) secondo quanto rappresentato, il Consiglio ha provveduto all'implementazione di pagoPA e consente di utilizzare la piattaforma con riferimento ad alcuni pagamenti; si raccomanda, quindi, di rendere effettiva la possibilità di utilizzare la piattaforma con riferimento a tutti i pagamenti, considerato che la scadenza per tale adempimento era fissata per il 28 febbraio 2021;

d) con riferimento alla connettività, secondo quanto da Voi rappresentato, il Consiglio non rende disponibile il servizio *wi-fi* gratuito al personale, ai consiglieri e ai dipendenti dei Gruppi. Si raccomanda di consentire la disponibilità di connettività in conformità a quanto disposto dalle *Linee guida per l'erogazione del wi-fi free pubblico* (ancora non pubblicate in versione definitiva) e, per quanto possibile, di garantire l'accesso al *wi-fi* anche agli utenti esterni;

e) con riguardo al sito *web* del Consiglio, si raccomanda di adeguare i contenuti alla normativa, come di recente modificata e alle linee guida sul tema emanate dall'AgID ai sensi dell'art. 71 CAD[36];

f) il Consiglio, secondo quanto da Voi rappresentato, ha sviluppato il sito istituzionale in osservanza delle prescrizioni della l. n. 4 del 2004, ma non ha provveduto alla sottomissione ad AgID della relativa Dichiarazione di accessibilità. Con riferimento all'obbligo di garantire l'accessibilità agli strumenti informatici di cui alla legge n. 4 del 2004, si è già detto *supra* (cfr. Sez. 2, lett. c) dell'approvazione delle Linee guida AgID sull'accessibilità degli strumenti informatici e, in particolare, delle modalità di verifica dell'accessibilità dei siti web e delle applicazioni mobili. Per tali strumenti informatici si ricorda che la Dichiarazione di accessibilità deve essere rilasciata e pubblicata in conformità alle prescrizioni delle Linee guida e dell'allegato I, assicurandone poi l'aggiornamento annuale. Con riferimento, poi, all'accessibilità dei documenti pubblicati sul sito, si ricorda che i documenti sono accessibili nella misura in cui gli stessi vengono redatti come documenti informatici nel rispetto delle regole tecniche attuative della Legge n. 4/2004

g) il Consiglio, in base a quanto rappresentato, non rileva telematicamente il giudizio degli utenti. Come specificato nelle *Linee guida di design per i servizi della PA*[37], la rilevazione "immediata, continua e sicura" del giudizio degli utenti, richiesta dall'art. 63, co. 2 del CAD, si realizza mediante un'adeguata progettazione dei servizi in rete. Pertanto, si invita a tenere presenti le indicazioni ivi contenute. Si ricorda, inoltre, che i dati relativi alla verifica di soddisfazione degli utenti devono comprendere le statistiche di utilizzo dei servizi. Si rileva infine che, secondo quanto previsto nel Piano Triennale 2021-2023, per il monitoraggio dei propri siti *web* le PA possono utilizzare *Web Analytics Italia*[38], una piattaforma nazionale *open source* che offre rilevazioni statistiche su indicatori utili al miglioramento continuo dell'esperienza utente.

5. SICUREZZA INFORMATICA E PRIVACY

5. A - Sicurezza informatica

La sicurezza informatica riveste un ruolo fondamentale per le amministrazioni in quanto garantisce la disponibilità, l'integrità e la riservatezza delle informazioni. Essa è inoltre direttamente collegata ai principi di *privacy* previsti dall'ordinamento giuridico.

Per quanto concerne la sicurezza, una delle attività principali del Responsabile per la transizione digitale è rappresentata dall'adeguamento alle misure minime contenute alla Circolare AgID n.

[36] Link: https://www.agid.gov.it/sites/default/files/repository_files/design-italia.pdf
[37] Link: https://www.agid.gov.it/sites/default/files/repository_files/design-italia.pdf
[38] La piattaforma è accessibile al seguente link: https://webanalytics.italia.it/

2/2017[39] alla quale le pubbliche amministrazioni erano tenute a dare puntuale attuazione entro il 31 dicembre 2017.

Le Misure, che si articolano nell'attuazione di controlli di natura tecnologica, organizzativa e procedurale, prevedono tre livelli di attuazione. Il livello minimo è quello al quale ogni organizzazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme. I livelli successivi rappresentano situazioni evolutive in grado di fornire livelli di protezione più completi e dovrebbero essere adottati fin da subito dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visti come obiettivi di miglioramento da parte di tutte le altre organizzazioni.

Come parte del processo di adeguamento, il Responsabile per la transizione al digitale deve, inoltre, compilare, firmare digitalmente e marcare temporalmente il "Modulo di implementazione" allegato alla Circolare[40] per poi inviarlo in conservazione.

Le misure di sicurezza indicate nel modello di implementazione vanno costantemente aggiornate e coordinate con la modulistica adottata dall'amministrazione ai sensi della normativa in materia di protezione dei dati personali (come il Registro delle attività di trattamento di cui all'art. 30, par. 2, Reg. UE 2016/679).

Si rileva, altresì, che, nonostante l'avvenuta abrogazione per opera del Correttivo dell'art. 50 bis CAD relativo alla continuità operativa, l'attuale art. 51, all'art. 2 quater recita: "*I soggetti di cui articolo 2, comma 2, predispongono, nel rispetto delle Linee guida adottate dall'AgID, piani di emergenza in grado di assicurare la continuità operativa delle operazioni indispensabili per i servizi erogati e il ritorno alla normale operatività*".

Va segnalato, da ultimo, come il Piano triennale per l'informatica nella PA 2020 – 2022 attribuisca un ruolo rilevante anche alle attività di monitoraggio e controllo. In particolare, il Piano prevede che le amministrazioni siano tenute monitorare e segnalare prontamente al CSIRT[41] gli incidenti informatici e ogni situazione di potenziale rischio, utilizzando i canali di comunicazione messi a disposizione dall'AgID.

Si segnala anche che, nell'ottica di diffondere la cultura del rischio cyber all'interno della PA e di rendere progressivamente autonomo ciascun ente nell'analisi e nella valutazione dei rischi ai quali è esposto, AgID ha predisposto un ***tool* di *cyber risk management***[42], che consente alle amministrazioni di effettuare operazioni di self assessment, predisporre gli opportuni piani di trattamento e mantenere il monitoraggio delle iniziative intraprese ai fini della riduzione del rischio informatico**.**

[39] Il testo integrale della Circolare e dei relativi allegati è disponibile al seguente link: http://www.gazzettaufficiale.it/eli/id/2017/05/05/17A03060/sg

[40] Il modello di implementazione in formato editabile è disponibile al seguente indirizzo Web: https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

[41] Il sito web del CSIRT è disponibile all'indirizzo: https://csirt.gov.it

[42] https://www.sicurezzait.gov.it/cyber/

Con particolare riferimento all'acquisizione di beni e servizi informatici, si devono segnalare alcuni provvedimenti a cui le amministrazioni sono tenute a conformarsi per finalità di sicurezza informatica. Si tratta in particolare delle:

• *Linee guida AgID per lo sviluppo del software sicuro*[43], composte di quattro allegati tecnici tematici (sviluppo software, sviluppo codice, adeguamento software di base, modellazione delle minaccie e individuazione delle azioni di mitigazione), il cui scopo è quello di fornire alle amministrazioni le *best practices* da seguire in sede di sviluppo che di adeguamento del software di base;

• *Linee guida AgID sulla sicurezza nel procurement ICT*[44], contenenti indicazioni tecnico-amministrative per garantire, nell'ambito delle procedure per l'approvvigionamento di beni e servizi informatici delle pubbliche amministrazioni, la rispondenza di questi ad adeguati livelli di sicurezza.

Da ultimo occorre segnalare che, con la recente adozione del D.L. 16 luglio 2020, n. 76 è stato introdotto nel CAD l'art. 13-*bis*, con cui si prevede che il Capo dipartimento della struttura della Presidenza del Consiglio dei ministri competente per la trasformazione digitale, entro sessanta giorni dall'entrata in vigore del Decreto, adotta il *codice di condotta tecnologica*, a cui tutte le amministrazioni dovranno conformarsi e con cui saranno disciplinate le modalità di progettazione, sviluppo e implementazione dei progetti, sistemi e servizi digitali, nel rispetto del principio di non discriminazione, dei diritti e delle libertà fondamentali delle persone e della disciplina in materia di perimetro nazionale di sicurezza cibernetica.

A fine di progettare, realizzare e sviluppare i sistemi informativi e i servizi digitali nel rispetto del codice di condotta tecnologica, il comma 2 del nuovo art. 13-*bis* prevede che le amministrazioni potranno avvalersi, singolarmente o in forma associata, di uno o più esperti in possesso di comprovata esperienza e qualificazione professionale nello sviluppo e nella gestione di processi complessi di trasformazione tecnologica e progetti di trasformazione digitale.

Nel codice di condotta tecnologica saranno indicate anche le principali attività, ivi compresa la formazione del personale, che il RTD dovrà svolgere in collaborazione con gli esperti, nonché il limite massimo di durata dell'incarico, i requisiti di esperienza e qualificazione professionale e il trattamento economico massimo da riconoscere agli esperti.

La norma prevede, inoltre, che le amministrazioni sono tenute a consentire lo *smart working* assicurando un adeguato livello di sicurezza informatica, in linea con le migliori pratiche e gli standard nazionali ed internazionali per la protezione delle proprie reti e a promuovere presso i dipendenti la consapevolezza sull'uso sicuro dei suddetti sistemi informativi, anche attraverso la diffusione di apposite linee guida, con cui disciplinare anche la tipologia di attività che possono essere svolte.

[43] Le Linee guida per lo sviluppo del software sicuro sono reperibili al seguente link: https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro

[44] Le Linee guida per lo sviluppo del software sicuro sono reperibili al seguente link: https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/2013910214200__OLG_Sicurezza_Procurement_ICT_versione_finale_pub.pdf

5.B - Privacy

Nell'ambito della trasformazione digitale di una pubblica amministrazione non possono essere evitate alcune brevi considerazioni in tema di *privacy*. In particolare, ci si soffermerà in questa sede, sugli elementi essenziali per valutare la conformità di un ente alla normativa in materia di dati personali.

Punto di riferimento per svolgere correttamente un'analisi sul tema è certamente il nuovo Regolamento (UE) n. 2016/679 con il quale il Legislatore europeo ha voluto uniformare e armonizzare la normativa europea relativa alla protezione dei dati personali.

Tale intervento si è inserito all'interno di un più ampio disegno d'azione volto a ridefinire gli strumenti posti a tutela dei dati personali, alla luce dell'incremento dell'utilizzo di strumenti automatizzati per il trattamento di dati personali e della diffusione di banche dati e archivi elettronici per la conservazione dei dati.

Il Regolamento, entrato in vigore nel giugno 2016, è definitivamente applicabile a decorrere dal 25 maggio 2018 ed ha avuto un impatto significativo sulla normativa nazionale e sull'organizzazione dei soggetti ai quali è imposto un adeguamento allo stesso.

È opportuno sottolineare che il Regolamento è lo strumento normativo dell'Unione Europea che non necessita di alcun intervento di recepimento da parte dei legislatori nazionali, ma è direttamente applicabile in ciascuno Stato Membro e vincola tutti i soggetti giuridici (pubblici e privati).

Occorre menzionare, inoltre, la normativa contenuta nel D.lgs. n. 196/2003, recante "Codice *privacy*", nonché alcuni provvedimenti di c.d. "*soft law*" come, ad esempio, i provvedimenti del Garante per la protezione dei dati italiano e le linee guida adottate dai Garanti europei riuniti nel *Working Party* 29 c.d. "WP29 (oggi EDPB, *European Data Protection Board*).

Si specifica, inoltre, che il Legislatore nazionale è intervenuto da ultimo con l'adozione del decreto legislativo 10 agosto 2018, n. 101, entrato in vigore il 19 settembre 2018, con l'obiettivo di adeguare il quadro normativo italiano alle disposizioni del Regolamento UE 2016/679.

Può essere utile, anzitutto, riportare alcune definizioni contenute nell'art. 4 del suddetto Regolamento al fine di precisare in modo chiaro le indicazioni fornite nel prosieguo.

In particolare:

- "**dato personale**": è qualsiasi informazione riguardante una persona fisica identificata o identificabile («**interessato**»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero d'identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- "**trattamento**": è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione,

diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- "**profilazione**": è qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- "**pseudonimizzazione**": è il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- "**archivio**": è qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- "**titolare del trattamento**": è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- "**responsabile del trattamento**": è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- "**consenso dell'interessato**": è qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

È opportuno soffermarsi, in particolare, sulla suddetta nozione di "*dato personale*" poiché la precisazione risulta utile per definire il perimetro dell'approfondimento.

È fondamentale specificare che le problematiche *privacy* riguardano solo quelle informazioni che possano essere qualificate come dati personali (in quanto riferiti a una persona fisica, secondo la definizione dell'art. 4 GDPR) e non anche dati che invece siano riferibili a una determinata persona giuridica.

È altresì opportuno ribadire che il diritto alla protezione dei dati personali è un diritto fondamentale dell'individuo, tutelato da norme nazionali e internazionali. Il diritto si sostanzia nell'autodeterminazione informativa, ossia in una serie di poteri conoscitivi e di controllo di ciascun individuo.

