REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORATO AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

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

BUONE PRATICHE DI TENUTA DELLE POSTAZIONI DI LAVORO A DISTANZA

A cura di

INNOVATORI SARDEGNA

Data documento: **Marzo 2020**
File: Buone pratiche di tenuta delle postazioni di lavoro a distanza_ver_03.docx
Versione: 03

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

A cura di

INNOVATORI SARDEGNA

Sommario

1. Scopo del documento

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

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

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

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

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

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

Prioritariamente, si richiama l'esigenza di informare tempestivamente il Titolare del trattamento in caso si venisse a conoscenza di eventi di violazione dei dati – c.d. *data breach* - secondo la procedura adottata dalla Regione Sardegna con deliberazione 51/3 del 16 ottobre 2018 – disponibile al seguente link:

https://delibere.regione.sardegna.it/protected/43411/0/def/ref/DBR43382/

Si raccomanda altresì di concordare le azioni indispensabili per un collegamento sicuro con il referente informatico della struttura di appartenenza e con il supporto della Direzione degli affari generali, prima di utilizzare i propri dispositivi e in ogni caso per ogni chiarimento in merito all'utilizzo della postazione.

2. Destinatari del documento

Sono destinatari del presente documento i dipendenti dell'amministrazione regionale.
Per il loro carattere generale, le istruzioni, possono essere estese a tutti i dipendenti del sistema Regione (previo recepimento degli enti).
Per ciascun ambito trattato, si è proceduto ad una breve analisi degli specifici aspetti di rischio riguardanti il non corretto trattamento dei dati personali e la sicurezza

informatica, nonché l'applicabilità delle contromisure al contesto degli uffici regionali. In coda ad ogni scheda è stato inserito un quadro sintetico di riferimento, strutturato (ove possibile e/o pertinente) in tre punti:

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

3. Arredi e postazione di lavoro

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

4. Dispositivi personali

L'utilizzo di dispositivi personali nel luogo di lavoro è sempre stato fonte di perplessità e divieti, specialmente nella pubblica amministrazione. In realtà il fenomeno è in forte crescita e non a caso, dal 2016, è stato persino recepito dal legislatore con un'apposita

modifica del Codice dell'Amministrazione Digitale volta addirittura a favorirlo, compatibilmente "**col rispetto delle condizioni di sicurezza nell'utilizzo**"[1]. Ciò vuol dire che se da un lato l'utilizzo di dispositivi personali deve essere incentivato al fine di facilitare il lavoro, il dialogo con i cittadini-utenti e di sfruttare i benefici, anche di risparmio, che possono derivarne per l'Amministrazione, dall'altro non può esserne consentito un utilizzo indiscriminato, con conseguente compromissione della sicurezza aziendale.

Fermo restando che sarebbe preferibile utilizzare dispositivi forniti dall'Amministrazione, sui quali i sistemi di sicurezza adeguati sono già attivi e verificati con regolarità, considerata la particolare situazione di emergenza, si raccomandano le seguenti azioni prima di collegarsi ai sistemi aziendali con i propri dispositivi personali:

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

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

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

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

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

[2] Si ricorda che Microsoft non fornisce più supporto per Windows 7, comprese le patch di sicurezza, a partire dal 14 Gennaio 2020.
https://support.microsoft.com/it-it/help/4057281/windows-7-support-ended-on-january-14-2020

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

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

Rischi:

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

5. Utilizzo del dispositivo dell'ufficio, previa autorizzazione del Dirigente

Prima di prelevare il pc dalla propria postazione lavorativa, il dipendente, autorizzato ad utilizzare il dispositivo dell'amministrazione e ferma restando la necessità del supporto tecnico del referente informatico, deve seguire le seguenti raccomandazioni:

- laddove nell'hard disk siano contenute ancora cartelle di lavoro contenenti dati personali o altre categorie di dati di natura personale, il dipendente procede a trasferire le cartelle sulle cartelle condivise ovvero a privare la documentazione stessa dal riferimento di dati personali;
- adottare ulteriori misure di protezione del proprio hard disk (considerato che lo stesso è comunque protetto da credenziali di accesso) come ad esempio la cifratura, necessaria comunque in presenza di categorie di dati di natura particolare.

6. WI-FI e connessione a reti esterne

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

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

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

di accesso, comunicare dati personali, etc..) oppure sia meglio limitarsi ad effettuare operazioni semplici quali la mera navigazione o le ricerche sul web.

