Versione 1.1 del 26 ottobre 2020

**Note di redazione**

Il presente documento contiene la documentazione necessaria per disciplinare l’utilizzo da parte dei lavoratori di dispositivi elettronici personali (“Bring Your Own Device”) o, se forniti dall’organizzazione, personalizzabili per attività di carattere lavorativo, come previsto dall’art. 12 c. 3 del D Lgs. 82/2005.

In ambito di PA si tiene conto anche della Circolare 1/2020 del Ministro per la Pubblica Amministrazione.

Il documento si compone di 3 parti:

1. Istruzioni di lavoro da osservare durante le sessioni di lavoro. E’ una autorizzazione al trattamento dei dati nell’ambito dello smart working.
2. Informativa sul trattamento che il Titolare potrà fare sui dati personali dell’interessato tramite i sistemi IT di gestione dello stesso smart working.
3. Una scheda tecnica che descriva, a grandi linee, le misure adottate presso l’organizzazione del titolare per garantire la sicurezza dei dati trattati. Si compone di 3 elementi:
	1. Ambiente server (tutte le misure di sicurezza implementate sulle infrastruttura IT che supportano la gestione del lavoro agile)
	2. Ambiente client (tutte le misure adottate sulla postazione di lavoro se fornita dal titolare)
	3. Ambiente client “privato” (tutte le misure adottare sulla postazione di lavoro se fornita dall’utente)

I punti **b.** e **c.** dovrebbero essere fra loro alternativi.

La scheda tecnica deve essere tenuta agli atti per documentare le soluzioni tecnologiche implementate.

**[In azzurro sono indicati i commenti, che dovranno essere cancellati];**

**[In verde sono indicate possibili soluzioni alternative];**

**In giallo sono indicati dettagli che devono essere verificati sulla realtà contingente.**

**Il presente documento è una proposta operativa che deve essere letta attentamente e personalizzata sullo specifico contesto del Titolare, che ne ha la piena responsabilità di adozione.**

Per qualsiasi necessità correlata al presente documento e al contesto della protezione dei dati personali è possibile chiedere indicazioni al proprio Responsabile Protezione Dati.

E’ possibile chiedere ulteriori informazioni e supporto per l’implementazione di adeguate soluzioni tecnologiche al personale tecnico di SI.net.

**ISTRUZIONI DI LAVORO DA OSSERVARE DURANTE LE SESSIONI REMOTE**

**DA PARTE DEGLI OPERATORI DELL’ORGANIZZAZIONE ATTRAVERSO L’UTILIZZO DI DISPOSITIVI ELETTRONICI PERSONALI O, SE FORNITI DALL’ORGANIZZAZIONE, DI DISPOSITIVI PERSONALIZZABILI**

Viste le prescrizioni di cui all’art. 12 del D. Lgs. 82/2005, che disciplinano le norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa, si autorizza \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ al trattamento dei dati personali secondo le modalità specificate nel presente documento, in cui sono indicate le specifiche istruzioni da seguire per garantire adeguate misure tecniche ed organizzative per la sicurezza dei dati durante le sessioni di lavoro remote.

**Istruzioni specifiche sul trattamento dei dati**

Si rammenta quanto disposto dall’art. 5 del Regolamento UE 2016/679. I dati personali oggetto di trattamento devono essere

* trattati in modo lecito, corretto e trasparente nei confronti dell’interessato («liceità, correttezza e trasparenza»);
* raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all’articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
* adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
* esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
* conservati in una forma che consenta l’identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all’articolo 89, paragrafo 1, fatta salva l’attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell’interessato («limitazione della conservazione»);
* trattati in maniera da garantire un’adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Inoltre si richiama particolare attenzione ai seguenti punti, aventi specifica attinenza con la sicurezza dei dati trattati durante le sessioni remote:

* cautela in qualsiasi trattamento effettuato su dati personali;
* trattamento esclusivo dei dati necessari all’attività lavorativa, astenendosi dal trattare i dati eccedenti le finalità;
* attenzione nel garantire la confidenzialità della documentazione trattata e la messa in sicurezza dei supporti messi in dotazione dall’ente.