Da un punto di vista sostanziale, è possibile affermare che - rispetto alla normativa interna tutt'ora vigente - il Regolamento manifesta un irrobustimento dei diritti degli interessati e configura una

serie di doveri in capo ai titolari del trattamento secondo una logica fondata sull'analisi del rischio e sul principio della responsabilizzazione ("*accountability*").

Il Regolamento prevede una serie di nuovi adempimenti a cui è tenuto il Titolare del trattamento, adempimenti che non erano previsti dalla disciplina precedente: come, ad esempio, la valutazione d'impatto *privacy* (artt. 35-36), la minimizzazione dei trattamenti secondo i criteri di privacy *by design* e *by default* (art. 25), l'adozione del registro dei trattamenti (artt. 35-36) e la nomina del Responsabile per la Protezione dei dati Personali (c.d. "DPO") (artt. 37-39).

Il trattamento di dati personali, per essere conforme alla nuova disciplina normativa, deve innanzitutto svolgersi nel rispetto dei principi fondamentali previsti dall'art. 5 che sono il principale strumento di verifica di idoneità del trattamento.

A tale riguardo, il trattamento è lecito quando è conforme alla legge e corretto quando avviene in modo tale da rispettare la volontà di tutela della legge, ossia senza artifici, raggiri o pressioni indebite nell'acquisizione dei dati. I dati devono essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo conforme a queste finalità che devono esser rese note all'interessato. Devono inoltre essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono stati raccolti, in una logica generale di minimizzazione dei dati trattati. A ciò si aggiunge il principio di esattezza dei dati che richiede un'attenta verifica sia in sede di raccolta, che in seguito, ed è strettamente legato all'identità personale dell'interessato e alla sua rappresentazione esteriore.

Inoltre, i dati devono essere conservati per il tempo necessario a realizzare le finalità per i quali sono stati raccolti, in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati.

Il trattamento deve, inoltre, garantire adeguati livelli di integrità e sicurezza dei dati che rappresentano anch'essi principi cardine del trattamento.

In una logica di gestione del rischio e responsabilizzazione dei titolari del trattamento, il Regolamento prevede, come sopra accennato, il nuovo principio dell'*accountability*. In virtù di tale principio, il titolare è chiamato a implementare misure in grado di proteggere efficacemente i dati personali fin dal momento della progettazione di processi e modelli di trattamento, garantendo il principio di necessità nel corso dell'esecuzione dei trattamenti, con riferimento alla quantità di dati trattati, ai tempi di conservazione e ai livelli di accessibilità. I principali strumenti di responsabilizzazione sono sintetizzati nell'approccio *privacy by design* e *by default*, nella nomina del Responsabile per la Protezione dei dati Personali e nell'adozione del Registro dei trattamenti.

Inoltre, il Regolamento impone al titolare di comunicare in modo chiaro e trasparente all'interessato i diritti che gli spettano.

In particolare, i diritti conoscitivi dell'interessato includono:

- il diritto ad avere l'informativa per ogni trattamento svolto (artt. 13 e 14): tale documento deve includere le informazioni sull'identità e i dati di contatto del titolare e del responsabile, sulle finalità del trattamento, sugli eventuali destinatari a cui sono comunicati i dati e se il

Titolare del Trattamento sia intenzionato a comunicare tali dati a paesi terzi non appartenenti all'Unione Europea. In aggiunta, il Titolare deve indicare il periodo di conservazione (o i criteri per determinare tale periodo), il diritto dell'interessato di chiedere l'accesso, il diritto di revocare il consenso, le possibili conseguenze della mancata comunicazione dei dati quando questi siano raccolti per dare esecuzione a un contratto, se è eventualmente svolta attività di profilazione;

- il diritto di accesso: il diritto di ottenere dal Titolare la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso diritto di ottenere l'accesso a una serie di informazioni indicate dall'art. 15 del Regolamento;
- il diritto alla comunicazione (art. 34) in caso di violazione dei dati personali che lo riguardano.

Invece, i diritti di controllo dell'interessato includono:

- il diritto a esprimere liberamente e in modo espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità. Si noti che il consenso non è richiesto quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte, o per adempiere un obbligo di legge (art. 6 par. 1 lett. a), b), c);
- il diritto alla revoca del consenso in qualsiasi momento (art. 7 par. 3);
- il diritto di opposizione al trattamento (art. 21) prevede che l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano;
- il diritto alla portabilità dei dati (art. 20), a norma del quale l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento;
- il diritto di rettifica e integrazione (art.16) in base al quale l'interessato ha il diritto a ottenere la rettifica dei dati personali inesatti che lo riguardano o l'integrazione dei dati personali incompleti;
- il diritto alla cancellazione e oblio (art. 17) a norma del quale l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano quando non sono più necessari per le finalità per le quali sono stati raccolti, quando l'interessato revoca il consenso o quando i dati personali sono stati trattati illecitamente;
- il diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (art. 22) pertanto, in tal caso, l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Con riferimento segnatamente al trattamento di dati personali nell'ambito di una pubblica amministrazione, oltre al rispetto di tutti i principi sopra menzionati, l'ente deve strutturarsi da un punto di vista amministrativo per far fronte all'adeguamento.

A tale proposito, va specificato che, con l'entrata in vigore del nuovo Regolamento, le pubbliche amministrazioni hanno dovuto strutturarsi in modo molto diverso rispetto a quanto prevedeva la normativa precedente.

I soggetti coinvolti nel trattamento dei dati personali sono essenzialmente i seguenti:

- titolare del trattamento;
- responsabili (esterni) del trattamento ed eventuali sub-responsabili (come, ad esempio, i fornitori dell'amministrazione);
- soggetti autorizzati;
- responsabile della protezione dei dati (c.d. DPO).

UFFICIO PRIVACY

Si segnala, anzitutto, che a differenza di quanto accadeva nel regime precedente nella vigenza del quale alcuni dirigenti venivano nominati "responsabili interni", in base al nuovo Regolamento europeo, tutte le attività del trattamento sono imputate al titolare, venendo meno la responsabilità di soggetti interni all'organizzazione.

Si aggiunge che, il D.lgs. n. 101/2018 con il quale, come già esposto, il Legislatore nazionale è intervenuto per adeguare il Codice Privacy al Regolamento europeo, specifica come il titolare del trattamento può strutturare la propria organizzazione.

A tale proposito, l'art. 2-quaterdecies del D.lgs. n. 196/2003 recita che: "*il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati le persone che operano sotto la propria autorità diretta*".

La disposizione appena citata colma il vuoto lasciato dal Regolamento europeo circa l'organizzazione degli enti e può essere interpretata alla luce della relazione illustrativa al decreto. Quest'ultima afferma che la suddetta disposizione consente di mantenere le funzioni e i compiti eventualmente assegnati a figure interne all'organizzazione.

Si segnala, comunque, che nella prassi applicativa, la necessità di rispettare il principio di "responsabilizzazione" del titolare del trattamento ha portato molte amministrazioni ad istituire appositi uffici ("privacy" o "protezione dati") con il compito di supportare il titolare negli adempimenti previsti dalla normativa in materia di protezione dei dati e nei rapporti con il DPO.

DPO

Il Regolamento riconferma le figure di titolare del trattamento e responsabile del trattamento e introduce una nuova figura: il Responsabile per la protezione dei dati personali (in inglese, *Data Protection Officer* o "DPO").

In particolare, l'art. 37, par. 1, lett. a) del Regolamento prevede che "*il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali*".

Come indicato dal WP29 nelle "*Linee-guida sui responsabili della protezione dei dati",* il DPO, nominato dal titolare e dal responsabile del trattamento, svolge un ruolo misto di vigilanza dei processi interni alla struttura del titolare e del responsabile con funzioni di consulenza per costoro, e di contatto con gli interessati e le autorità garanti; per svolgere i suoi compiti deve esser investito di ogni questione interna in materia di tutela dei dati personali.

Il DPO può essere un soggetto interno o esterno all'ente. In questo ultimo caso, si tratta di un appalto di servizi.

In ogni caso, il professionista deve esser scelto in base alla sua professionalità e alle sue competenze specialistiche in materia di protezione dei dati personali.

I compiti del DPO possono esser sinteticamente riassunti come segue:

- deve esser tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
- informa e fornisce consulenza al titolare, al responsabile del trattamento, ai dipendenti sulla normativa in materia di protezione dei dati personali;
- sorveglia l'osservanza del Regolamento;
- coopera con l'autorità di controllo in caso di *data breach* e funge da punto di contatto con il Garante Privacy per le questioni connesse al trattamento.

Sicurezza informatica e *privacy* – Stato dell'arte e adempimenti del Consiglio regionale della Sardegna

Dopo aver illustrato il quadro normativo in materia di sicurezza informatica e protezione dei dati personali, si indicano le principali priorità da affrontare nell'ottica di assicurare un pieno adempimento degli obblighi innanzi citati.

- In base a quanto da Voi rappresentato, l'Amministrazione consiliare ha provveduto all'implementazione delle misure minime di sicurezza. Si ricorda che il RTD, oltre a compilare il modulo, deve firmarlo digitalmente, marcarlo temporalmente, versarlo in conservazione e aggiornarlo ogni volta che intervengano delle modifiche con riferimento alle misure.

In aggiunta, occorre eventualmente valutare l'implementazione di ulteriori misure (cfr. Circolare AgID n. 2/2017).

Come più volte ribadito dall'AgID, a seconda della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa dell'amministrazione, le misure minime possono essere implementate in modo graduale seguendo i tre livelli di attuazione previsti:

1. minimo: è quello al quale ogni pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme;

2. standard: è il livello, superiore al livello minimo, che ogni amministrazione deve considerare come base di riferimento in termini di sicurezza e rappresenta la maggior parte delle realtà della amministrazione italiana;

3. avanzato: deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.

- Secondo quanto rappresentato, il Consiglio ha provveduto a designare un Responsabile per la protezione dei dati esterno (RPD o DPO).

L'Amministrazione consiliare dovrà completare l'adeguamento *privacy* provvedendo prioritariamente all'aggiornamento di informative e nomine e predisponendo i registri del trattamento. A tale proposito, dovrà riportare le misure indicate nel modulo di cui alla circolare AgID n. 2/2017 anche all'interno dei registri. Pur se non direttamente richiamato dal Reg. (UE) 2016/679 (GDPR) e dal D. Lgs. n. 196/2003 (così come modificato dal D. Lgs. n. 101/2018), si ritiene che le misure di sicurezza previste all'interno della Circolare debbano essere implementate anche al fine di assicurare il pieno adempimento della prescrizione dettata dall'art. 32 GDPR.

Particolare attenzione dovrà essere prestata all'aggiornamento delle valutazioni del rischio (e quindi delle misure di sicurezza) alla luce della veloce transizione verso forme flessibili di svolgimento delle prestazioni lavorative dei dipendenti.

6. ACQUISTI DI BENI E SERVIZI ICT

6.A – I vincoli di spesa per gli acquisti *ICT*

Disposizioni specifiche per gli acquisti ICT rilevanti ai fini del presente parere non sono contenute nel CAD ma sono state dettate dalla Legge n. 208/2015 (c.d. "Legge di bilancio per il 2016") che – all'art. 1, commi 512 e ss. – ha disciplinato la razionalizzazione dei processi di approvvigionamento di tali beni e servizi. Tale norma ha, infatti, previsto uno specifico regime per gli acquisti del settore informatico imponendo alle organizzazioni del settore pubblico di far ricorso alle convenzioni di CONSIP e degli altri soggetti aggregatori, così come chiarito di recente anche dai Giudici contabili secondo i quali i servizi ICT, in quanto considerati "*una speciale categoria merceologica*", sono oggetto di *"specifiche disposizioni di legge"* che impongono, *"senza alcuna distinzione di valore, il ricorso alle convenzioni CONSIP o dei soggetti aggregatori*" (così Corte dei conti, sez. reg.le di controllo Umbria, Deliberazione 28 aprile 2016, n. 52).

In particolare, il regime introdotto dalla Legge di Stabilità 2016 è particolarmente stringente e prevede che:

a) le amministrazioni pubbliche e le società inserite nel conto consolidato della PA devono approvvigionarsi esclusivamente tramite CONSIP o i soggetti aggregatori;

b) l'approvvigionamento autonomo (fuori dalle soluzioni messe a disposizione da CONSIP e dagli altri soggetti aggregatori) è limitato ai soli casi in cui il bene o il servizio non sia disponibile o idoneo al soddisfacimento dello specifico fabbisogno dell'amministrazione, ovvero in casi di necessità ed urgenza. In tali casi, inoltre, tale approvvigionamento autonomo è subordinato all'apposita autorizzazione motivata dell'organo di vertice amministrativo di ciascun ente;

c) per la spesa per la gestione corrente del settore ICT effettuata fuori dagli strumenti CONSIP, ciascuna amministrazione deve conseguire un obiettivo di risparmio pari al 50% rispetto alla spesa del triennio precedente;

d) il Piano Triennale per l'informatica nella pubblica amministrazione[45], redatto dall'Agenzia per l'Italia Digitale e approvato dal Presidente del Consiglio dei Ministri, contiene l'indicazione dei beni e servizi di particolare rilevanza strategica che le amministrazioni devono acquisire prioritariamente, affermando che – nell'ottica della razionalizzazione dei *datacenter* – sono bloccati tutti gli interventi di evoluzione dei *datacenter* esistenti (così come confermato dalla Circolare AgID n. 2/2016[46] e dal Piano triennale per l'informatica nella PA 2017-2019).

