Perimetro Dati Personali Comuni

Questo perimetro è composto da piattaforme che trattano i Dati Personali “comuni”. «dato personale»: 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 di 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.

Per i servizi contrattualizzati che prevedono il trattamento di Dati Personali Comuni sono state definite le seguenti misure.

Laddove applicabile, all’interno del testo requisito, è indicata la corrispondente misura minima Agid soddisfatta attraverso la nomenclatura ABSC (Agid Basic Security Controll), cioè con identificatore gerarchico a tre livelli x,y.z preceduti dalla lettera M per indicare la misura come minima (**[M].x.y.z**).

ID MISURA	Categoria	Testo requisito
CdC-ICT.003.1	Canali di comunicazione	Le piattaforme e gli apparati in DC TIM sono protetti da meccanismi per la rilevazione del traffico anomalo (es. sonde di sicurezza) in grado di rilevare sia attacchi provenienti dalla rete di gruppo TIM verso le piattaforme, sia attacchi uscenti dalle piattaforme (qualora gestite da personale di TIM) verso la rete pubblica.
CdC-ICT.006.1	Canali di comunicazione	Sulle piattaforme al momento della messa in produzione del sistema, viene svolta una attività di vulnerability assessment (ingaggiando le funzioni preposte) con una metodologia di tipo non intrusivo e/o con l’utilizzo di tool automatici. La possibilità di effettuare l’attività di VA è valutata e documentata al momento della messa in produzione della piattaforma, in funzione delle possibili criticità emerse durante la fase collaudo. Qualora sulla piattaforma non sia stato svolto un VA in fase di rilascio della stessa in ambiente di esercizio, tale intervento dovrà essere pianificato dalle funzioni preposte. In ogni caso deve essere prevista la rivalutazione del VA in caso di modifiche significative della piattaforma ingaggiando le funzioni preposte.
CdC-ICT.007.1	Canali di comunicazione	Sono previsti meccanismi di protezione perimetrale (es. Firewall) delle infrastrutture e dei sistemi. Tali meccanismi ispezionano e proteggono, laddove applicabile, almeno i 3 macro-flussi: 1. dalle reti interne TIM, cliente, fornitore verso la piattaforma; 2. dalla rete pubblica Internet verso la piattaforma; 3. dalla piattaforma verso la rete pubblica Internet.
CdC-ICT.008.1	Canali di comunicazione	Sono adottate e documentate politiche di configurazione degli apparati di sicurezza (es. tipologie e direzione flussi attraverso Firewall, ecc.).
CdC-ICT.009.1	Canali di comunicazione	Nel caso vengano utilizzati accessi in VPN ai sistemi è identificabile in forma nominativa l’utilizzatore di un dato indirizzo IP (ad esempio mediante VPN client-to-lan o meccanismi di client-authentication delle sessioni).

