Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

REDATTO:	SIGLA	CE.PS/C
VERIFICATO/APPROVATO	SIGLA	CE.PS/C
LISTA DI DISTRIBUZIONE:	il presente documento viene distribuito alla funzione di Vendita interessata MEB-M/C.ALTU, al Cliente e, in caso di accettazione, alla funzione Procurement, a tutte le mandanti del RTI ed ai loro fornitori	
TIPO ATC	**Raggruppamento Temporaneo di Imprese**	

Il presente documento è stato redatto in coerenza con il Codice Etico e di Condotta ed il Modello Organizzativo 231 del Gruppo Telecom Italia

TIM S.p.A.

Sede legale: Via Gaetano Negri, 1 - 20123 Milano
Sede secondaria e Direzione Generale: Corso d'Italia, 41 - 00198 Roma
Casella PEC: telecomitalia@pec.telecomitalia.it

Codice Fiscale/P. IVA e Iscrizione al Registro delle Imprese di Milano: 00488410010
Iscrizione al Registro A.E.E. IT08020000000799
Capitale Sociale € 11.677.002.855,10 interamente versato

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

Sommario

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

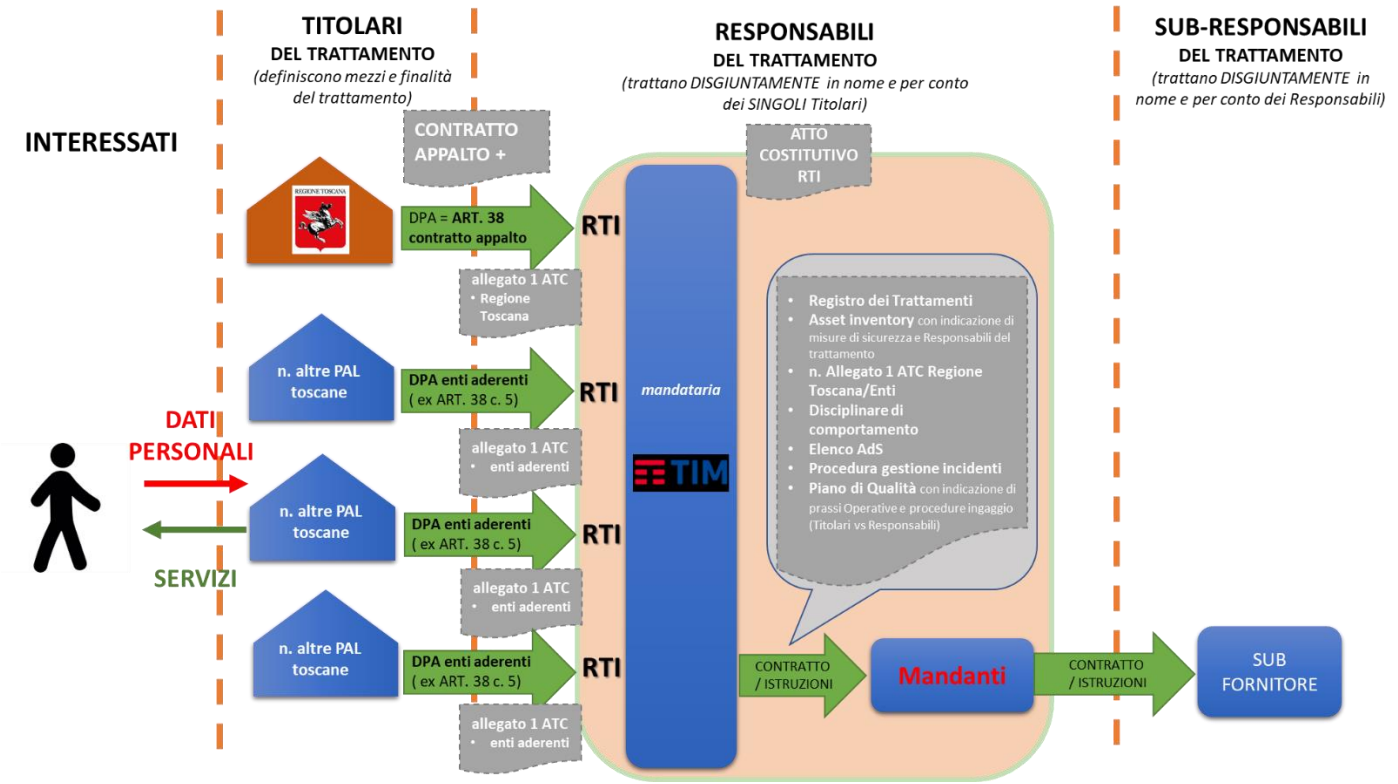
1. REGISTRAZIONE MODIFICHE DOCUMENTO

La tabella seguente riporta la registrazione delle modifiche apportate al documento.

DESCRIZIONE MODIFICA	VERSIONE	DATA
Prima emissione	1	29/11/2019
Inserito schema ambito di applicazione, dettaglio sulle categorie di interessati e rimando al repository per trattamenti e misure di sicurezza.	2	21/05/2020
Inserimento Kyndryl Italia in qualità di mandante del RTI	3	09/07/2022

2. AMBITO DI APPLICAZIONE

Il presente documento si applica a tutti i Titolari del Trattamento e a tutti i componenti la RTI come di seguito schematizzato.



3. ALLEGATO TECNICO DI COMPLIANCE

Per inquadrare la logica, condivisa con Regione Toscana, con cui è stato predisposto il documento, si descrive nel seguito la struttura del Registro dei Trattamenti dei Titolari a cui TIM collabora per la tenuta e l'aggiornamento delle informazioni:

Registro dei Trattamenti dei Titolari:

- Traccia la nomina avvenuta da parte di uno o più Titolari ed identifica le società (Mandataria, Mandanti, Subfornitori) nominate a vario titolo Responsabili e Sub-Responsabili del Trattamento.