Va aggiunto, sempre con riferimento alla spesa - al fine di effettuare un'analisi il più possibile completa - che, come noto e come sarà approfondito nel prosieguo, è in atto anche una riorganizzazione del parco dei *data center* della pubblica amministrazione attraverso un'opera di razionalizzazione utile sia a ridurre i costi di gestione sia a uniformare e aumentare la qualità dei servizi offerti alle pubbliche amministrazioni (anche in termini di *business continuity, disaster recovery* ed efficienza energetica).

6.B – La razionalizzazione dei *data center*

Il Piano Triennale per l'informatica nella Pubblica Amministrazione, fin dalla sua prima edizione (2017-2019), ha perseguito l'obiettivo di razionalizzazione delle infrastrutture digitali.
Le tre principali direttrici della strategia sulle infrastrutture fisiche portata avanti dal Piano triennale sono:

1. la razionalizzazione e il consolidamento dei *data center* della pubblica amministrazione attraverso la progressiva dismissione dei data center obsoleti e inefficienti, con l'obiettivo di ridurre i costi di gestione delle infrastrutture IT in favore di maggiori investimenti in nuovi servizi digitali (vedi *supra*, Sez. 6. A);
2. la realizzazione del "Modello *cloud* della PA" e l'applicazione del principio "*cloud first*" con cui si intende facilitare la migrazione dei servizi delle pubbliche amministrazioni verso tale modello;

[45] https://pianotriennale-ict.italia.it/
[46] La Circolare AgID n. 2/2016 è disponibile al seguente link:
http://www.agid.gov.it/sites/default/files/documentazione/circolare_piano_triennale_24.6.2016._def.pdf

3. l'adeguamento del modello di connettività al paradigma *cloud*, favorendo la razionalizzazione delle spese per la connettività delle pubbliche amministrazioni e la diffusione della connettività nei luoghi pubblici a beneficio delle pubbliche amministrazioni, dei cittadini e delle imprese.

In attuazione di quanto previsto nelle precedenti edizioni del Piano triennale, l'AgID ha dato avvio, con la Circolare n. 5 del 30 novembre 2017, ad un Censimento del Patrimonio *ICT* della PA per individuare le infrastrutture fisiche:

1) candidabili ad essere utilizzate da parte dei Poli Strategici Nazionali (PSN);
2) con requisiti minimi di affidabilità e sicurezza dal punto di vista infrastrutturale e/o organizzativo (*data center* con carenze strutturali/organizzative considerate minori - classificabili nel Gruppo A);
3) con carenze strutturali e/o organizzative o che non garantiscono la continuità dei servizi (*data center* classificabili nel Gruppo B).

In data 20 febbraio 2020 l'AgID ha annunciato la conclusione del censimento. Secondo i dati sintetici resi disponibili[47], ne sono stati individuati 35 candidabili a PSN, mentre altri 27 sono stati classificati nel Gruppo A. I restanti sono stati classificati nel Gruppo B (compresi quelli delle amministrazioni che non hanno partecipato al censimento, così come previsto all'art. 4 dalla Circolare AgID n. 1 del 2019).[48]

Il Piano Triennale 2020-2022 è intervenuto su tale classificazione dei *data center* (poi ribadita nel Piano Triennale 2021-2023), prevedendo che le categorie "infrastrutture candidabili ad essere utilizzate da parte dei PSN" e "Gruppo A", come delineate nella Circolare n. 1/2019[49], sono rinominate "A".

Con particolare riferimento alle amministrazioni locali, secondo le ultime disposizioni contenute nel Piano, le amministrazioni i cui *data center* sono stati classificati nel gruppo B, al fine di razionalizzare le infrastrutture digitali sono tenute, in alternativa:

- a dismettere le proprie infrastrutture migrare i propri servizi verso soluzioni *cloud* qualificate da AgID, previa trasmissione ad AgID dei piani di migrazione;
- stringere accordi con altre amministrazioni per consolidare le infrastrutture e servizi all'interno di *data center* classificati "A" (cioè, secondo la precedente denominazione, PSN e *data center* del Gruppo A).

[47] La sintesi del rapporto sul Censimento ICT è disponibile al seguente link: http://www.agid.gov.it/sites/default/files/repository_files/sintesi_rapporto_censimento_patrimonio_ict.pdf

[48] La Circolare AgID n. 1 del 2019 sul Censimento del patrimonio ICT delle Pubbliche Amministrazioni e classificazione delle infrastrutture idonee all'uso da parte dei Poli Strategici Nazionali è reperibile al link: https://www.agid.gov.it/sites/default/files/repository_files/circolare_1_agid_2019_id_2.pdf

[49] Si rappresenta che, come indicato nel Piano 2020-2022, entro dicembre 2020 è prevista l'emanazione della circolare AgID per l'attuazione e il monitoraggio della strategia di razionalizzazione dei data center delle pubbliche amministrazioni locali, in aggiornamento di quanto previsto dalla Circolare AgID 1/2019.

Con riguardo ai limiti di spesa, poi, il nuovo Piano prevede che le PA proprietarie di *data center* di gruppo B devono richiedere l'autorizzazione ad AgID per le spese in materia di *data center* nelle modalità stabilite dalla Circolare AgID n. 1/2019, mentre le PA proprietarie di *data center* classificati "A" possono continuare a gestire e manutenere le proprie infrastrutture, comunque comunicando ad AgID le relative spese secondo le modalità di cui alla Circolare n. 1/2019.

In tema di infrastrutture fisiche, in conclusione, si devono menzionare le recenti previsioni del D.L. 16 luglio 2020, n. 76. Con le modifiche introdotte all'art. 33-septies del D.L. n. 179/2012 dall'art. 35 del Decreto, si dà continuità al processo di razionalizzazione delle infrastrutture ICT della pubblica amministrazione, proseguendo il percorso intrapreso con le precedenti edizioni del Piano triennale per l'informatica nella PA e il censimento dei data center portato a termine da AgID nel 2020. Si prevedono, però, anche importanti novità.

In particolare, si introduce a livello normativo l'**obbligo** per le amministrazioni, sia centrali che locali, di provvedere alla migrazione dei servizi erogati tramite infrastrutture di elaborazione dati prive di adeguati standard. Per quanto riguarda le amministrazioni centrali, la migrazione dovrà essere effettuata verso un'infrastruttura pubblica ad alta affidabilità, localizzata sul territorio nazionale, il cui sviluppo è promosso dalla Presidenza del Consiglio dei ministri. In alternativa, la migrazione potrà avvenire verso altre infrastrutture esistenti, anche proprie, purché munite dei requisiti individuati da AgID con proprio regolamento adottato, ai sensi del comma 4 del citato art. 33-*septies*, d'intesa con la competente struttura della Presidenza del Consiglio dei ministri. Alle amministrazioni centrali è rimessa, inoltre, la possibilità di migrare verso l'infrastruttura realizzata da Sogei S.p.A. oppure verso soluzioni *cloud* per la pubblica amministrazione, nel rispetto dei requisiti fissati da AgID nel citato regolamento. Le **amministrazioni locali** saranno tenute a migrare verso un'infrastruttura pubblica ad alta affidabilità, localizzata sul territorio nazionale, il cui sviluppo è promosso dalla Presidenza del Consiglio dei ministri. In alternativa, saranno tenute a migrare verso le infrastrutture esistenti munite dei requisiti di cui al regolamento AgID, o verso soluzioni *cloud* per la pubblica amministrazione, sempre nel rispetto dei requisiti fissati da AgID con il regolamento. Dagli obblighi di migrazione, invece, sono escluse le amministrazioni che svolgono funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e consultazioni elettorali, nonché di comunicazione di emergenza e di allerta in ambito di protezione civile.

Con **il regolamento** previsto dall'art. 33-*septies*, comma 4 del Decreto-legge n. 179/2012, adottato con determinazione DG dell'AgID n. 628/2021[50], AgID ha definito i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione[51] (nonché le caratteristiche di qualità, di sicurezza, di performance e scalabilità,

[50] Il "Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitale per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la Pubblica Amministrazione" è reperibile al seguente link: https://trasparenza.agid.gov.it/archivio28_provvedimenti-amministrativi_0_123065_725_1.html

[51] Cfr. l'allegato A al Regolamento AgID, consultabile al seguente link: https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/2134818432500__ORegolamento+servizi+cloud.pdf

interoperabilità, portabilità dei servizi *cloud* per la pubblica amministrazione, di cui si dirà *infra*). Come previsto nel Regolamento, ulteriori livelli minimi delle infrastrutture digitali della PA, inoltre, sono stati definiti con gli atti successivi, adottati dall'Autorità per la Cybersicurezza Nazionale il 18 gennaio 2022[52].

Secondo quanto previsto dal Regolamento, l'adeguamento ai nuovi requisiti minimi delle infrastrutture dovrà avvenire entro 12 mesi dall'entrata in vigore del regolamento stesso e dall'emanazione degli atti successivi dell'ACN, dunque, rispettivamente, entro il 3 gennaio e il 18 gennaio 2023.

6.C – Il modello *cloud* della PA. Cenni sull'approvvigionamento di soluzioni *cloud* da parte della PA

Nell'ambito della strategia sulla trasformazione digitale della pubblica amministrazione italiana, l'adozione del paradigma del *cloud computing* rappresenta un elemento fondamentale poiché incide profondamente sia sull'organizzazione degli uffici che sui processi di erogazione dei servizi ai cittadini. Il ricorso al *cloud*, d'altra parte, viene favorito in quanto si ritiene determini notevoli vantaggi in termini di incremento di affidabilità e sicurezza dei sistemi, innalzamento della qualità dei servizi erogati e risparmi di spesa per le pubbliche amministrazioni.

La strategia per le infrastrutture fisiche della PA, già contenuta nel Piano Triennale per l'informatica nella pubblica amministrazione 2017-2019 e 2019-2021, è stata ulteriormente sviluppata nel Piano per gli anni 2020-2022 e poi da ultimo ribadita nel Piano Triennale 2021-2023.

Nell'ambito della strategia complessiva di cui sopra è stata descritta la parte relativa alla razionalizzazione dei *data center*, è stato previsto uno specifico percorso per la creazione di un ambiente *cloud* per la pubblica amministrazione. In particolare, il principio affermato è quello del "*cloud first*", secondo il quale le pubbliche amministrazioni devono prioritariamente adottare il paradigma *cloud* prima di qualsiasi altra opzione tecnologica[53].

Come esposto, l'adozione dell'infrastruttura *cloud* viene favorita per varie ragioni di efficienza ed economicità.

Nel Piano triennale le infrastrutture sono suddivise in:

a) *cloud* pubblico: i *cloud service provider* (CSP) qualificati presso l'AgID;

b) *cloud* privato: i poli strategici nazionali (PSN) individuati secondo le indicazioni dell'AgID;

c) infrastruttura *Community Cloud* realizzata dal raggruppamento temporaneo di imprese aggiudicatario del contratto quadro Consip SPC *Cloud* lotto 1, fino al termine del contratto (2021).

[52] Cfr. l'allegato A2 all'atto di aggiornamento di ACN, consultabile al seguente link: https://assets.innovazione.gov.it/1642754054-all1det307acn.pdf

[53] Al fine di facilitare l'adozione del "Modello *cloud* della PA", l'AgID e il Team per la trasformazione digitale hanno avviato un Programma nazionale di abilitazione al *cloud*, anche detto "*Cloud Enablement Program*". Il programma si ispira al principio "*cloud first*", secondo il quale, come anticipato, le pubbliche amministrazioni in fase di definizione di un nuovo progetto e/o di sviluppo di nuovi servizi, devono, in via prioritaria, valutare la possibilità di adottare il paradigma *cloud* prima di qualsiasi altra tecnologia.

Invece, le soluzioni in *cloud* possono essere di tipo *Software as a service* (Saas), *Platform as a service* (Paas) e *Infrastructure as a service* (Iaas).

In particolare, il *public cloud* identifica un'infrastruttura di proprietà di un fornitore (il *cloud provider*) nel quale l'uso del sistema informatico non è dedicato a un singolo utente, ma ad una molteplicità di fruitori indeterminati. È questo il caso dei fornitori di servizi *cloud* disciplinati dalle Circolari dell'AgID numero 2 e 3, entrate in vigore il 20 maggio 2018[54]. Le Circolari prevedono l'obbligo per le amministrazioni di ricorrere a soggetti esterni qualificati: per tale motivo, a partire dal 1° aprile 2019, le amministrazioni possono acquisire solo servizi qualificati da soggetti qualificati in base alla procedura definita e gestita dall'Agenzia per l'Italia Digitale[55].

Quando si parla di *private cloud*, si fa riferimento, invece, alla realizzazione e all'uso di un sistema di "nuvole" realizzato e gestito *ad hoc* per una singola azienda o per una singola pubblica amministrazione, così da avere un sistema in cui queste ultime possono decidere autonomamente chi farvi accedere (ad esempio, dipendenti e collaboratori).

Chiaramente la valutazione sulla scelta della tipologia di modello *cloud* (pubblico, privato o ibrido) è guidata principalmente dalla finalità del servizio all'utente e dalla natura di dati trattati. In proposito si segnala che AgID, nell'ambito del Programma di abilitazione al *cloud*, ha predisposto il *Cloud enablement kit*[56], che raccoglie metodologie, strumenti e buone pratiche e fornisce alle pubbliche amministrazioni possibili soluzioni per elaborare una propria strategia di migrazione dei servizi verso il *cloud*.

Con riferimento specificamente al processo di qualificazione[57], come previsto nelle circolari, lo stesso si struttura in tre fasi: richiesta, conseguimento e mantenimento della qualificazione.