ID MISURA	Categoria	Testo requisito
CoA-ICT.010.1	Controllo accessi	Quando il sistema utilizza la password come dispositivo di autenticazione, sono adottate misure per la protezione (ad es. cifratura) delle credenziali memorizzate a sistema (ad es. password sistemistiche ed applicative, certificati digitali). Devono inoltre essere previste misure di protezione della password (ad es. cifratura) anche quando transitano in rete e nel canale in fase di autenticazione (incluse le connessioni M2M). **[M] 5.11.1:** **[M] 5.11.2:**
PdE-ICT.010.1	Protezione degli elaboratori	La piattaforma, e le sue componenti, sviluppate internamente da TIM (o da un suo fornitore) sono dotate di software sviluppato secondo metodologie di sviluppo sicuro laddove è applicabile
AuL-ICT.008.1 AuL-ICT.008.2	Audit log	La piattaforma tramite cui è effettuato il trattamento di dati, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale da: - produrre la registrazione degli accessi logici (Access Log), compresi i tentativi falliti di accesso, effettuati da parte degli Amministratori di Sistema Addetti IT interni ed esterni - conservare le registrazioni per un periodo di sei mesi a meno di analisi del rischio che prevedano fino a 12 mesi o accordi contrattuali specifici con il cliente che prevedano tempi superiori ai 6 mesi.
AuL-ICT.009.1	Audit log	Nel caso gli End User Autorizzati si configurino come Amministratori di Sistema Software, la piattaforma tramite cui è effettuato il trattamento di Dati Personali, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa è configurata in maniera tale da: - prevedere meccanismi di registrazione degli accessi logici (access log), compresi i tentativi falliti di accesso; - conservare le registrazioni per un periodo di sei mesi.
AuL-ICT.010.1 AuL-ICT.010.2	Audit log	E' garantita la completezza, l'immodificabilità e la possibilità di verificare l'integrità delle registrazioni dei log di accesso degli Addetti IT (ad es. tramite l'invio a sistemi di Log Collecting centralizzati).
AuL-ICT.011.1	Audit log	Nel caso gli End User Autorizzati si configurino come Amministratori di Sistema Software (accesso a livello del Sistema Operativo, del Data Base, dei middleware, di tutte le componenti infrastrutturali comprese le piattaforme di back up e di manutenzione dell'Applicativo), è garantita la completezza, l'immodificabilità e la possibilità di verificare l'integrità delle registrazioni dei log di accesso all'applicativo degli stessi.
AuL-ICT.012.1 AuL-ICT.012.2	Audit log	La piattaforma tramite cui è effettuato il trattamento di dati, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale da prevedere tecnologie di sincronizzazione al fine di mantenere allineata la data e l'ora associata agli accessi registrati nei log.
AuL-ICT.013.1 AuL-ICT.013.2	Audit log	Le registrazioni dei log relativi agli accessi (access log) alla piattaforma degli Addetti IT includono le seguenti informazioni: - il sistema target e l'eventuale applicazione acceduta;

ID MISURA	Categoria	Testo requisito
		- evento che ha generato il log (login, logout, failure login); - utenza, data e ora di inizio / fine connessione. **[M] 5.1.2:**
AuL-ICT.014.1 AuL-ICT.014.2	Audit log	Nel caso gli End User Autorizzati si configurino come Amministratori di Sistema IT, le registrazioni dei log di accesso (access log) degli stessi all'applicativo includono le seguenti informazioni: - il sistema target e l'eventuale applicazione acceduta; - evento che ha generato il log (login, logout, failure login); - utenza, data e ora di inizio / fine connessione. **[M] 5.1.2:**
Bck-ICT.002.1 Bck-ICT.002.2	Back-up	Al fine di garantire la disponibilità e l'integrità dei dati è prevista la definizione e l'esecuzione di procedure di backup con cadenza almeno settimanale per i dati di configurazione e per i dati del Cliente. **[M] 10.1.1:** **[M] 10.3.1:** **[M] 10.4.1:**
CdA-ICT.002.1 CdA-ICT.002.2	Credenziali di autenticazione	Tutti i profili di accesso e le politiche di gestione delle utenze degli Addetti IT (interni ed esterni) delle piattaforme sono verificati e aggiornati. Tale verifica avviene con frequenza almeno annuale o comunque a seguito di eventi significativi (es. cambi organizzativi, evoluzioni di sistema, etc.). **[M] 5.1.1:**
CdA-ICT.003.1 CdA-ICT.003.2	Credenziali di autenticazione	Il Gestore, o un suo delegato, autorizza le utenze degli Addetti IT all'accesso ai dati nella fase di creazione, modifica o monitoraggio (gestione credenziali di accesso). **[M] 5.2.1:**
CdA-ICT.004.1 CdA-ICT.004.2	Credenziali di autenticazione	Gli amministratori di sistema sono stati formalmente nominati. **[M] 5.2.1:**
CdA-ICT.005.1 CdA-ICT.005.2	Credenziali di autenticazione	Per una gestione delle credenziali di autenticazione, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in modo tale da associare a ciascun utenza dedicata agli Addetti IT credenziali di autenticazione individuali (costituite da una User-ID e un dispositivo di autenticazione - ad es. password). La piattaforma, inoltre, deve prevedere all'accesso meccanismi automatici di verifica delle stesse. **[M] 5.10.2:**
CdA-ICT.006.1 CdA-ICT.006.2	Credenziali di autenticazione	Per una gestione delle credenziali di autenticazione, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in modo tale da associare a ciascun utenza dedicata agli End User Autorizzati credenziali di autenticazione individuali (costituite da una User-ID e un dispositivo di autenticazione - ad es. password). La piattaforma, inoltre, deve prevedere all'accesso meccanismi automatici di verifica delle stesse.