    - Per il dettaglio sull'articolazione degli specifici trattamenti, tipo dati, livello di criticità, il registro rimanda all'Asset Inventory SCT alimentato con le informazioni la cui responsabilità è dei singoli Titolari.

Per le misure di sicurezza da adottare sui vari Asset il Registro rimanda all'Allegato Tecnico di Compliance (ATC)

Allegato Tecnico di Compliance (ATC)

- Identifica le adeguate e preventive misure di Sicurezza e Compliance tecniche ed organizzative da applicare sui vari Asset associando le stesse in base al livello di criticità del dato trattato ed alla tipologia di Asset;
- Il presente documento è richiamato nelle lettere di nomina a Responsabili del trattamento delle Mandanti e degli eventuali loro Subfornitori (Sub-Responsabili) in modo da condividere all'interno dell'RTI una comune Politica di Applicazione della Sicurezza e della Compliance.

Asset inventory SCT

Oltre alle specifiche informazioni tecniche, l'Asset Inventory, alimentato con le informazioni fornite da ciascun Titolare del trattamento, per ciascun Asset, permetterà di identificare:

- Categoria di Interessati e loro numerosità, categoria di Dati Personali,
- Trattamenti previsti (es. Gestione Sistemistica, backup, Gestione DB, etc..)
    - Per ogni trattamento, l'Asset identifica il Responsabile e/o Responsabili a cui sono assegnati i trattamenti previsti nell'ambito del contratto e della rispettiva nomina
        - Per ogni responsabile viene identificato il personale Autorizzato al trattamento /Amministratori di Sistema (AdS)

La **relazione tra l'Asset Inventory SCT ed il Registro dei Trattamenti del Titolare** permetterà di:

- Associare le applicazioni all'Asset infrastrutturale (anche nel caso in cui non siano in gestione all'RTI)
- Associare eventuali altri Responsabili del trattamento nominati direttamente da ciascun Titolare (es. loro fornitori applicativi)

Allo scopo si prevede di integrare le informazioni presenti nel Registro Trattamenti di Regione Toscana con le informazioni dell'Asset Inventory SCT utilizzando una copia del Registro Trattamenti di Regione Toscana (**Registro Trattamenti SCT**).