I soggetti pubblici e privati, che vogliono fornire *cloud* alle amministrazioni e, quindi, qualificarsi ed entrare nel Catalogo[58], devono inoltrare informazioni e documentazione che attestino la loro conformità a una serie di requisiti organizzativi, di sicurezza, di performance e scalabilità, interoperabilità e portabilità fissati dalle Circolari dell'AgID nn. 2 e 3 del 2018[59].

[54] Le circolari sono disponibili all'indirizzo https://cloud.italia.it/projects/cloud-italia-circolari/it/latest/

[55] Allo stato attuale, il Registro pubblico dei CSP qualificati, rinvenibile sul sito dell'AgID (link: https://cloud.italia.it/marketplace/supplier/market/index_csp.html), contiene circa 50 CSP. Sono 5, invece, i *Cloud Service Provider* iscritti ai sensi dell'art. 192 del Codice dei Contratti Pubblici nell'elenco tenuto dall'Autorità Nazionale Anticorruzione delle amministrazioni aggiudicatrici e degli enti aggiudicatori che operano mediante affidamenti diretti nei confronti di proprie società *in house* di cui all'art. 2 del D.lgs n. 50/2016.

[56] Il *Cloud enablement kit* di AgID è disponibile al seguente link: https://cloud.italia.it/it/cloud-enablement/#kit

[57] Si deve segnalare che è in corso una fase di transizione dalla normativa di cui alle Circolari dell'AgID nn. 2 e 3 del 2018 verso l'applicazione del nuovo Regolamento sulla qualificazione dei servizi cloud, che, in accordo alla normativa vigente, affida all'Autorità per la Cybersicurezza Nazionale (ACN) le funzioni in materia di processo di qualificazione dei servizi cloud per la PA. Le attività per la qualificazione continueranno ad essere svolte dall'AgID fino all'entrata in vigore dei decreti del Presidente del Consiglio dei Ministri di cui all'art. 17, c. 5, del decreto-legge 14 giugno 2021, n. 82, di trasferimento delle funzioni ad ACN.

[58] Il *marketplace* è raggiungibile all'indirizzo https://cloud.italia.it/marketplace

[59] Si rileva che le richiamate circolari saranno prossimamente sostituite dal regolamento in materia di servizi cloud di recente adottato dall'AgID (v. supra, nota 54).

Elemento fondamentale da tenere in considerazione sin da ora è che i soggetti che intraprendono il processo di qualificazione in una prima fase si limitano a presentare autocertificazioni e sulla base di queste ultime vengono inseriti nel catalogo.

La qualificazione ha durata pari a 24 mesi a decorrere dalla data di iscrizione nel registro pubblico disponibile su cloud.italia.it.

L'AgID può verificare in ogni momento il possesso dei criteri di ammissibilità e dei requisiti previsti per la qualificazione conseguita. La perdita del possesso dei criteri di ammissibilità e/o di almeno uno dei requisiti comporta la revoca della qualificazione ed è per questo che nei contratti con i fornitori le amministrazioni dovrebbero assicurarsi l'impegno dei *provider* a mantenere la qualificazione per l'intera durata del rapporto. Peraltro, ai sensi delle Circolari AgID n. 2 e 3 del 2018, è compito delle singole amministrazioni acquirenti monitorare l'effettivo mantenimento dei requisiti di qualificazione da parte del *provider.* Come di recente specificato dall'AgID con determinazione n. 419/2020[60] (recante "Chiarimenti applicativi in merito alle Circolari AGID nn. 2 e 3 del 9 aprile 2018, recanti i criteri per la qualificazione dei Cloud Service Provider per la PA e dei servizi SaaS per il Cloud della PA"), **è compito delle singole pubbliche amministrazioni verificare l'effettivo rispetto delle dichiarazioni prodotte in sede di qualificazione dal fornitore**. In caso di servizi non conformi a quanto autodichiarato dal fornitore, la pubblica amministrazione è tenuta a segnalare la circostanza ad AgID che, in caso di esito confermativo dell'apposita verifica, procede alla revoca della qualificazione. Al riguardo AgID ha altresì precisato che **il possesso della qualificazione può essere richiesto** dalle pubbliche amministrazioni quale requisito per l'acquisizione di servizi Iaas, Paas e Saas **unicamente in fase di aggiudicazione** e non già in fase di partecipazione alla procedura di acquisizione.

Con particolare riferimento ai requisiti tecnici di sicurezza, *privacy* e protezione dei dati richiesti ai *provider* ai fini del conseguimento della qualificazione (cfr. nelle richiamate Circolari AgID del 2018, le previsioni degli allegati recanti i criteri per la qualificazione dei *Cloud Service Provider* della PA), si sottolinea che, se da una parte il fornitore *cloud* è tenuto a dichiarare la qualità offerta e l'affidabilità del servizio durante tutto il ciclo di vita, dall'altra, che è compito delle singole amministrazioni acquirenti assicurarsi che le pattuizioni relative alla qualità del servizio costituiscano parte integrante del contratto di fornitura.

Da ultimo si devono segnalare, poi, altre previsioni del D.L. 16 luglio 2020, n. 76. A seguito delle modifiche all'art. 12 del CAD, si prevede che al fine di agevolare la diffusione del **lavoro agile**, le pubbliche amministrazioni **acquistano beni e progettano e sviluppano i sistemi informativi e i servizi informatici con modalità idonee a consentire ai lavoratori di accedere da remoto ad applicativi, dati e informazioni necessari allo svolgimento della prestazione lavorativa**, assicurando un adeguato livello di **sicurezza informatica** e promuovendo la consapevolezza dei lavoratori sull'uso sicuro degli strumenti impiegati, in particolare i servizi in ***cloud***. Si prevede inoltre che le pubbliche amministrazioni adottino ogni misura atta a garantire la sicurezza informatica e la **protezione dei dati**, compresa la diffusione di linee guida presso i lavoratori o la regolamentazione

[60] La determinazione n. 419/2020 è reperibile al seguente link: https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/2026512314600__O419+DT+DG+n.+419+-+22+sett+2020+-+Chiarimenti+applicativi+Circolari+2-3+2018+-+18.9.20+%28002%29.pdf

delle attività che possono essere svolte. Si prevede, infine, che nella realizzazione e lo sviluppo dei sistemi informativi e dei servizi digitali, deve essere garantito il rispetto del *codice di condotta tecnologia* e, inoltre, deve essere **sempre assicurata l'integrazione con le piattaforme abilitanti PagoPa, SPID, CIE ed IO** (cfr. nuovo art. 13-*bis* del CAD, commi 3 e 4).

Nel quadro appena descritto si è inserita la nuova strategia italiana sul cloud, di recente pubblicazione[61].

La strategia si inserisce in continuità con alcune scelte innovative che assicurano la coerenza rispetto al PNRR. Il principio seguito è sempre quello del cloud first.

La strategia prevede di mettere in sicurezza i servizi erogati dalle amministrazioni e in particolare, in conformità a quanto già previsto:

- le **amministrazioni centrali** i cui sistemi informativi non hanno i requisiti definiti da AgID, migrano i servizi ospitati su tali sistemi verso l'infrastruttura ad alta affidabilità promossa dalla Presidenza del Consiglio dei Ministri, anche detta Polo Strategico Nazionale oppure verso i servizi cloud qualificati;
- le **amministrazioni locali** i cui sistemi informativi non hanno i requisiti definiti da AgID, migrano i servizi ospitati su tali sistemi verso soluzioni cloud qualificate da AgID; o in alternativa, possono rivolgersi ad altre amministrazioni locali (data center di tipo A), o al Polo Strategico Nazionale per consolidare le proprie infrastrutture e servizi.

La scelta di quali servizi migrare verso soluzioni cloud qualificate o verso infrastrutture pubbliche – munite dei requisiti minimi stabiliti dalla normativa avviene sulla base della **classificazione dei dati** e dei servizi digitali dell'ente, secondo il Modello di recente adottato dall'ACN[62] ai sensi del Regolamento dell'AgID in materia di infrastrutture digitali e servizi cloud per la PA[63], entrato in vigore il 3 gennaio 2022.

Le classi dei dati e servizi sono identificate sulla base del danno che una loro compromissione, in termini di confidenzialità, integrità e disponibilità, provocherebbe al sistema Paese. Tali classi sono:

- Strategico: dati e servizi la cui compromissione può avere un impatto sulla sicurezza nazionale;
- Critico: dati e servizi la cui compromissione potrebbe determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale del Paese;

[61] Il documento strategico pubblicato dal Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei ministri è accessibile al seguente url: https://cloud.italia.it/strategia-cloud-pa/.

[62] Il "*Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione*", adottato dall'AgID il 15 dicembre 2021, è consultabile al seguente link: https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/2134818432500__ORegolamento+servizi+cloud.pdf

[63] Il "*Modello per la predisposizione dell'elenco e della classificazione dei dati e dei servizi digitali delle pubbliche amministrazioni*", adottato dall'ACN il 18 gennaio 2022, è consultabile al seguente link: https://assets.innovazione.gov.it/1642694063-det_306_all1_20220118_modello.pdf

- Ordinario: dati e servizi la cui compromissione non provochi l'interruzione di servizi dello Stato o, comunque, un pregiudizio per il benessere economico e sociale del Paese.

Secondo quanto previsto nel citato Regolamento, entro il 18 luglio 2022 le amministrazioni sono tenute a trasmettere all'ACN l'elenco e la classificazione dei dati e dei servizi digitali secondo il modello, sul quale l'Agenzia effettua un'attività di **verifica di conformità**. L'elenco e la classificazione, poi, devono essere soggetti a costante aggiornamento.

6.D – Acquisizione del *software* e riuso

Sempre con riferimento al tema degli acquisti ICT, risulta necessario richiamare altresì brevemente alcune norme del Codice dell'amministrazione digitale concernenti, in generale, l'acquisizione di *software* da parte della PA e, più in particolare, il riuso di sistemi informatici.

L'art. 68 del D.lgs. n. 82 del 2005 (Codice dell'amministrazione digitale, di seguito CAD), prima disposizione del capo VI del Codice relativo a "SVILUPPO, ACQUISIZIONE E RIUSO DI SISTEMI INFORMATICI NELLE PUBBLICHE AMMINISTRAZIONI", riprende un ragionamento proprio del diritto d'autore e collega lo sviluppo di "*oggetti informatici*" al concetto di titolarità. La norma parla anche di riuso come diritto/dovere di usare e di dare in uso ad altri in considerazione di una spesa che è già stata sostenuta e che ha natura di investimento generale della PA.

Fondamentale rilevanza riveste la valutazione comparativa che la pubblica amministrazione deve effettuare, ai sensi della suddetta norma, prima di procedere ad un acquisto quando intende acquisire programmi informatici o parti di essi.

Il succitato art. 68 CAD, infatti, prevede che: "*Le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato:*

a.software sviluppato per conto della pubblica amministrazione;

b.riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione;

c.software libero o a codice sorgente aperto;

d.software fruibile in modalità cloud computing;

e.software di tipo proprietario mediante ricorso a licenza d'uso;

f.*software combinazione delle precedenti soluzioni*".

Come esposto, il comma 1-*bis* della norma in oggetto impone all'amministrazione di effettuare una valutazione comparativa delle diverse soluzioni disponibili prima di procedere all'acquisto mediante le procedure del Codice dei contratti pubblici e di farlo sulla base dei seguenti criteri:

a. costo complessivo del programma o soluzione quale costo di acquisto, di implementazione, di mantenimento e supporto;

b. livello di utilizzo di formati di dati e di interfacce di tipo aperto nonché di standard in grado di assicurare l'interoperabilità e la cooperazione applicativa tra i diversi sistemi informatici della pubblica amministrazione;

c. garanzie del fornitore in materia di livelli di sicurezza, conformità alla normativa in materia di protezione dei dati personali, livelli di servizio tenuto conto della tipologia di software acquisito.

Il successivo comma 1-*ter* prevede, poi, che, ove dalla valutazione comparativa di tipo tecnico ed economico, secondo i criteri riportati nel comma 1 *bis*, risulti motivatamente l'impossibilità di accedere a soluzioni già disponibili all'interno della pubblica amministrazione, o a *software* liberi o a codici sorgente aperto, adeguati alle esigenze da soddisfare, è consentita l'acquisizione di programmi informatici di tipo proprietario mediante ricorso a licenza d'uso.

Il Codice aggiunge, infine, che la suddetta valutazione deve essere effettuata secondo le modalità e i criteri definiti dall'AgID.

Ci si sofferma, a questo punto, sull'art. 69 del CAD che è rubricato "*Riuso delle soluzioni e standard aperti*" ed è stato di recente profondamente modificato dal Correttivo al Codice del dicembre 2017 (D.lgs. n. 217/2017).

In particolare, la disposizione prevede che le pubbliche amministrazioni titolari di soluzioni e programmi informatici realizzati su specifiche indicazioni del committente pubblico, salvo motivate ragioni di ordine e sicurezza pubblica, difesa nazionale e consultazioni elettorali, hanno l'obbligo di rendere disponibile il relativo codice sorgente, completo della documentazione e rilasciato in repertorio pubblico sotto licenza aperta, in uso gratuito ad altre pubbliche amministrazioni o ai soggetti giuridici che intendano adattarli alle proprie esigenze.