ID MISURA	Categoria	Testo requisito
		[M] 5.10.2: **[M] 5.2.1:**
CdA-ICT.007.1 CdA-ICT.007.2	Credenziali di autenticazione	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a impedire la riassegnazione di User-ID ad altri autorizzati neppure in tempi diversi. **[M] 5.10.2:**
CdA-ICT.009.1 CdA-ICT.009.2	Credenziali di autenticazione	La piattaforma è configurata in modo tale che garantisca una soluzione tecnica o procedurale che consenta, in caso di cancellazione di utenze (assegnate ad Addetti IT), di risalire in maniera certa alla persona fisica assegnataria, in un dato periodo, dell'utenza in oggetto. Tali informazioni sono conservate per almeno un periodo di 60 mesi dalla cancellazione delle utenze. **[M] 5.10.2:**
CdA-ICT.011.1 CdA-ICT.011.2	Credenziali di autenticazione	La piattaforma consente di associare le utenze degli Addetti IT ai profili rispettando i principi di "need to know" e "segregation of duties" **[M] 5.1.1:** **[M] 5.1.2:** **[M] 5.2.1:**
CdA-ICT.012.1	Credenziali di autenticazione	L'applicativo è sviluppato in maniera tale da consentire la definizione di insiemi di profili di accesso per gli End User Autorizzati che garantiscano i principi di "need to know".
CdA-ICT.013.1 CdA-ICT.013.2	Credenziali di autenticazione	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa deve essere configurata in maniera tale che effettui la verifica (almeno settimanale se eseguita tramite modalità automatiche o mensile per analisi procedurali), di tutte le utenze associate ad Addetti IT che hanno lasciato l'azienda al fine di cessare tempestivamente tutte le relative abilitazioni sulla piattaforma. **[M] 5.2.1**:
CdA-ICT.014.1 CdA-ICT.014.2	Credenziali di autenticazione	Tutte le utenze degli Addetti IT sono sottoposte a rivalutazioni periodiche circa la sussistenza delle esigenze che ne hanno portato all'attivazione. In particolare le revisioni delle utenze devono essere previste con periodicità almeno annuale **[M] 5.1.1:**
CdA-ICT.015.1 CdA-ICT.015.2	Credenziali di autenticazione	L'applicativo è sviluppato in maniera tale da prevedere meccanismi in grado di consentire l'estrazione delle informazioni necessarie alla verifica della corretta attribuzione delle credenziali di autenticazione e dei relativi profili di autorizzazione degli End User Autorizzati. **[M] 5.2.1:**
CdA-ICT.018.1	Credenziali di autenticazione	La piattaforma consente la sospensione delle utenze inattive degli End User Autorizzati a valle di periodi di inattività pari o maggiori a 6 mesi, salvo le utenze per le quali è stata preventivamente richiesta ed autorizzata una deroga sulla base di una necessità operativa.
CdA-ICT.019.1 CdA-ICT.019.2	Credenziali di autenticazione	Il gruppo in carico della creazione e della assegnazione delle credenziali di autenticazione agli Addetti IT richiedenti risulta essere nominato e costituito da un numero circoscritto di Addetti IT preventivamente individuati. **[M] 5.2.1:**