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

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

Rischi:

- Intercettazione di dati
- Intrusioni sui dispositivi

Rimedi per l'ufficio:

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

Rimedi per gli utenti:

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

7. Supporti di archiviazione rimovibili

L'utilizzo di supporti di archiviazione removibili (chiavette USB, hard disk portatili, CD, etc.) è una pratica comune che comporta diversi rischi. La sempre maggiore capienza dei supporti invoglia gli utilizzatori a memorizzarvi grandi quantità di dati senza procedere a cancellazioni. Col tempo, si tende a perdere memoria di cosa è contenuto

nei supporti e l'elevata miniaturizzazione aumenta il rischio di smarrimenti. La promiscuità nell'utilizzo dei supporti fa sì inoltre che questi siano bersaglio di software malevoli (virus, malware, etc.) volti a sfruttare tali dispositivi come veicolo delle infezioni, da un PC all'altro. Infine, l'affidabilità di alcuni supporti di bassa qualità non è elevata e quasi mai nota all'utente[5].

Rischi:

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

Rimedi per l'ufficio:

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

Rimedi per gli utenti:

- ridurre al minimo l'utilizzo di tali supporti;
- non utilizzare supporti removibili al di fuori di quelli forniti dall'ufficio;
- in mancanza di idonee chiavette USB fornite dall'ufficio, valutare l'affidabilità di quelle proprie anche attraverso una scansione per verificare la presenza di virus, limitando comunque l'inserimento di dati personali e utilizzando credenziali di accesso e adeguati strumenti di protezione dei dati;
- controllare periodicamente il contenuto dei supporti e procedere alla cancellazione dei contenuti obsoleti;

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

- utilizzare la rete interna dell'Amministrazione per spostare grosse moli di dati;
- preferire differenti metodi di condivisione di file per la condivisione con altri utenti interni e soprattutto esterni.

8. Posta elettronica

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

Per quanto riguarda le caselle personali o di servizio (non PEC), nonostante l'attuale *Modello Organizzativo Generale della Gestione Documentale*[6] e la circolare sul buon utilizzo della posta elettronica impongano l'utilizzo delle sole caselle istituzionali[7], ancora alcuni dipendenti inoltrano la propria corrispondenza verso caselle private (es: Gmail). Oltre a violare la regolamentazione interna, tale comportamento rappresenta una violazione del Regolamento, in quanto spesso i messaggi contengono dati personali. Tali dati finiscono per essere *trattati* da soggetti esterni all'Amministrazione (imprese, sistemi informatici, amministratori di sistema) privi di apposito incarico o contratto, spesso anche al di fuori del territorio UE. Si ribadisce, pertanto, il divieto di utilizzare strumenti diversi da quelli forniti dall'Amministrazione o reindirizzamenti a caselle di posta personali.

Rimedi per gli utenti:

- Disattivare ogni tipo di inoltro dei messaggi di posta istituzionale su proprie caselle private o non autorizzate;
- Disattivare l'anteprima dei messaggi;
- Rispettare scrupolosamente le buone pratiche di sicurezza nell'apertura dei messaggi di posta:

[6] DGR 24/27 del 14.05.2018 – Allegato 1
[7] "È vietato l'uso di altre caselle e-mail per l'invio di documenti d'ufficio e per qualsiasi altra attività che si riferisca ad informazioni e dati in possesso dell'ufficio".

- Eliminare immediatamente messaggi di posta contenenti dati personali per i quali non si è stati incaricati del trattamento. Avvisare prontamente il mittente;
- Verificare sempre l'attendibilità dell'indirizzo email del mittente rispetto al nome, nonché il contenuto e lo stile di scrittura dell'oggetto e del corpo dei messaggi;
- **Attenzione in particolare in questo periodo ai falsi messaggi riguardo l'emergenza COVID-19, in quanto sono stati riscontrati tentativi di pirateria informatica (hackeraggio) utilizzando tali modalità**;
- In caso di dubbi, non aprire immediatamente link o allegati e contattare i colleghi informatici;

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

9. Gestione di credenziali, password e autenticazione

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

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

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

password manager, che consentono una gestione professionale delle credenziali e dispongono altresì di funzionalità strettamente integrate[9] con i sistemi operativi e i dispositivi dell'utente.

Rischi:

- Smarrimento o furto di credenziali, *phishing*[10];
- Accesso abusivo a sistema informatico.

Rimedi per gli utenti:

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

10. Chat e videoconferenze

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

Il mercato, compreso quello del software libero, offre una grande quantità di applicazioni di chat e videoconferenza, anche su dispositivi mobili, ma non tutte sono adatte alle esigenze di riservatezza di una pubblica amministrazione. Nelle more di una soluzione unica fornita dall'Amministrazione regionale, si raccomanda pertanto particolare cautela nell'utilizzo di strumenti provenienti da fonti non autorevoli o di dubbia affidabilità.