Aggiunge, sempre nell'ottica di favorire il riuso dei programmi informatici di proprietà della pubblica amministrazione, che nei capitolati o nelle specifiche di progetto deve essere previsto, ove possibile, che l'amministrazione committente sia sempre titolare di tutti i diritti sui programmi e i servizi delle tecnologie dell'informazione e della comunicazione, appositamente sviluppati per essa, salvo che risulti eccessivamente oneroso per comprovate ragioni di carattere tecnico-economico.

È utile ribadire che, quando si parla di titolarità di un *software* in materia di riuso ai sensi dell'art. 69 CAD, si tratta di un prodotto realizzato su indicazioni specifiche della pubblica amministrazione che può aver commissionato lo stesso attraverso contratto di appalto o altra fattispecie negoziale (quando il contratto preveda l'acquisizione in capo alla PA di tutti i diritti di proprietà intellettuale e industriale sul *software*) oppure di un prodotto realizzato da risorse interne all'amministrazione. Si aggiunge che, chiaramente, tutto il *software* a riuso è *open source* ma non tutto il *software open source* è a riuso.

Dal combinato disposto degli articoli 68 e 69 del CAD, si evince, infatti, che il *software* in riuso è esclusivamente quello rilasciato sotto licenza aperta da una pubblica amministrazione. Quest'ultimo è, dunque, un sottoinsieme di tutto il *software open source* disponibile per l'acquisizione.

Il comma 2-*bis* dell'art. 69 CAD conclude affermando che **il codice sorgente, la documentazione e la relativa descrizione tecnico funzionale di tutte le soluzioni informatiche di cui al comma 1 sono pubblicati attraverso una o più piattaforme individuate dall'AgID con proprie Linee guida.**

L'AgID, in collaborazione con il Team per la trasformazione digitale, ha di recente redatto linee guida su acquisizione e riuso di *software* per le pubbliche amministrazioni[64] che sono state pubblicate il 9 maggio 2019 a seguito di consultazione pubblica.

Come anticipato, il documento denota un sensibile cambio di approccio rispetto alla disciplina precedente. In linea con le ultime modifiche del CAD, infatti, si nota una svolta a favore del riuso e le linee guida si pongono come punto di avvio di un processo culturale che veda le pubbliche amministrazioni protagoniste di un sempre maggiore ricorso al *software* aperto.

Si rileva, anzitutto, che il documento si propone di attuare quanto stabilito dagli artt. 68 e 69 del CAD. Intende, infatti, come disposto dall'articolo 68, comma 1 *ter*, individuare le modalità e i criteri con i quali un'amministrazione deve effettuare la valutazione comparativa descritta nel citato articolo per decidere la modalità di acquisizione di un *software* e, come statuito dall'articolo 69, comma 2 *bis*, individuare la piattaforma per la pubblicazione di codice sorgente sotto licenza aperta e documentazione del *software* messo a riuso dalle amministrazioni, indicando anche le modalità tecniche di utilizzo.

Il documento vuole ribadire altresì che: "*i principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica (comma 1 dell'art. 68 CAD) si raggiungono attuando quanto previsto dal comma 2 dell'art. 69 del CAD: "il riuso dei programmi informatici di proprietà delle pubbliche amministrazioni" garantendo che queste ultime, oltre ad essere titolari del software, rendano il software open source attraverso l'apposizione di una licenza aperta".* Le linee guida in oggetto sostituiscono la precedente circolare n. 63/2013 dell'AgID. Ebbene, le nuove linee guida,

[64] Disponibili al seguente link: https://www.agid.gov.it/sites/default/files/repository_files/lg-acquisizione-e-riuso-software-per-pa-docs_pubblicata.pdf

dopo una breve parentesi riservata all'analisi delle soluzioni[65] e dei criteri per la valutazione[66], si soffermano sulle fasi della valutazione comparativa.

Il percorso previsto dal documento è strutturato in tre macro-fasi: la prima ha l'obiettivo di definire le esigenze della pubblica amministrazione specificando i bisogni e i vincoli organizzativi ed economici che condizionano le scelte per l'identificazione di una soluzione adeguata alle esigenze dell'amministrazione; nell'ambito della seconda fase, l'amministrazione accerta la possibilità di soddisfare le proprie esigenze utilizzando una soluzione già in uso (soluzioni a riuso) presso le altre amministrazioni o a *software* libero o codice sorgente aperto (soluzioni *open source*); la terza fase interviene nel caso in cui la seconda non permetta di rispondere alle esigenze della pubblica amministrazione e dunque si deve ricorrere a programmi informatici di tipo proprietario con licenza d'uso e/o realizzazioni *ex novo*.

Si sottolinea che, con riguardo specificamente alla seconda fase, la pubblica amministrazione, a partire dalla disponibilità di soluzioni a riuso delle pa e soluzioni *open source*, deve verificare il soddisfacimento delle proprie esigenze in tali soluzioni. Peraltro, le linee prevedono che, per razionalizzare la spesa, la verifica di soddisfacimento delle esigenze debba rivolgersi prima alle soluzioni a riuso e solo dopo alle soluzioni *open source* (cioè *software* rilasciato sotto licenza aperta ma non di titolarità di una pubblica amministrazione e quindi non pubblicato a riuso). D'altra parte, l'attuazione dell'art. 69 CAD assicura che le soluzioni a riuso rendano disponibile il relativo codice sorgente, completo della documentazione, in repertorio pubblico sotto licenza aperta.

[65] La seguente lista di definizioni descrive le sei soluzioni previste dalla normativa:

A - software sviluppato per conto della pubblica amministrazione Soluzione detta anche «opzione make»: la PA affida lo sviluppo del software (sia esso ex novo o modifica di software esistente) a un fornitore e quest'ultimo si impegna a consegnare alla P.A. il software sviluppato sulla base dei requisiti da questa definiti. Per esempio, nel ciclo di vita del software (analisi, progettazione, sviluppo, collaudo, rilascio, manutenzione) la P.A. potrebbe occuparsi delle fasi di analisi e progettazione, definendo i requisiti del software, per poi affidare lo sviluppo al fornitore.

B - Riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione Soluzione «riu- so» di un software della P.A. (o suoi componenti) già esistente e disponibile.

C - software libero o a codice sorgente aperto software con licenza Open Source (vedi Glossario (pagina 5)). In particolare, si intende tutto il software distribuito sotto una licenza certificata da OSI (lista completa6), come descritto in Licenze per il software aperto (pagina 26).

D - software fruibile in modalità cloud computing Soluzione nella quale la P.A. acquisisce il software come servizio. In questa soluzione non sono ricomprese le soluzioni HaaS (Hardware as a Service) e IaaS (Infrastructure as a Service).

E - software di tipo proprietario mediante ricorso a licenza d'uso software soggetto a condizioni di licenza d'uso di tipo proprietario da installare «on premise».

F - software combinazione delle precedenti soluzioni software realizzato con componenti appartenenti a più di una categoria tra quelle precedenti. Ad esempio, software in cui una soluzione in riuso si appoggia su un middleware Open Source e accede a un database proprietario, con componenti realizzate appositamente per conto dell'amministrazione destinataria della soluzione. È di fatto la tipologia più comune tra quelle effettivamente in uso nelle pubbliche amministrazioni.

[66] Costo complessivo, utilizzo di formati di dati aperti, utilizzo di interfacce aperte, utilizzo di standard per l'interoperabilità, livelli di sicurezza, conformità alla normativa in materia di protezione dei dati personali, livelli di servizio del fornitore.

È importante sottolineare che, una volta e solo se accertata l'impossibilità di individuare una soluzione a riuso o *open source*, l'amministrazione può procedere alla redazione di un documento che motivi le ragioni dell'accertata impossibilità. Solo a quel punto, le linee guida prevedono che si possano esaminare contestualmente le soluzioni proprietarie e quelle volte a una realizzazione *ex novo*.

Peraltro, nel caso in cui si opti per la realizzazione *ex novo*, considerando i commi 1 e 2 dell'Articolo 69 che disciplinano la messa a riuso del software che verrà realizzato, le linee rimandano al tema dello sviluppo di software ex novo per le informazioni su come progettare questa realizzazione per adempiere ai commi citati e metterlo così a riuso.

Nel caso che si proceda ad una acquisizione di *software* proprietario sotto licenza, si ricorda che l'Amministrazione deve, ove possibile, acquisire la titolarità del codice sviluppato per metterlo a riuso.

Ebbene, sembra che, in effetti, il Codice dell'amministrazione digitale abbia delineato un vero e proprio modello di riuso. Come esposto, infatti, il Legislatore manifesta un *favor* affinché, nell'ambito della valutazione comparativa di cui all'art. 68, l'amministrazione scelga soluzioni a riuso o *open source*. Nel caso in cui dovesse rendersi necessario, per il soddisfacimento delle specifiche esigenze, ricorrere alla realizzazione di un software *ex novo* o alla personalizzazione di un *open source* esistente, invece, l'amministrazione potrà utilizzare proprie risorse o ricorrere ad un appalto per farlo. In quest'ultimo caso, tuttavia, ai sensi dell'art. 69, comma 2, l'amministrazione deve garantirsi l'acquisizione della titolarità di tutti i diritti di proprietà intellettuale e industriale sul *software* in oggetto. Peraltro, in caso di realizzazione, l'amministrazione deve pubblicare il codice del proprio *software* sotto una licenza aperta in una piattaforma che rispetta i requisiti previsti dalle linee guida registrandone il rilascio dentro *Developers* Italia. Secondo quanto previsto dal Piano triennale 2020-2022, infatti, a partire da ottobre 2020 le PA sono tenute a dichiarare, all'interno del catalogo di *Developers* Italia[67], quali software di titolarità di un'altra PA hanno preso in riuso.

Si noti che, se il *software* in oggetto dovesse essere scelto per il soddisfacimento delle proprie esigenze da un'altra amministrazione e da quest'ultima personalizzato, la personalizzazione è comunque soggetta a quanto previsto dall'art. 69, comma 1 del CAD e risulta dunque necessario il rilascio del relativo codice sorgente sotto licenza aperta.

Tutto il procedimento descritto dovrebbe essere reso possibile mediante l'utilizzo della piattaforma *Developers* Italia dell'AgID.

Come sintetizzato dalle linee guida, dunque, "*il modello del riuso tramite software Open Source consente quindi di trovare un software, valutarlo e personalizzarlo senza stipulare alcuna convenzione con l'amministrazione che ha messo a riuso il software stesso, oltre all'accettazione della licenza Open Source che si perfeziona con il semplice download. Inoltre, il software è disponibile online e non è quindi necessaria alcuna richiesta di accesso.*

È importante però considerare che il software potrebbe non essere «pronto all'uso». L'amministrazione potrebbe quindi avere necessità di un intervento tecnico per installare il software,

[67] Link: https://developers.italia.it/

adattarlo alle proprie esigenze, formare il personale che dovrà usarlo, avere a disposizione supporto e manutenzione. Per tutti questi interventi, l'amministrazione può usare proprie risorse o forniture, poiché nessun vincolo da questo punto di vista è imposto all'amministrazione che ha realizzato il software e lo ha messo a riuso".

Da ultimo, si segnala quanto previsto dall'art. 53 del D.L. 31 maggio 2021, n. 77 (c.d. "Decreto Semplificazioni 2021"), come modificato in sede di conversione dalla Legge 29 luglio 2021, n. 108. Ai sensi del comma 1 della norma citata, "*Fermo restando, per l'acquisto dei beni e servizi di importo inferiore alle soglie di cui all'articolo 35 del decreto legislativo 18 aprile 2016, n. 50, quanto previsto dall'articolo 1, comma 2, lettera a), del decreto-legge 16 luglio 2020, n. 76, convertito, con modificazioni, dalla legge 11 settembre 2020, n. 120, così come modificato dal presente decreto, le stazioni appaltanti possono ricorrere alla procedura di cui all'articolo 48, comma 3"* sarebbe a dire, **procedura negoziata senza previa pubblicazione del bando** ex art. 63 del Codice dei contratti pubblici, "*in presenza dei presupposti ivi previsti, in relazione agli affidamenti di importo superiore alle predette soglie, aventi ad oggetto l'acquisto di beni e servizi informatici, in particolare basati sulla tecnologia cloud, nonché servizi di connettività, finanziati in tutto o in parte con le risorse previste per la realizzazione dei progetti del PNRR, la cui determina a contrarre o altro atto di avvio del procedimento equivalente sia adottato entro il 31 dicembre 2026, anche ove ricorra la rapida obsolescenza tecnologica delle soluzioni disponibili tale da non consentire il ricorso ad altra procedura di affidamento*".

Al successivo comma 2, si prevede, inoltre, che le amministrazioni possano **stipulare immediatamente il relativo contratto**, previa acquisizione di un'**autocertificazione** dell'operatore economico aggiudicatario attestante il possesso dei requisiti, riprendendo quanto era stato già previsto al riguardo dall'art. 75, comma 3 del D.L. n. 18 del 2020 (c.d. "Cura Italia"). Sono fatti salvi, tuttavia, gli obblighi euro-unitari di *stand still*. Per le verifiche antimafia, invece, si procede ai sensi di quanto già previsto dall'articolo 3 del D.L. n. 76 del 2020. Per ovviare alle eventuali conseguenze derivanti dall'immediata stipula del contratto, effettuata prima dell'espletamento della verifica sul possesso dei requisiti, si prevede che il contratto sia stipulato sotto condizione risolutiva, ferme restando le verifiche successive ai fini del comprovato possesso dei requisiti da completarsi entro 60 giorni.
Ai commi 3 e 4 dell'art. 53, al fine di consentire al **Dipartimento per la trasformazione digitale** della Presidenza del Consiglio dei Ministri di coordinare gli acquisti ICT finalizzati alla realizzazione del PNRR (garantendo il rispetto del cronoprogramma, la coerenza tecnologica e infrastrutturale dei progetti di trasformazione digitale), si attribuisce a quest'ultimo il potere di rendere **pareri obbligatori e vincolanti sugli elementi essenziali delle procedure di affidamento**, potendo guidare le amministrazioni aggiudicatrici con prescrizioni riguardanti l'oggetto, le clausole principali, i tempi e le modalità di acquisto.