ID MISURA	Categoria	Testo requisito
CdA-ICT.020.1 CdA-ICT.020.2	Credenziali di autenticazione	E' precluso l'utilizzo di utenze di Sistema su processi automatici (ad esempio le utenze di Sistema non sono utilizzate come utenze Machine to Machine).
CdA-ICT.021.1 CdA-ICT.021.2	Credenziali di autenticazione	E' precluso l'utilizzo di utenze di sistema e M2M da parte di persone fisiche, ad eccezione di attività saltuarie (es. gestione emergenze).
CdA-ICT.022.1 CdA-ICT.022.2	Credenziali di autenticazione	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale che le utenze di sistema non nominali (comprese le M2M) devono essere comunque assegnate (in termini di responsabilità) ad una persona fisica, tipicamente un Responsabile di esercizio o un suo delegato. **[M] 5.10.2:**
CdA-ICT.023.1 CdA-ICT.023.2	Credenziali di autenticazione	Gli addetti IT a cui sono assegnate utenze deputate allo svolgimento di attività di sicurezza relative alla protezione dei sistemi (per es. configurazione regole FW o monitoraggio allarmi di sicurezza) sono distinti, a livello di singolo individuo, dagli altri addetti IT degli stessi sistemi. La separazione, a livello di singolo individuo, è applicata anche tra chi configura gli strumenti di sicurezza (es. FW o IDS) e chi svolge attività di verifica della sicurezza (es. vulnerability assessment). **[M] 5.1.1:**
CdA-ICT.024.1 CdA-ICT.024.2	Credenziali di autenticazione	Gli addetti IT a cui sono assegnate utenze deputate alla gestione dei file di log sono distinti, a livello individuale, dagli altri addetti IT dello stesso sistema. Nel caso di sistema di supporto dedicato alla gestione dei file di log non sussiste vincolo di incompatibilità con le attività di gestione sistemistica / applicativa del sistema stesso.
CdA-ICT.025.1 CdA-ICT.025.2	Credenziali di autenticazione	Per una gestione delle modalità di accesso dedicate a ciascun Addetto IT interno ed esterno, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale che quando il sistema utilizza la password come dispositivo di autenticazione, essa effettui controlli automatici volti a garantire che la password risponda alle caratteristiche previste dalle vigenti policy aziendali. **[M] 5.11.1**: **[M] 5.7.4:**
CdA-ICT.026.1	Credenziali di autenticazione	La piattaforma consente la sospensione delle utenze inattive degli Addetti IT a valle di periodi di inattività pari o maggiori a 6 mesi, (salvo le utenze preventivamente autorizzate per soli scopi di gestione tecnica per le quali sia stata concessa una deroga da parte del Gestore IT o suoi delegati). Nel caso di infattibilità tecnica il controllo può essere di tipo procedurale, con frequenza almeno mensile, garantendo comunque la sospensione trascorsi 6 mesi di inattività.
CdC-ICT.002.1 CdC-ICT.002.2	Canali di comunicazione	E' prevista l'adozione di apparati hardware e software (ad es. firewall) in grado di contrastare tentativi di accesso non autorizzato da reti dati pubbliche (Internet) al fine di rispettare i livelli di isolamento e protezione dei dati trattati dalla piattaforma stessa. **[M] 8.1.2:**
CdC-ICT.012.1 CdC-ICT.012.2	Canali di comunicazione	Per tutti i sistemi in perimetro per i quali sia consentito l'accesso al sistema da parte di entità terze/esterne all'azienda (fornitori), è garantita, salvo diversa indicazione, la sicurezza dei dati scambiati verso l'esterno (es. canali con protocolli sicuri, meccanismi di cifratura).