Inoltre occorrerà osservare scrupolosamente tutte le misure di sicurezza già in atto e quelle che saranno successivamente adottate dal titolare, nonché ogni ulteriore istruzione che sarà impartita in relazione a determinati trattamenti.

Infine si fa presente che tutte le disposizioni di futura emanazione correttive od integrative della normativa attualmente vigente in materia di protezione dei dati personali devono essere scrupolosamente osservate.

Le presenti indicazioni sono tassative.

**Utilizzo dei supporti e degli strumenti di lavoro**

**Chiavi: [qualora sia prevista anche la specifica dotazione di chiavi di accesso fisico]**

* Qualora si disponga di chiavi di accesso agli uffici e alle sedi, è obbligatorio custodirle in sicurezza e segnalare immediatamente eventuali casi di furto o smarrimento.
* I dati trattati devono essere custoditi in luoghi non accessibili a soggetti non autorizzati. La custodia in sicurezza può essere garantita attraverso la chiusura a chiave di armadi e/o interi locali.

**Documenti e supporti, analogici e digitali:**

* Durante l’attività lavorativa, è consentito solamente trattare soltanto i dati necessari, astenendosi dal trattare dati eccedenti le finalità.
* Verificare sempre che la documentazione cartacea presa in carico venga adeguatamente inventariata al momento dell’uscita dalla sede dell’organizzazione, così come venga adeguatamente tracciata la sua restituzione.
* In caso di consultazione di documenti cartacei in luoghi in cui sono presenti altri soggetti, prestare sempre attenzione che non possano essere lette, neanche accidentalmente, le informazioni ivi contenute. Prestare sempre attenzione a non mostrare in chiaro eventuali nomi presenti su documenti o fascicoli che li contengano.
* Non lasciare incustoditi in luoghi pubblici (bar, parcheggi, ecc) documenti cartacei e supporti di memorizzazione digitale.

**Strumenti di elaborazione:**

* Eventuali postazioni di lavoro portatili messe a disposizione dal titolare per lo svolgimento delle autorità lavorative vanno sempre presidiate e non vanno mai lasciate incustodite in luoghi pubblici. [qualora sia prevista la messa a disposizione di strumenti di proprietà dell’ente]
* Non lasciare incustoditi o accessibili a terzi non autorizzati la postazione di lavoro e gli strumenti elettronici mentre è in corso una sessione di lavoro.
* Accertarsi di non rendere conoscibili a soggetti indiscriminati i dati trattati, prestando attenzione che nessuno possa vedere la informazioni gestite attraverso gli strumenti di elaborazione, specie se le sessioni lavorative sono effettuate in luoghi pubblici.
* Qualora un tecnico richieda di collegarsi alla postazione di lavoro tramite strumenti di controllo remoto, è indispensabile
	+ verificare l’identità dell’operatore remoto (tramite conoscenza diretta o comunicazione preventiva)
	+ controllare se è autorizzato allo svolgimento dell’intervento (tramite preventiva apertura di ticket, autorizzazione, …)
	+ presidiare la postazione durante l’intervento, a meno che non sia stato concordato diversamente.

**Credenziali di accesso:**

* Non utilizzare password semplici, brevi e/o riconducibili alla propria realtà personale (data di nascita, nomi di parenti ecc).
* Per sistemi diversi devono essere utilizzate credenziali diverse, al fine di mitigare i rischi legati al password reuse.
* Le credenziali personali di accesso ai sistemi devono essere custodite in sicurezza (senza lasciarle scritte in prossimità della postazione di lavoro).
* Prestare sempre attenzione che altri soggetti non siano in grado di vedere le password digitate.
* Non condividere credenziali di accesso con colleghi, è fondamentale che gli utenti utilizzino credenziali assegnate in maniera univoca.

**Posta elettronica e internet:**

* Durante la navigazione su internet e la fruizione di servizi on line, non utilizzare le stesse credenziali di accesso per ambiti professionali e per contesti di carattere privato.
* Limitare al minimo la navigazione internet contemporanea per finalità private e professionali, utilizzando finestre o browser differenti per i due ambiti.
* Per la comunicazione telematica di dati e documenti di carattere professionale utilizzare esclusivamente strumenti ufficiali messi a disposizione dall’organizzazione. Astenersi tassativamente dall’utilizzo di sistemi in rete (cloud) di carattere privato per veicolare informazioni di tipo lavorativo.
* Non utilizzare le stesse password per caselle di posta private e per caselle di lavoro.
* Non utilizzare lo stesso strumento di consultazione delle caselle di posta (browser, client di posta) per le caselle private e per le caselle di lavoro.
* Non inoltrare dati e documenti di lavoro su caselle private. Qualora incidentalmente delle informazioni di carattere professionale siano state veicolate su caselle di posta private è necessario rimuoverle il prima possibile, e comunque immediatamente dopo il loro utilizzo in ambito professionale.