6.E – Acquisto di strumenti informatici accessibili

Con riguardo all'obbligo di garantire l'accessibilità degli strumenti informatici, si rinvia a quanto esposto *supra* (sez. 2, lett. c). Con specifico riferimento agli acquisti *ICT*, si deve rilevare che, in considerazione di quanto disposto dall'art. 17, co. 1, lett. j-*bis* del CAD, spetta al RTD il compito di

assicurare il rispetto dei requisiti tecnici di accessibilità degli strumenti informatici, esercitando il potere di pianificazione e coordinamento degli acquisti *ICT* che la disposizione citata espressamente gli attribuisce.

Si deve ricordare in proposito che, ai sensi dell'art. 4, co. 2 della Legge "Stanca", i contratti aventi ad oggetto la realizzazione e la modifica di siti web e applicazioni mobili che non prevedono il rispetto dei requisiti di accessibilità sono sanzionati con nullità. La stessa sanzione è prevista, inoltre, in caso di rinnovo, modifica o novazione dei contratti già in essere alla data di pubblicazione delle Linee Guida AgID, laddove non si provveda all'integrazione degli stessi con apposita clausola sul rispetto dei requisiti di accessibilità.

Acquisti di beni e servizi ICT – Stato dell'arte e adempimenti del Consiglio regionale della Sardegna

Alla luce di quanto esposto, con riferimento agli obblighi in materia di infrastrutture materiali e piattaforme abilitanti posti dal Piano triennale per l'informatica 2021-2023, si rileva quanto segue.

Secondo quanto rappresentato, l'Amministrazione consiliare non ha partecipato al censimento dei *data center* promosso dall'AgID e, pertanto, presumibilmente è stata classificato nel Gruppo B. Conseguentemente, si ritiene che l'amministrazione debba provvedere alla migrazione dei propri dati e servizi verso altre infrastrutture o soluzioni.

Si ricorda che, in ottemperanza a quanto stabilito dalla strategia per le infrastrutture digitali, come declinata dal Piano triennale, le amministrazioni locali, al fine di razionalizzare le infrastrutture digitali:

• dismettono le infrastrutture di gruppo B e migrano i propri servizi verso soluzioni cloud qualificate dall'AgID;

• in alternativa, possono stringere accordi con altre amministrazioni per consolidare le infrastrutture e servizi all'interno di data center valutati affidabili e sicuri dall'AgID ai sensi della normativa vigente.

Si ricorda, inoltre, che in ossequio a quanto previsto dal recente Regolamento dell'AgID, le attività di migrazione dovranno essere precedute dal necessario censimento e classificazione dei dati e dei servizi digitali dell'ente, in osservanza del Modello definito dall'ACN d'intesa con il Dipartimento per la Trasformazione Digitale. Particolare attenzione, dunque, dovrà essere prestata ai dati classificati come critici e strategici, i quali non potranno essere ospitati su infrastrutture pubbliche munite di requisiti minimi adeguati alla classe di dati e servizi. Secondo quanto stabilito nel regolamento:

- l'elenco con la classificazione dei dati e dei servizi digitali dell'ente dovrà essere predisposto e trasmetto all'ACN entro il 18 luglio 2022 (e poi essere costantemente aggiornato);

- il piano di migrazione dovrà essere definito e trasmesso al Dipartimento per la Trasformazione Digitale entro il 28 febbraio 2023 e le attività pianificate dovranno essere completate entro il 30 giugno 2026.

Con riferimento alle infrastrutture e ai servizi *cloud* offerti da privati, si ricorda la necessità che gli uffici si sincerino sempre che i fornitori di tali servizi abbiano ottenuto la qualificazione (oggi rilasciata dall'AgID, in futuro dall'ACN) e che le dichiarazioni rese in tale sede siano veritiere. Si raccomanda di verificare anche il mantenimento della qualificazione per tutta l'esecuzione del contratto.

Per gli acquisti di strumenti informatici, poi, si raccomanda di inserire espliciti riferimenti ai requisiti tecnici di accessibilità nei contratti con i fornitori incaricati di realizzare siti web e applicazioni per conto dell'ente; analoghi riferimenti andranno inseriti nei contratti per l'approvvigionamento di postazioni di lavoro e software destinati all'utilizzo da parte di dipendenti/collaboratori con disabilità. Con riferimento alla sicurezza informatica, poi, si deve segnalare quanto previsto nel Piano Triennale 2021-2023, in cui si ribadisce che le PA, nei procedimenti di acquisizione di beni e servizi ICT devono far riferimento alle *Linee guida sulla sicurezza nel procurement ICT*[68]. Si raccomanda, inoltre, di fare riferimento alle *Linee guida per lo sviluppo del software sicuro*, sia in fase di sviluppo del software o del codice, che di adeguamento del software di base (v. *supra*, cap. 5.A).

7. VALORIZZAZIONE DEL PATRIMONIO INFORMATIVO DELLA PA

I dati costituiscono uno dei principali patrimoni digitali della pubblica amministrazione. Pertanto, la valorizzazione di questo patrimonio digitale è un obiettivo strategico perseguito in ambito sia europeo che nazionale.

La strategia di *data governance* delineata a livello nazionale si propone di sfruttare il patrimonio informativo della PA secondo due principali direttrici, che saranno oggetto di specifico approfondimento:

a) condividere i dati tra le pubbliche amministrazioni, perché possano essere utilizzati nell'ambito dei fini istituzionali propri di ciascuna amministrazione, al fine di raggiungere obiettivi di razionalizzazione dei dati, eliminando duplicazioni non necessarie, in attuazione del principio *once only* (per cui si evita di richiedere informazioni già in possesso delle PA);
b) rendere disponibili i dati della PA in formato aperto (*open data*), consentendo il riutilizzo dei dati da parte di chiunque e per qualunque scopo, anche commerciale (purché non vi siano particolari restrizioni).

[68] Le Linee guida AgID sulla sicurezza nel *procurement* ICT, adottate in via definitiva il 17 maggio 2020, sono reperibili al seguente link: https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/2013910214200__OLG_Sicurezza_Procurement_ICT_versione_finale_pub.pdf

a) Condivisione dei dati tra pubbliche amministrazioni

L'art. 50 del CAD individua gli obblighi posti a carico delle pubbliche amministrazioni volti a consentire la fruizione e il riutilizzo del patrimonio informativo pubblico.

La norma in esame, innanzitutto prevede che i dati delle pubbliche amministrazioni devono essere formati, raccolti, conservati in modo tale da renderli accessibili e disponibili, così da consentirne la fruizione e la riutilizzazione, sia alle altre pubbliche amministrazioni, che ai privati.

A tal fine, e in generale, è previsto che ciascuna amministrazione, nel rispetto della disciplina in materia di protezione dei dati personali e dei limiti al diritto di accesso stabiliti dall'art. 24 della L. n. 241/1990, rende accessibile e fruibile alle altre amministrazioni qualunque dato trattato, quando l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, senza oneri a carico di quest'ultima, eccetto quelli necessari per la prestazione di elaborazioni aggiuntive.

Ogni amministrazione, dunque, nell'ambito delle proprie funzioni istituzionali, deve poter condurre analisi dei propri dati anche in combinazione con quelli detenuti da altre amministrazioni, nonché dagli altri soggetti di cui all'art. 2, comma 2, del CAD (concessionari di pubblici servizi e società a controllo pubblico). Le modalità con cui svolgere le attività di analisi sono individuate dall'AgID nelle Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico[69].

Nell'ottica di favorire tali processi di condivisione, nonché di garantire l'attuazione del principio *once only*, l'art. 50, comma 2-*ter* (comma di recete aggiunto dal D.l. n. 34/2020, conv. con mod. dalla L. n. 77/2020) prevede che le pubbliche amministrazioni certificanti – cioè le e amministrazioni e i gestori di pubblici servizi che detengono nei propri archivi le informazioni e i dati contenuti nelle dichiarazioni sostitutive rese ai sensi del D.P.R. n. 445/2000 – ne assicurano la fruizione da parte delle pubbliche amministrazioni e dei gestori di servizi pubblici, attraverso la predisposizione di **accordi quadro** e, su richiesta del privato dichiarante, forniscono conferma scritta della corrispondenza di quanto dichiarato con le risultanze dei dati da essa custoditi.

A ciò va aggiunto che il Legislatore reca una specifica disciplina per particolari tipologie di dati. Si tratta delle basi di dati di interesse nazionale di cui all'art. 60 del CAD, ossia l'insieme delle informazioni raccolte e gestite digitalmente dalle pubbliche amministrazioni, omogenee per tipologia e contenuto e la cui conoscenza è rilevante per lo svolgimento delle funzioni istituzionali delle altre pubbliche amministrazioni, anche solo per fini statistici (tra cui, ad. es., le basi dati del casellario giudiziale, del registro delle imprese, dell'anagrafe nazionale della popolazione residente, ecc.) In tema si segnala che l'AgID, oltre alle richiamate *Linee guida per la valorizzazione del patrimonio informativo pubblico*, ha altresì adottato le *Linee guida per i cataloghi dati* [70].

Tra le basi dati di interesse nazionale, una menzione particolare merita il Repertorio Nazionale dei Dati Territoriali (RNDT), ossia il catalogo nazionale dei metadati che attengono, direttamente o

[69] Le Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico sono reperibili al seguente link: https://docs.italia.it/italia/daf/lg-patrimonio-pubblico/it/stabile/index.html.

[70] Le Linee guida per i cataloghi dati sono reperibili al link: https://docs.italia.it/media/pdf/linee-guida-cataloghi-dati-dcat-ap-it/stabile/linee-guida-cataloghi-dati-dcat-ap-it.pdf

indirettamente, a una località o area geografica specifica, istituito ai sensi del D.lgs. 32/2010 in attuazione della direttiva INSPIRE (direttiva 2007/2/CE). Le regole tecniche di popolamento del RNDT sono attualmente contenute nel DPCM 10 novembre 2011. Al riguardo, però, si segnala che è in corso la consultazione delle Linee guida AgID recanti "*regole tecniche per la definizione del contenuto del Repertorio nazionale dei dati territoriali, nonché delle modalità di prima costituzione e di aggiornamento dello stesso*"[71], le quali, una volta definitivamente approvate, sostituiranno il citato decreto.

Al fine di consentire il pieno utilizzo delle basi dati di interesse nazionale da parte delle amministrazioni, l'art. 50-*ter* del CAD prevede l'istituzione della **Piattaforma Digitale Nazionale Dati** (PDND). L'adozione di tale infrastruttura digitale è volta a migliorare e semplificare l'interoperabilità e lo scambio dei dati pubblici tra pubbliche amministrazioni, standardizzare e promuovere la diffusione degli *open data*, ottimizzare i processi di analisi dati e generazione di sapere, nonché semplificare gli adempimenti amministrativi dei cittadini e delle imprese, in conformità alla disciplina vigente e agli accordi quadro previsti dall'articolo 50.

Di recente il Decreto "Semplificazioni" (D.L. n. 76/2020, conv. con mod. dalla L. n. 120/2020) ha ridefinito la disciplina della PDND (già istituita con il D. Lgs. n. 217/2017, ma non ancora divenuta operativa), l'infrastruttura digitale di cui all'art. 50-*ter* del CAD, gestita dalla Presidenza del Consiglio dei Ministri e finalizzata a favorire l'utilizzo del patrimonio informativo pubblico per finalità istituzionali. La PDND, è previsto, ha lo scopo di assicurare l'interoperabilità dei sistemi informativi e delle basi di dati delle pubbliche amministrazioni e dei gestori di servizi pubblici, mediante l'accreditamento, l'identificazione e la gestione dei livelli di autorizzazione dei soggetti abilitati ad operare sulla stessa, nonché la raccolta e conservazione delle informazioni relative agli accessi e alle transazioni effettuate suo tramite. Rispetto alla precedente formulazione, si segnala che non è prevista l'acquisizione di dati detenuti dalle diverse amministrazioni ma, piuttosto, la loro condivisione attraverso interfacce di programmazione delle applicazioni (API). Allo sviluppo di dette interfacce provvedono i soggetti abilitati con il supporto della Presidenza del Consiglio dei ministri e in conformità alle Linee guida AgID in materia di interoperabilità[72].

In aggiunta, occorre segnalare che lo stesso Decreto "Semplificazioni" ha introdotto nel CAD anche altre importanti novità, volte ad accrescere il patrimonio informativo pubblico e ad assicurarne la condivisione.

Innanzitutto, il Decreto "Semplificazioni" ha attribuito alla Presidenza del Consiglio dei Ministri il compito di adottare – di concerto con il Ministero dell'economia e delle finanze e il Ministero dell'interno – la **Strategia nazionale dati**, nell'ambito della quale dovranno essere identificate le tipologie, i limiti, le finalità e le modalità di messa a disposizione dei dati aggregati e anonimizzati di

[71] La bozza delle Linee guida sulle regole tecniche del RNDT è consultabile al seguente link: https://geodati.gov.it/geoportale/images/struttura/documenti/LG-RNDT_v.1.0c_bozza.pdf

[72] Si segnala che di recente l'AgID, con determinazione n. 547 del 1° ottobre 2021, ha adottato le "Linee guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici" e le "Linee guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni", consultabili al seguente url: https://trasparenza.agid.gov.it/archivio28_provvedimenti-amministrativi_0_123008_725_1.html

cui sono titolari le pubbliche amministrazioni, le società a controllo pubblico e i concessionari di pubblici servizi (cfr. art. 50-*ter*, comma 4, CAD).