ID MISURA	Categoria	Testo requisito
CoA-ICT.004.1 CoA-ICT.004.2	Controllo accessi	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa prevede meccanismi automatici di verifica atti a garantire i requisiti di robustezza delle credenziali di autenticazione. A tal fine deve essere prevista l'implementazione di controlli automatici volti a garantire che le credenziali di autenticazione (per es. password) rispondano alle caratteristiche di sicurezza previste. In particolare la password deve prevedere: • lunghezza minima pari a 8 caratteri o al massimo permesso dal sistema; • complessità (la password deve essere costituita da caratteri diversi per tipologia quali lettere, numeri, simboli speciali) • diversità dalle precedenti 4 password (password history); In caso di soluzione/piattaforma destinata alla Pubblica Amministrazione (AgID ABSC Minimo): • se l'autenticazione a più fattori non è supportata, si utilizzano credenziali di elevata robustezza (almeno 14 caratteri) per le utenze da Addetto IT; • se per l'autenticazione si utilizzano certificati digitali viene garantito che le chiavi private siano adeguatamente protette. **[M] 5.7.1:** **[M] 5.7.4:** **[M] 5.11.1:** **[M] 5.11.2:**
CoA-ICT.006.1 CoA-ICT.006.2	Controllo accessi	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a richiedere la sostituzione al primo accesso delle password temporanee inizialmente assegnate a ciascun Addetto IT. **[M] 5.11.1:**
CoA-ICT.007.1 CoA-ICT.007.2	Controllo accessi	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a richiedere la sostituzione al primo accesso delle password temporanee inizialmente assegnate a ciascun End User Autorizzato. **[M] 5.11.1:**
CoA-ICT.008.1 CoA-ICT.008.2	Controllo accessi	Per una gestione delle credenziali di autenticazione dedicate a ciascun Addetto IT, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a richiedere la sostituzione periodica della password almeno ogni 6 mesi e almeno ogni 3 mesi in caso di trattamento di dati sensibili e giudiziari. **[M] 5.7.3:**
CoA-ICT.009.1	Controllo accessi	Per una gestione delle credenziali di autenticazione dedicate a ciascun End User Autorizzato al Trattamento, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a richiedere la sostituzione periodica della password almeno ogni 6 mesi nel caso di sistemi che trattano dati personali e almeno ogni 3 mesi in caso di trattamento di dati sensibili e giudiziari.
CoA-ICT.014.1 CoA-ICT.014.2	Controllo accessi	Per una gestione di base delle credenziali di autenticazione, la piattaforma IT deve essere configurata in modo tale che associ a ciascun Addetto IT un "profilo di autorizzazione" adeguato a garantire l'accesso ai soli dati che sono strettamente necessari per adempiere ai compiti affidati. **[M] 5.1.1:**