**Sicurezza dei contesti domestici utilizzati per attività lavorativa:**

* I dispositivi personali messi a disposizione dall’utente devono essere equipaggiati almeno con sistemi antivirus, oltre che di eventuali ulteriori sistemi di sicurezza messi a disposizione dall’organizzazione; devono inoltre essere provvisti di tutti i più recenti aggiornamenti sicurezza del sistema operativo del dispositivo utilizzato.
* E’ necessario separare tempi e contesti professionali da quelli della vita privata, limitando al minimo la convivenza di questi aspetti al fine di evitare commistioni che potrebbero comportare rischi alla riservatezza delle informazioni trattate in ambito lavorativo.
* Le postazioni di lavoro private tramite le quali si trattano dei dati per conto dell’organizzazione devono essere protette con password di accesso dedicate all’attività lavorativa; le credenziali dedicate alle attività lavorative non devono essere condivise con altri soggetti conviventi o congiunti.
* Lo scaricamento di dati e documenti correlati all’ambito lavorativo sulla postazione di lavoro locale deve attenersi al principio di necessità, limitandosi al minimo indispensabile. E’ importante ricordare che l’utilizzo in locale di documenti comporta lo scaricamento di files in cartelle specifiche (es. cartelle “Temp” dedicate a particolari programmi o cartella “download”), per cui occorre verificare l’eventuale persistenza di copie di lavoro.
* In caso di scaricamento di dati e documenti per attività lavorative sulla postazione di lavoro privata, questi devono essere localizzati in ambienti informatici protetti con password e devono persistere sulle postazioni per il tempo minimo necessario a perseguire le finalità di carattere professionale, dopo di che vanno messi in sicurezza nella rete dell’organizzazione e cancellati dalla postazione di lavoro.
* Il salvataggio di dati e documenti correlati all’ambito professionale può essere effettuato solo su supporti dedicati all’utilizzo esclusivamente lavorativo; non è consentito l’utilizzo promiscuo di supporti di memorizzazione per dati di carattere privato e di carattere professionale.

**Interazione con le strutture preposte alla gestione ICT dell’organizzazione**

* E’ necessario attenersi a tutte le istruzioni contenute nel presente documento e alle ulteriori istruzioni di carattere operativo e tecnico che l’organizzazione potrebbe fornire.
* Per tutto quanto non disciplinato nel presente documento in ambito ICT, è necessario attenersi alle prescrizioni del disciplinare di utilizzo delle risorse informatiche adottato dall’organizzazione con delibera xxx del yyy
* In caso di dubbi sul contenuto del presente documento o sull’utilizzo delle risorse tecnologiche nell’ambito delle attività remote, si raccomanda di contattare la struttura preposta scrivendo a \_\_\_\_\_\_\_\_\_\_\_\_\_ o telefonando al numero \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Rapporto con soggetti terzi**

* Prima di rilasciare documenti, dati o credenziali a soggetti terzi, verificare l’identità dei destinatari e la presenza di adeguate autorizzazioni al rilascio.
* Comunicare e/o diffondere solo i dati personali preventivamente autorizzati dal Titolare.
* In caso di richieste di informazioni o documenti confrontarsi prontamente con il referente del Titolare sul da farsi.

**Incidenti di sicurezza**

Qualora si riscontri un incidente di sicurezza sulle risorse informative o sugli strumenti dati in dotazione dal Titolare, che possa o meno sfociare in una violazione da notificare all’autorità Garante della Privacy, è necessario comunicarlo immediatamente al referente del Titolare, al fine di allestire prontamente adeguate misure di mitigazione del danno.