Un'ulteriore novità normativa di particolare rilievo concerne i **dati dei concessionari di pubblici servizi**, per i quali è previsto l'obbligo di rendere disponibili alle amministrazioni concedenti, per fini statistici e di ricerca e per lo svolgimento dei compiti istituzionali delle pubbliche amministrazioni, i dati acquisiti e generati nella fornitura del servizio agli utenti e relativi anche all'utilizzo del servizio medesimo da parte degli utenti. In particolare, l'art. 50-*quater* del CAD dispone che l'obbligo a carico dei concessionari deve essere previsto nei contratti e nei capitolati relativi all'affidamento delle concessioni. Le amministrazioni concedenti, poi, sono a loro volta tenute a rendere disponibili tali dati alle altre pubbliche amministrazioni per le medesime finalità e nel rispetto dell'art. 50 del CAD.

Infine, si segnala la recente previsione in forza della quale l'inadempimento dell'obbligo di rendere disponibili e accessibili le proprie basi dati ovvero i dati aggregati e anonimizzati – ai sensi dell'art. 50-*ter*, comma 5 – costituisce mancato raggiungimento di uno specifico risultato e di un rilevante obiettivo da parte dei dirigenti responsabili delle strutture competenti e comporta la riduzione, non inferiore al 30 per cento, della retribuzione di risultato e del trattamento accessorio collegato alla performance individuale dei dirigenti competenti, oltre al divieto di attribuire premi o incentivi nell'ambito delle medesime strutture.

b) *Open data*

L'attenzione agli *open data* delle pubbliche amministrazioni si sviluppa in ambito europeo a partire dall'adozione della direttiva (CE) 2003/98 relativa al riutilizzo dell'informazione nel settore pubblico (poi rivista dalla direttiva (UE) 2013/37) con la quale è stato introdotto l'obbligo per gli enti pubblici degli stati membri dell'UE di mettere a disposizione i propri dati e rispettivi metadati in qualunque formato e, quando possibile, in formato aperto e leggibile meccanicamente.

La direttiva (CE) 2003/98 oggi è stata abrogata e sostituita dalla direttiva (UE) 2019/1024 (relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico), che ha elevato la valorizzazione del patrimonio informativo pubblico a obiettivo strategico dell'Unione.

Questo perché la disponibilità dei dati in formati accessibili e adatti alla condivisione e al riutilizzo è in grado di contribuire al miglioramento del mercato interno, consentendo ai privati di individuare nuovi modi di utilizzarli al fine di fornire servizi nuovi e innovativi. Affinché la diffusione dei dati messi a disposizione del settore pubblico avvenga in condizioni eque e non discriminatorie, dunque, si prevede il preciso obbligo in capo agli Stati membri di formare dati di tipo aperto.

Di recente il concetto è stato ribadito nella **Strategia europea per i dati** (Comunicazione COM(2020) 66 final[73]), in cui si prevede la possibilità di un nuovo intervento legislativo europeo in materia.

[73] La Strategia europea per i dati è consultabile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

Per quanto concerne la disciplina nazionale, il Codice dell'amministrazione digitale, all'art. 1, comma 1, lett. l-*ter*, definisce i "dati di tipo aperto" come quei dati che presentano le seguenti caratteristiche:

1) sono disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato;
2) sono accessibili in formati aperti, sono adatti all'utilizzo automatico e sono provvisti dei relativi metadati;
3) sono resi disponibili gratuitamente oppure ai costi marginali sostenuti per la loro riproduzione e divulgazione (salvo quanto previsto dall'articolo 7 del decreto legislativo 24 gennaio 2006, n. 36).

Dalle sopra riportate definizioni ricaviamo che i principi propri del concetto di dato aperto sono i seguenti:

- **disponibilità e accessibilità** (i dati devono essere disponibili nel loro complesso, per un prezzo non superiore a un ragionevole costo di riproduzione, preferibilmente mediante scaricamento da internet. I dati devono essere inoltre disponibili in un formato utile ed elaborabile);
- **riutilizzo e ridistribuzione** (i dati devono essere forniti a condizioni tali da permetterne il riutilizzo e la ridistribuzione. Ciò comprende la possibilità di combinarli con altre basi di dati);
- **partecipazione universale** (tutti devono essere in grado di usare, riutilizzare e ridistribuire i dati. Non devono essere poste discriminazioni di ambiti di iniziativa in riferimento a soggetti o gruppi di persone. Per esempio, il divieto di utilizzare i dati per scopi commerciali o le restrizioni che permettono l'uso solo per determinati fini non sono contemplabili con la suddetta definizione).

Il rispetto delle caratteristiche degli *open data* dipende dalla scelta della licenza d'uso con cui i dati sono rilasciati dal suo titolare. Le possibilità di riuso dei dati pubblicati, dunque, dipendono da tale scelta. Tuttavia, la normativa stabilisce che la titolarità del dato non consente alle amministrazioni pubbliche di attuare comportamenti volti ad affermare vincoli di esclusiva che possano limitare l'accesso alle informazioni. L'amministrazione è sempre tenuta, quindi, a rendere disponibile il proprio patrimonio informativo di dati e documenti digitali con licenze di tipo aperto che consentano il riuso (anche commerciale) e la maggiore elaborazione possibile, nel rispetto esclusivamente della riservatezza dei dati personali e delle altre norme vigenti sulla confidenzialità di determinate categorie di informazioni.

In ossequio al principio di *open data by default*, enunciato dall'art. 52 del CAD, infatti, qualora vengano pubblicati contenuti digitali senza il riferimento espresso a una licenza, i contenuti si intendono rilasciati in formato aperto. Altrimenti, le licenze d'uso devono sempre essere esplicitate.

L'elencazione delle principali licenze *open* utilizzabili dalle amministrazioni per la pubblicazione dei dati aperti è stata ricostruita nelle richiamate *Linee Guida per la valorizzazione del patrimonio informativo pubblico* adottate dall'AgID. Si tratta, in particolare, di:

I. licenze con richiesta di attribuzione dei dati elaborati. Rientrano in tale categoria la licenza *CC-BY* della famiglia delle licenze internazionali *Creative Commons*, la *IODL* (*Italian Open Data License*) nella sua versione 2.0 e la *Open Data Commons Attribution License* (*ODC-BY*) per dati/*database*;

II. licenze con richiesta di attribuzione e anche con richiesta di condivisione in formato aperto dei dati elaborati. Rientrano in tale categoria la licenza *CC-BY-SA* della famiglia delle licenze internazionali *Creative Commons*, la *IODL* (*Italian Open Data License*) nella sua versione 1.0 e la *Open Data Commons Open Database License* (*ODbL*);

III. licenze c.d. "Pubblico Dominio" (come la CC 0), che non richiedono nemmeno l'attribuzione dei dati elaborati.

Valorizzazione del patrimonio informativo del Consiglio regionale della Sardegna

Alla luce di quanto esposto, con riferimento agli obblighi in materia di condivisione e riuso del patrimonio informativo della PA, si rileva quanto segue.

L'amministrazione deve adottare un proprio atto regolamentare, nell'ambito del quale disciplinare:

- le modalità per effettuare il periodico censimento del patrimonio informativo dell'Amministrazione consiliare. Al riguardo, si ricorda che, ai sensi dell'art. 53, comma 1-*bis* del CAD e dell'art. 9 del D. Lgs. 14 marzo 2013, n. 33, le amministrazioni hanno l'obbligo di pubblicare anche il catalogo dei dati e dei metadati, nonché delle relative banche dati in loro possesso e i regolamenti che disciplinano l'esercizio della facoltà di accesso telematico e il riutilizzo di tali dati e metadati;

- le licenze standard con le quali sono rilasciati i dati detenuti dall'amministrazione, da rendere esplicite in fase di pubblicazione degli stessi.

8. SANZIONI E RESPONSABILITÀ

L'omesso o incompleto adempimento delle norme sin qui citate, pur se non espressamente sanzionato, deve ritenersi immediatamente cogente, anche in virtù delle conseguenze derivanti dal mancato rispetto delle disposizioni riportate.

In particolare, sulla base dell'art. 12, comma 1-*ter*, CAD, è possibile delineare i seguenti profili di responsabilità:

- responsabilità civile e penale nel caso del mancato adempimento degli obblighi di cui alla Sezione 2 del presente documento (ad esempio, nel caso in cui – a causa della mancata nomina del Responsabile di transizione digitale o del mancato adeguamento alle misure di sicurezza – sia stato prodotto un danno a terzi);

- responsabilità civile e penale nel caso del mancato adempimento degli obblighi di cui alla Sezione 3 (ad esempio, se - a causa della scorretta digitalizzazione/conservazione di un documento – l'amministrazione dovesse perdere un contenzioso o risultare inadempiente a un obbligo di legge, societario o contabile);
- responsabilità civile per l'inadempimento delle misure di cui alla Sezione 5 (laddove non fossero garantiti agli utenti i diritti ai servizi in rete previsti dal Codice);
- responsabilità amministrativo - contabile per il danno erariale arrecato alla p.a. in tutte le numerose fattispecie in cui il rispetto delle previsioni di legge consentirebbe di conseguire notevoli risparmi (ad es. in caso di investimenti in infrastrutture immateriali o di ricorso alle comunicazioni analogiche, pur in presenza di disposizioni normative di segno contrario), nonché in caso di acquisto di strumenti informatici non conformi agli standard tecnici imposti dalla normativa (ad es. in materia di accessibilità).;
- responsabilità disciplinare per violazione degli obblighi previsti dalla legge (così, ad es., in caso di inosservanza delle disposizioni in materia di accessibilità, per espressa previsione dell'art. 9 della l. n. 4/2004 – Legge "Stanca"), dal codice di comportamento o dalle direttive impartite;
- responsabilità dirigenziale per il solo personale dirigenziale che non raggiunga i risultati posti dal vertice politico o si discosti dalle direttive impartite. Si ricorda che può costituire titolo di responsabilità dirigenziale anche l'inadempimento di disposizioni di legge, quali quelle in materia di pagamenti alla PA (in particolare, la mancata adesione a PagoPA – v. in questo documento Sezione 4, lett. b)) e in materia di accessibilità (v. art. 9 della l. n. 4/2004 – Legge "Stanca").

Sempre in tema di responsabilità dirigenziale, poi, di particolare importanza sono alcune disposizioni recentemente introdotte dal D.L. 16 luglio 2020, n. 76. Il Decreto prevede la **riduzione del 30 per cento della retribuzione di risultato e del trattamento accessorio collegato alla *performance* e il divieto di attribuire premi e incentivi, ai dirigenti responsabili,** in caso di**:**

- violazione delle disposizioni di cui agli artt. 64, comma 3 *bis* e 64-*bis* del CAD in materia di accesso telematico ai servizi;
- progettazione, realizzazione e sviluppo di servizi digitali e sistemi informatici in violazione del codice di condotta tecnologica di cui all'art. 13-*bis* del CAD;
- inadempimento dell'obbligo di rendere disponibili i dati di cui all'art. 50 del CAD.

Da ultimo, si rileva che il recentissimo D.L. 31 maggio 2021, n. 77 (convertito, con modificazioni, dalla Legge 29 luglio 2021, n. 108 – c.d. "Decreto Semplificazioni 2021"), ha introdotto nel CAD il **nuovo art. 18-*bis***, con cui sono stati rafforzati i poteri dell'AgID in materia di vigilanza, verifica, controllo e monitoraggio dell'attuazione degli obblighi di transizione digitale, nonché sono stati attribuiti alla medesima Agenzia significativi poteri sanzionatori nei confronti delle amministrazioni inadempienti.

La norma mira a rafforzare la disciplina sanzionatoria in caso di violazione degli obblighi legati alla trasformazione digitale, al fine di assicurare l'attuazione dell'Agenda digitale italiana ed europea,

nonché la digitalizzazione dei cittadini, delle pubbliche amministrazioni e delle imprese, anche in base agli obiettivi fissati dal Piano Nazionale di Ripresa e Resilienza (PNRR).

In particolare, l'Agenzia potrà procedere d'ufficio o su segnalazione del difensore civico digitale. Qualora ravvisi la violazione degli obblighi di cui alle norme espressamente indicate al comma 5 del nuovo art. 18-*bis*, potrà procedere alla contestazione e, qualora le violazioni vengano effettivamente accertate al termine della procedura, potrà comminare una sanzione amministrativa pecuniaria in misura proporzionale alla gravità della violazione accertata. In particolare, scaduti tutti i termini fissati per porvi rimedio, le amministrazioni potranno ricevere una sanzione da 10.000 a 100.000 euro.