Misure adottate per la protezione dei Dati Personali Comuni

ID MISURA	Categoria	Testo requisito
Doc-ICT.002.1	Documentazione	Viene garantita l'esistenza di un elenco aggiornato degli eventuali Partner/Fornitori che concorrono all'erogazione del servizio, nella misura in cui effettivamente intervengano nel trattamento dei dati del Cliente. Tale documentazione deve riportare le seguenti informazioni: - identificativo della società esterna; - descrizione sintetica delle responsabilità affidate; - riferimento al contratto di fornitura.
PdE-ICT.003.1 PdE-ICT.003.2	Protezione degli elaboratori	La piattaforma prevede il corretto funzionamento e aggiornamento del software di protezione antivirus (prevenzione, rilevazione e rimozione virus e malicious code). Per le piattaforme non sincronizzate con l'infrastruttura antivirus aziendale l'aggiornamento deve avvenire con cadenza almeno mensile. **[M] 8.1.1:**
PdE-ICT.004.1 PdE-ICT.004.2	Protezione degli elaboratori	Al fine di minimizzare la vulnerabilità della piattaforma e garantire un livello minimo di protezione delle informazioni aziendali nelle piattaforme, sono installati, almeno annualmente, gli aggiornamenti del software applicativo (Patch Management).
PdE-ICT.005.1 PdE-ICT.005.2	Protezione degli elaboratori	Al fine di minimizzare la vulnerabilità della piattaforma e garantire un livello minimo di protezione delle informazioni aziendali nelle piattaforme, sono installati, almeno annualmente, gli aggiornamenti del software di sistema (Patch Management).
PdE-ICT.006.1 PdE-ICT.006.2	Protezione degli elaboratori	Sono state previste attività di configurazione che prevedano la modifica delle impostazioni predefinite del fornitore (ad esempio password, community SNMP, ecc...), l'eliminazione di account e servizi non necessari e la risoluzione delle vulnerabilità di sicurezza note. **[M] 5.3.1:**
PdE-ICT.007.1 PdE-ICT.007.2	Protezione degli elaboratori	Le componenti della piattaforma sono dotate di software per il quale l'azienda ha i diritti di utilizzo
PdE-ICT.008.1	Protezione degli elaboratori	Tutti i terminali utilizzati per connettersi al sistema prevedono la funzionalità di screensaver con password o in alternativa il sistema abbatte la sessione dopo 15 minuti o, qualora necessario per esigenze operative documentate, di un periodo di inattività limitato entro le 12 ore.
PdE-ICT.009.1 PdE-ICT.009.2	Protezione degli elaboratori	Per i trattamenti che prevedono l'hosting fisico dei dati all'interno di siti TIM, il sistema risiede all'interno di un Data Center, di un Service Center, di una Centrale o di un sito con equivalente livello di sicurezza fisica. Nel caso di trattamenti in siti di terze parti devono essere previste e applicate politiche e misure per stabilire e mantenere il medesimo livello di sicurezza fisica in linea con quanto già previsto dalle policy e procedure aziendali specifiche.
PdE-ICT.012.1 PdE-ICT.012.2	Protezione degli elaboratori	E' prevista l'adozione di procedure documentabili e/o tecnologie che consentano la gestione sicura e protetta del codice sorgente del programma. Inoltre i codici sorgente non risiedono sui server in esercizio, se non risultano necessari alla normale operatività del sistema.
Ris-ICT.008.1 Ris-ICT.008.2	Riservatezza	E' prevista la stesura e la corretta implementazione di procedure atte a regolare il processo di cancellazione dei dati del cliente a seguito della cessazione del contratto (ad es. cessazione di qualsiasi obbligazione derivate da accordi contrattuali oppure in applicazione di specifiche normative) assicurando che tali dati vengano cancellati in maniera definitiva e irreversibile al fine di impedire trattamenti non autorizzati degli stessi da parte di Addetti IT o di eventuali altri Clienti. Le tempistiche di cancellazione sono in linea con quanto previsto a livello contrattule.

ID MISURA	Categoria	Testo requisito
Ris-ICT.009.1	Riservatezza	E' garantito l'isolamento logico dei dati relativi a clienti differenti su una medesima piattaforma. In particolare non deve essere possibile accedere/visualizzare i dati di un Cliente diverso da quello che ha acceduto alla piattaforma.
Ris-ICT.010.1	Riservatezza	E' prevista la separazione degli ambienti dedicati alle attività di sviluppo, test e collaudo dall'ambiente di esercizio della piattaforma. Per gli ambienti diversi da quello di produzione nel caso vengano utilizzati dati reali di esercizio, sono garantiti tutti i requisiti di compliance previsti.
Ris-ICT.011.1	Riservatezza	E' prevista la redazione formale di apposite procedure di estrazione o trasmissione dei dati trattati dalla piattaforma. Tali estrazioni/trasmissioni devono consentire la portabilità dei dati tramite l'esportazione degli stessi in formati standard in relazione alla tecnologia utilizzata (ad es. sistemi di tipo UNIX) e al layer di trattamento (ad es. DB).