**Interventi di emergenza che necessitino l’utilizzo di credenziali dell’incaricato**

In caso di necessità che renda indispensabile e indifferibile intervenire con le credenziali assegnate, per esclusive necessità di garantire la continuità dei servizi e/o la sicurezza dei dati, potrà essere consentito ad un soggetto specificamente designato l’accesso ai dati ed agli strumenti informatici, tramite modifica delle password dell’utente. Non appena possibile il personale espressamente designato dal Titolare provvederà ad informare l’assegnatario delle credenziali dell’avvenuta procedura. Al suo rientro questi dovrà obbligatoriamente provvedere ad impostare nuove password di accesso.

Luogo, data \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Per presa visione \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Informativa ai sensi Regolamento UE 2016/679 per il trattamento dei dati di carattere tecnico/organizzativo effettuato nell’ambito delle attività lavorative svolte da remoto (art. 12 D. Lgs. 82/2005)**

La informiamo che i dati raccolti saranno trattati ai sensi della normativa vigente in tema di protezione dei dati personali. I dati trattati sono le credenziali di accesso al sistema da remoto (che non saranno comunque conosciute da altri soggetti, se non eventualmente nella fase di primo rilascio) [qualora vengano fornite specifiche credenziali di accesso] e il tracciamento dei tempi di sessione da remoto al sistema informativo del Titolare, limitandosi alla memorizzazione degli orari di inizio e di fine sessione. Sono inoltre tracciate le informazioni di presa in carico e di scarico di documenti e strumenti di lavoro da parte del dipendente, previste per lo svolgimento della prestazione di “lavoro agile”.

Il trattamento viene effettuato con finalità correlate alle gestione dei dati nel contesto dell’iniziativa “lavoro agile”, come previsto dalla legge 81/2017 in combinato con il DPCM 4 marzo 2020 oltre che dall’art. 12 del D. Lgs. 82/2005 (Codice dell’Amministrazione Digitale), ai sensi dall’art. 6 par. 1 lett. b) del Regolamento UE 679/2016.

I Suoi dati potranno essere trattati da soggetti privati e pubblici per attività strumentali alle finalità indicate, di cui l’organizzazione si avvarrà come responsabili del trattamento. Potranno essere inoltre comunicati a soggetti pubblici per l’osservanza di obblighi di legge, sempre nel rispetto della normativa vigente in tema di protezione dei dati personali.

Non è previsto il trasferimento di dati in un paese terzo, a meno che il trattamento non sia tutelato da specifiche clausole di salvaguardia.

Le comunichiamo inoltre che il conferimento dei dati è necessario per l’osservanza degli adempimenti di legge e l’adozione di adeguate misure tecniche e organizzative volte ad assicurare il trattamento dei dati in sicurezza, e che qualora non verranno acquisite tali informazioni non sarà possibile ottemperare agli obblighi di legge.

I dati saranno conservati per il tempo necessario a perseguire le finalità indicate e nel rispetto degli obblighi di legge previsti dalle normative.

Potrà far valere, in qualsiasi momento e ove possibile, i Suoi diritti, in particolare con riferimento al diritto di accesso ai Suoi dati personali, nonché al diritto di ottenerne la rettifica o la limitazione, l’aggiornamento e la cancellazione, oltre che al diritto di opposizione al trattamento, salvo vi sia un motivo legittimo del Titolare del trattamento che prevalga sugli interessi dell’interessato, ovvero per l’accertamento, l’esercizio o la difesa di un diritto in sede giudiziaria.

Il Titolare non adotta alcun processo decisionale automatizzato, compresa la profilazione, di cui all’articolo 22, paragrafi 1 e 4, del Regolamento UE n. 679/2016.

Ha diritto di proporre reclamo all’Autorità Garante per la protezione dei dati personali qualora ne ravvisi la necessità.

Potrà esercitare i Suoi diritti rivolgendosi al Titolare o al Responsabile della protezione dei dati, reperibili ai contatti di seguito indicati.