Le violazioni sanzionabili sono relative, in particolare a:

- gli obblighi in tema di pagamenti elettronici;
- gli obblighi in tema di servizi online (consentire agli utenti di esprimere la soddisfazione rispetto alla qualità, anche in termini di fruibilità, accessibilità e tempestività, del servizio reso e pubblicare sui propri siti i dati risultanti, ivi incluse le statistiche di utilizzo);
- gli obblighi legati alla formazione dei fascicoli informatici e alla consultazione degli stessi;
- gli obblighi legati alla conservazione ed esibizione dei documenti;
- l'obbligo di rendere disponibili i dati ai sensi dell'art. 50 del CAD;
- l'obbligo di rendere disponibili e accessibili le basi dati ovvero i dati aggregati per il funzionamento della Piattaforma Digitale Nazionale Dati;
- l'obbligo di rendere accessibili i servizi tramite SPID, CIE e app IO;
- gli obblighi in materia di migrazione e razionalizzazione della spesa per i data center previsti dall'art. 33-septies del D.L. n. 179/2012.

La sanzione pecuniaria potrà essere comminata anche per la mancata ottemperanza alla richiesta di dati, documenti o informazioni effettuata dall'Agenzia nell'esercizio delle funzioni di vigilanza, verifica, controllo e monitoraggio, ovvero di trasmissione di informazioni o dati parziali o non veritieri. In questo caso, però, l'AgID potrà applicare la sanzione ridotta della metà.

Le violazioni accertate, inoltre, oltre ad essere pubblicate su un'apposita sezione del sito dell'AgID, incideranno sulla valutazione della performance individuale dei dirigenti responsabili, comportando dunque responsabilità dirigenziale e disciplinare.

Onde evitare eventuali sanzioni o contestazioni, dunque, si raccomanda di dare attuazione a quanto disposto dal Piano triennale per l'informatica 2020-2022, effettuando un periodico monitoraggio dello stato di avanzamento della *roadmap* degli adempimenti previsti dal Piano, che sarà oggetto di rilevazione da parte di AgID attraverso la raccolta di un apposito *format*.

CAPITOLO PIANO TRIENNALE	DESCRIZIONE CAPITOLO	OBIETTIVO	DESCRIZIONE OBIETTIVO	Cod.PT 2020	Cod.PT 2021	ENTE	Rif. Temporale come da PIANO TRIENNALE	PRIORITA'	INIZIO ATTIVITA' ENTE	FINE ATTIVITA' ENTE	OBIETTIVO	STATO	URGENZA	Descrizione	STATO AVANZAMENTO LAVORI ENTE gennaio 2022	REFERENTE	NOTE ENTE
6	COMPONENTI TECNOLOGICHE - SICUREZZA INFORMATICA	OB. 6.1	Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA	CAP6.PA.LA06	CAP6.PA.LA06	TUTTI	Entro dicembre 2023	PRIORITA' 5: DA CHIUDERE NEL 2023			SICUREZZA	DA PIANIFICARE	BASSA	Le PA si adeguano alle Misure minime di sicurezza ICT per le pubbliche amministrazioni aggiornate	L'ente procede con l'aggiornamento	IT-DPO	
8	GOVERNARE LA TRASFORMAZIONE DIGITALE	OB. 8.3	Migliorare i processi di trasformazione digitale e di innovazione della PA - Il monitoraggio del Piano triennale	CAP8.PA.LA31	CAP8.PA.LA31	TUTTI	Entro dicembre 2023	PRIORITA' 5: DA CHIUDERE NEL 2023			MONITORAGGIO	CONTINUATIVA	BASSA	Le PA partecipano alle attività di monitoraggio per la misurazione dei target 2022 degli Risultati Attesi del Piano secondo le modalità definite da AGID e Dipartimento per la Trasformazione Digitale - Le PA panel partecipano alle attività di monitoraggio del Piano triennale secondo le modalità definite da AGID	si procederà il prossimo anno con la scadenza	RTD	
1	COMPONENTI TECNOLOGICHE - SERVIZI	OB.1.1	Migliorare la capacità di generare ed erogare servizi digitali		CAP1.PA.LA19	Comuni con una popolazione > 15.000 abitanti, le città metropolitane, le università e istituti di istruzione universitaria pubblici, le regioni e province autonome	Entro dicembre 2023	PRIORITA' 5: DA CHIUDERE NEL 2023	N.A.	N.A.	WEB ANALYTICS	N.A.	N.A.	Almeno i Comuni con una popolazione superiore a 15.000 abitanti, le città metropolitane, le università e istituti di istruzione universitaria pubblici, le regioni e province autonome attivano Web Analytics Italia o un altro strumento di rilevazione delle statistiche di utilizzo dei propri siti web che rispetti adeguatamente le prescrizioni indicate dal GDPR	N.A.	N.A	
1	COMPONENTI TECNOLOGICHE - SERVIZI	OB.1.2	Migliorare l'esperienza d'uso e l'accessibilità dei servizi		CAP1.PA.LA22	TUTTI	Entro dicembre 2023	PRIORITA' 5: DA CHIUDERE NEL 2023			SITO WEB/APP	DA PIANIFICARE	BASSA	Le Amministrazioni adeguano i propri siti web rimuovendo, tra gli altri, gli errori relativi a 2 criteri di successo più frequentemente non soddisfatti, come pubblicato sul sito di AGID	si procederà il prossimo anno con la scadenza	RELAZIONI CON IL PUBBLICO-MKTG E COMUNICAZIONI - IT	
1	COMPONENTI TECNOLOGICHE - SERVIZI	OB.1.2	Migliorare l'esperienza d'uso e l'accessibilità dei servizi		CAP1.PA.LA23	Amministrazioni centrali, le Regioni e le province autonome, le città metropolitane e i Comuni > 150.000 abitanti	Entro dicembre 2023	PRIORITA' 5: DA CHIUDERE NEL 2023	N.A.	N.A.	SITO WEB/APP	N.A.	N.A.	Le Amministrazioni centrali, le Regioni e le province autonome, le città metropolitane e i Comuni sopra i 150.000 abitanti comunicano ad AGID, tramite l'applicazione form.agid.gov.it, l'esito dei test di usabilità del proprio sito istituzionale -	N.A.	N.A	
1	COMPONENTI TECNOLOGICHE - SERVIZI	OB.1.3	Piena applicazione del Regolamento Europeo EU 2018/1724 (Single Digital Gateway)		CAP1.PA.LA25	TUTTI	Entro dicembre 2023	PRIORITA' 5: DA CHIUDERE NEL 2023			REGOLAMENTO UE 2018/1724	DA VERIFICARE	BASSA	Le Pubbliche Amministrazioni competenti per i dati necessari all'esecuzione dei procedimenti amministrativi ricompresi nelle procedure di cui all'Allegato 16 il del Regolamento UE 2018/1724, mettono a disposizione dati strutturati ovvero dati non strutturati in formato elettronico secondo ontologie e accessibili tramite API nel rispetto delle specifiche tecniche del Single Digital Gateway. Nel caso di Pubbliche Amministrazioni che rendono disponibili i dati non strutturati, le stesse amministrazioni predispongono la pianificazione di messa a disposizione degli stessi dati in formato strutturato prevedendo il completamento dell'attività entro Dicembre 2025	si verifica e si procede in tal senso	IT	
3	COMPONENTI TECNOLOGICHE - PIATTAFORME	OB. 3.2	Aumentare il grado di adozione delle piattaforme abilitanti esistenti da parte delle pubbliche amministrazioni		CAP3.PA.LA21	TUTTI	Entro dicembre 2023	PRIORITA' 5: DA CHIUDERE NEL 2023			PIATTAFORME	DA PIANIFICARE	BASSA	Le PA aderenti a pagoPA e App IO assicurano per entrambe le piattaforme l'attivazione di nuovi servizi in linea con i target sopra descritti e secondo le modalità attuative definite nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR)	deve procedere ad aderire a IO	IT	
3	COMPONENTI TECNOLOGICHE - PIATTAFORME	OB. 3.3	Incrementare il numero di piattaforme per le amministrazioni ed i cittadini		CAP3.PA.LA22	PA centrali e i Comuni	Entro dicembre 2023	PRIORITA' 5: DA CHIUDERE NEL 2023	N.A.	N.A.	PIATTAFORME	N.A.	N.A.	Le PA centrali e i Comuni, in linea con i target sopra descritti e secondo la roadmap di attuazione prevista dal Piano Nazionale di Ripresa e Resilienza (PNRR), dovranno integrarsi alla Piattaforma Notifiche Digitali	N.A.	N.A	
3	COMPONENTI TECNOLOGICHE - PIATTAFORME	OB. 3.3	Incrementare il numero di piattaforme per le amministrazioni ed i cittadini		CAP3.PA.LA23	TUTTI	Entro dicembre 2023	PRIORITA' 5: DA CHIUDERE NEL 2023			OPEN DATA	DA PIANIFICARE	BASSA	Le PA in perimetro, secondo la roadmap di attuazione prevista dal Piano Nazionale di Ripresa e Resilienza (PNRR), dovranno integrare 90 API nella Piattaforma Digitale Nazionale Dati	Avendo limitate risorse interne, Viste le premesse, si aprirà il dialogo con Regione Sardegna per avere delle Linee Guida in merito.Si valuterà di conseguenza la definizione di un progetto ad hoc relativo all'OPENDATA : definire un PROGETTO DATI anche a livello di INTEROPERABILITA' indagare e capire creando la squadra. valutare il link e capire cosa dell'ente può essere condiviso. https://www.agid.gov.it/it/dati/basi-dati-interesse-nazionale	IT	
4	COMPONENTI TECNOLOGICHE - INFRASTRUTTURE	OB. 4.1	Migliorare la qualità dei servizi digitali erogati dalle amministrazioni locali migrandone gli applicativi on-premise (data center Gruppo B) verso infrastrutture e servizi cloud qualificati		CAP4.PA.LA15	PAL proprietarie di data center di gruppo A	Entro gennaio 2023	PRIORITA' 5: DA CHIUDERE NEL 2023	N.A.	N.A.	DATA CENTER IN CLOUD	N.A.	N.A.	Le PAL con data center di tipo "A" adeguano tali infrastrutture ai livelli minimi di sicurezza, capacità elaborativa e di affidabilità e all'aggiornamento dei livelli minimi di sicurezza, capacità elaborativa e di affidabilità che le infrastrutture devono rispettare per trattare i dati e i servizi digitali classificati come ordinari, critici e strategici come indicato nel Regolamento	N.A.	N.A	
4	COMPONENTI TECNOLOGICHE - INFRASTRUTTURE	OB. 4.1	Migliorare la qualità dei servizi digitali erogati dalle amministrazioni locali migrandone gli		CAP4.PA.LA16	PAL	Entro febbraio 2023	PRIORITA' 5: DA CHIUDERE NEL 2023			DATA CENTER IN CLOUD	DA PIANIFICARE	BASSA	Le PAL con obbligo di migrazione verso il cloud trasmettono al DTD e all'AGID i piani di migrazione mediante una piattaforma dedicata messa a disposizione dal DTD come indicato nel Regolamento	L'ente vuole indagare tra le diverse soluzioni e iniziare a predisporre il piano	IT	
4	COMPONENTI TECNOLOGICHE - INFRASTRUTTURE	OB. 4.2	Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali migrandone gli applicativi on-premise (Data Center Gruppo B) verso infrastrutture e servizi cloud qualificati (incluso PSN)		CAP4.PA.LA21	PAC con data center di tipo "A"	Entro gennaio 2023	PRIORITA' 5: DA CHIUDERE NEL 2023	N.A.	N.A.	DATA CENTER IN CLOUD	N.A.	N.A.	Le PAC con data center di tipo "A" adeguano tali infrastrutture ai livelli minimi di sicurezza, capacità elaborativa e di affidabilità e all'aggiornamento dei livelli minimi di sicurezza, capacità elaborativa e di 44 affidabilità che le infrastrutture devono rispettare per trattare i dati e i servizi digitali classificati come ordinari, critici e strategici come indicato nel Regolamento	N.A.	N.A	
4	COMPONENTI TECNOLOGICHE - INFRASTRUTTURE	OB. 4.2	Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali migrandone gli applicativi on-premise (Data Center Gruppo B) verso infrastrutture e servizi cloud qualificati (incluso PSN)		CAP4.PA.LA22	PAC	Entro febbraio 2023	PRIORITA' 5: DA CHIUDERE NEL 2023	N.A.	N.A.	DATA CENTER IN CLOUD	N.A.	N.A.	Le PAC con obbligo di migrazione verso il cloud trasmettono al DTD e all'AGID i relativi piani di migrazione mediante una piattaforma dedicata messa a disposizione dal DTD come indicato nel Regolamento	N.A.	N.A	
7	GOVERNANCE - LEVE PER L'INNOVAZIONE	OB. 7.1	Rafforzare le leve per l'innovazione delle PA e dei territori		CAP7.PA.LA10	TUTTI	Entro ottobre 2023	PRIORITA' 5: DA CHIUDERE NEL 2023			FABBISOGNI INNOVAZIONE	CONTINUATIVA	BASSA	Le PA, che ne hanno necessità, programmano i fabbisogni di innovazione, beni e servizi innovativi per l'anno 2024	La partita del procurement è complessa e il settore degli approvvigionamenti IT è strategico .si lavora per ottenere approvvigionamenti pianificati che puntino sull'innovazione	RTD E IT	
7	GOVERNANCE - LEVE PER L'INNOVAZIONE	OB. 7.1	Rafforzare le leve per l'innovazione delle PA e dei territori		CAP7.PA.LA11	PA PILOTA	Entro dicembre 2023	PRIORITA' 5: DA CHIUDERE NEL 2023	N.A.	N.A.	N.A	N.A.	N.A.	Almeno una PA pilota aggiudica un appalto secondo la procedura del Partenariato per l'innovazione, utilizzando piattaforme telematiche interoperabili	N.A.	N.A	