Si raccomanda inoltre di prestare attenzione al fatto che la comunicazione avvenga su canali cifrati, possibilmente in modalità *end-to-end* [11], in quanto è sempre concreto il

[9] Auto completamento dei campi dei moduli, riconoscimento automatico delle URL, generazione sicura di password complesse, supporto di dispositivi hardware per la memorizzazione della master password, integrazione SSH, etc...
[10] https://it.wikipedia.org/wiki/Phishing
[11] https://it.wikipedia.org/wiki/Crittografia_end-to-end

rischio di intercettazione, da parte di terzi non autorizzati, del contenuto delle conversazioni e dei messaggi scambiati. Ciò è ancora più importante nel caso in cui si vogliano comunicare delle credenziali di autenticazione ai sistemi (cosa che andrebbe comunque fatta in maniera multicanale: es: trasmissione della username via chat/posta e della password via telefono).

Infine, in particolare per le chat, si ricorda sempre la possibilità che parte dei contenuti scambiati permanga sulle memorie dei dispositivi (temporanee e non). Pertanto, appare non raccomandabile utilizzare tali strumenti per lo scambio sistematico di documenti, per i quali sono più adatti altri canali.

Rischi:

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

Rimedi per gli utenti:

- Utilizzare soluzioni di chat e videconferenza note e affidabili;
- Utilizzare soluzioni che garantiscano riservatezza e la cifratura *end-to-end* della comunicazione. In particolare, si suggerisce l'uso dell'App *Signal*, al posto di WhatsApp[12];
- Utilizzare le chat come modalità di comunicazione veloce / occasionale, ma non per lo scambio sistematico di documenti, magari riservati;
- Evitare o ridurre al minimo la trasmissione di credenziali di autenticazione (nome utente, password, pin, etc.) su canali non sicuri. In ogni caso, separare le credenziali su più canali di trasmissione.

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

- Utilizzare periodicamente programmi di pulizia dei file temporanei dei dispositivi.

11. Cartelle condivise

Le cosiddette “cartelle condivise”, utilizzate come luogo di memorizzazione e scambio dei documenti digitali, sono uno strumento di lavoro divenuto oramai comune all’interno dell’Amministrazione. Grazie al collegamento in VPN, gli utenti impegnati nel lavoro a distanza possono accedere alle cartelle condivise in maniera analoga a come farebbero in ufficio[13].

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

In primo luogo, anche ai sensi della già citata regolamentazione regionale in materia[14], si ricorda che lo strumento principale per generare e memorizzare i documenti digitali dell’Amministrazione è il sistema SIBAR documentale. Pertanto, anche al fine di limitare la duplicazione delle banche dati, occorrerebbe ridurre al minimo la copia sulle cartelle condivise di documenti già presenti sul SIBAR. Quanto detto assume ancora più rilevanza nel caso di documenti contenenti dati personali, per i quali debbono essere garantite tutte le misure di sicurezza e di conservazione previste dalle norme di settore, che il SIBAR deve fornire già di per sé. Appare ovvio sottolineare come tali duplicati aumentino la probabilità di incorrere in diffusione impropria dei dati, mancata cancellazione e diverse tipologie possibili di *data breach*.

In secondo luogo, senza un forte controllo dell'organizzazione e dei contenuti delle cartelle stesse, al crescere dei volumi è facile perdere contezza di quanto in esse memorizzato. Questa situazione, ad esempio, impedisce di soddisfare correttamente le eventuali richieste di cancellazione di dati personali[15], oltre che di rispettare le prescrizioni in materia di *scarto* dei documenti digitali.

13 Previo coinvolgimento del supporto informatico, per realizzare gli opportuni collegamenti di rete.

14 D.G.R. n. 24/27 del 14.05.2018 - *“Modello organizzativo generale della gestione documentale regionale. Misure di adeguamento al Codice dell'Amministrazione digitale e al Regolamento europeo in materia di protezione dei dati personali.”*

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

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

Le cartelle condivise andrebbero dunque utilizzate principalmente per lo scambio temporaneo di documenti in bozza, o per la memorizzazione di copie di file di lavoro troppo grandi per essere continuamente acceduti via SIBAR (es: planimetrie, immagini, etc..). Andrebbero inoltre sottoposte a periodico svuotamento, anche forzato, della cui schedulazione dovrebbero essere informati tutti gli utenti. Nei casi in cui si trattino dati di natura particolare, è necessario utilizzarle in accoppiata alle tecniche di cifratura.

Rischi:

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

Rimedi per l'ufficio:

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

Rimedi per gli utenti:

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

12. Cloud e condivisione di documenti digitali

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

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

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

Si ricorda inoltre che dal 1° gennaio 2019 tutte le Amministrazioni hanno l'obbligo di approvvigionarsi di servizi cloud unicamente da "fornitori qualificati", secondo la

procedura formale prevista da AgID[16] e che pertanto ogni altro tipo di ricorso a cloud di terzi, al di fuori di tali regole, appare ancor più fuori norma.

Rischi:

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

Rimedi per l'ufficio:

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

Rimedi per gli utenti:

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

16 Il Cloud della PA: https://cloud-pa.readthedocs.io/it/latest/

Autori

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