Il Titolare del trattamento dei dati è il \_\_\_\_\_\_\_\_\_\_\_ che Lei potrà contattare ai seguenti riferimenti:

Telefono: \_\_\_\_\_\_\_\_\_\_ – E-mail: \_\_\_\_\_\_\_\_\_\_ - Indirizzo PEC: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Potrà altresì contattare il Responsabile della protezione dei dati al seguente indirizzo di posta elettronica: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_, li \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Firma per esteso e leggibile per presa visione\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SCHEDA TECNICA ARCHITETTURA IT PER LO SMART WORKING**

**Ambiente server – misure di sicurezza adottate dal Titolare**

|  |
| --- |
| Sistema operativo e ambiente applicativo aggiornato |
| Strumenti e procedure di backup definite |
| Sistemi di sicurezza perimetrale installati e aggiornati (firewall) |
| Sistemi antimalware installati e aggiornati |
| Tracciamento delle sessioni di connessione alla rete da parte di postazioni remote |
| Cifratura delle connessioni [attraverso installazione VPN] [attraverso certificato https] [attraverso cifratura dell’applicativo di collegamento remoto] |
| Complessità password connessione al sistema [è la prima password di accesso, prima di accedere agli applicativi; descrivere la configurazione adottata, quella seguente è solo un esempio]:* Lunghezza minima 8 caratteri
* Almeno 1 lettera maiuscola, 1 minuscola, 1 carattere speciale
* Scadenza password 90 giorni
 |
| Complessità password ambiente applicativo: [descrivere la configurazione adottata, quella seguente è solo un esempio]* Lunghezza minima 8 caratteri
* Almeno 1 lettera maiuscola, 1 minuscola, 1 carattere speciale
* Scadenza password 90 giorni
 |
| Gestione Amministratori di Sistema: [descrivere la configurazione adottata, quella seguente è solo un esempio]* Tracciamento Log Amministratori di Sistema
* Lunghezza minima password 14 caratteri
* Gestione password utenze impersonali
* Elenco degli Amministratori di Sistema
 |
| Modalità di connessione all’ambiente server: [sessione terminal server] [connessione tramite programma condivisione desktop remoto <nome software>] [connessione remote dektop rdp] [accesso web] |
| Dati e documenti trattati dall’utente: [localizzati sull’ambiente server] [trattati sulla postazione di lavoro] |
| Gestione contratti con responsabili esterni (manutentori sistemi e software, gestione sicurezza) compliant con GDPR |

**Ambiente postazione di lavoro mobile – misure di sicurezza adottate dal Titolare [se fornisce la postazione di lavoro mobile]**

|  |
| --- |
| Sistema operativo e ambiente applicativo aggiornato |
| Strumenti e procedure di backup definite [se i dati sono localizzati sulla postazione di lavoro] |
| Sistemi di sicurezza perimetrale installati e aggiornati (firewall) |
| Sistemi antimalware installati e aggiornati |
| Complessità password connessione al sistema:… |
| Complessità password ambiente applicativo: *<descrivere la configurazione adottata, quella seguente è solo un esempio>** Lunghezza minima 8 caratteri
* Almeno 1 lettera maiuscola, 1 minuscola, 1 carattere speciale
* Scadenza password 90 giorni
 |
| Modalità di connessione all’ambiente server: [sessione terminal server] [connessione tramite programma condivisione desktop remoto <nome software>] [connessione remote dektop rdp] [accesso web] |
| Dati e documenti trattati dall’utente: [localizzati sull’ambiente server] [trattati sulla postazione di lavoro] |
| Gestione contratti con responsabili esterni (manutentori sistemi e software, gestione sicurezza) compliant con GDPR |
| Cifratura del notebook |

**Ambiente postazione di lavoro remota – misure di sicurezza adottate dall’utente (Bring Your Own Device) [se la postazione è dell’utente]**

|  |
| --- |
| Sistema operativo e ambiente applicativo aggiornato |
| Strumenti e procedure di backup definite (se i dati sono localizzati sulla postazione di lavoro) |
| Sistemi di sicurezza perimetrale installati e aggiornati (firewall) |
| Sistemi antimalware installati e aggiornati |
| Complessità password connessione al sistema:… |
| Modalità di connessione all’ambiente server: [sessione terminal server] [connessione tramite programma condivisione desktop remoto <nome software>] [connessione remote dektop rdp] [accesso web] [si può specificare se viene installata dal Titolare] |
| Dati e documenti trattati dall’utente: [localizzati sull’ambiente server] [trattati sulla postazione di lavoro] |
| Cifratura del notebook [se si tratta di postazione di lavoro mobile] [si può specificare se viene attivata dal Titolare] |