Il Registro Trattamenti SCT sarà analogamente utilizzato dalla RTI anche per tracciare i propri trattamenti afferenti ad altri Enti Titolari Aderenti al SCT diversi da Regione Toscana.

Atti di Nomina (DPA)

- Formalizzare gli atti di nomina (DPA) che riportano le Istruzioni e le misure di sicurezza di carattere generale e rimandano all'ATC per le misure di dettaglio.

L'ATC rappresenterà quindi un documento ufficiale sia verso il Titolari del Trattamento che verso il Responsabile del Trattamento.

Nelle prime tabelle del paragrafo successivo vengono raccolti i dati di riferimento per le due figure presentate.

Nella tabella al paragrafo 1.1 sono riportate le tipologie di dati ed i tipi di trattamento su cui il Responsabile è coinvolto nell'erogazione del servizio.

Nelle tabelle al paragrafo 2, sono riportate le misure tecniche ed organizzative adeguate di Sicurezza e Compliance che il Responsabile si impegna ad applicare, differenziate in base alla classificazione a cui appartiene il dato personale trattato dall'asset.

Il dettaglio e la relazione intercorrente tra il trattamento agito, le categorie di interessati, dati personali coinvolti, nonché le conseguenti misure applicate sarà tracciato nell'Asset Inventory.

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

4. ANAGRAFICA TITOLARE, RESPONSABILI, TIPO INTERESSATI, TIPO DATI, TIPO TRATTAMENTI

Anagrafica Titolare del Trattamento

Titolare del trattamento: Ragione Sociale	AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO
Referente Cliente ("Referente DPO se disponibile" o referente tecnico)	
Nome Referente	Mario
Cognome Referente	Arcella
Email	dpo@dsu.toscana.it
Cellulare	335 5790043
Telefono	

Anagrafica TIM - Mandataria RTI

Fornitore	
Fornitore: Ragione Sociale	**TIM Spa**
Codice Fiscale /Partita IVA	00488410010
Rappresentante per Fornitori extra UE	
Mail Rappresentante per Fornitori extra UE	

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

Anagrafica BV Tech - subfornitore di TIM:

Fornitore	
Fornitore: Ragione Sociale	**BV Tech Spa**
Codice Fiscale /Partita IVA	05009770966
Rappresentante per Fornitori extra UE	
Mail Rappresentante per Fornitori extra UE	

Anagrafica IBM Italia Spa - mandante RTI:

Fornitore	
Fornitore: Ragione Sociale	**IBM Italia Spa**
Codice Fiscale /Partita IVA	10914660153
Rappresentante per Fornitori extra UE	
Mail Rappresentante per Fornitori extra UE	

Anagrafica Sistemi Informativi Srl– subfornitore di IBM

Fornitore	
Fornitore: Ragione Sociale	**Sistemi Informativi Srl**
Codice Fiscale /Partita IVA	01528071002
Rappresentante per Fornitori extra UE	
Mail Rappresentante per Fornitori extra UE	

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

Anagrafica Enterprice Services S.p.A. - mandante RTI:

Fornitore	
Fornitore: Ragione Sociale	Enterprise Services Italia S.r.l.
Codice Fiscale /Partita IVA	12582280157
Rappresentante per Fornitori extra UE	
Mail Rappresentante per Fornitori extra UE	

Anagrafica Lutech Spa - mandante RTI:

Fornitore	
Fornitore: Ragione Sociale	Lutech Spa
Codice Fiscale /Partita IVA	02824320176
Rappresentante per Fornitori extra UE	
Mail Rappresentante per Fornitori extra UE	

Anagrafica Dedalus Italia Spa - mandante RTI:

Fornitore	
Fornitore: Ragione Sociale	Dedalus Italia Spa
Codice Fiscale /Partita IVA	05994810488
Rappresentante per Fornitori extra UE	
Mail Rappresentante per Fornitori extra UE	

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

Anagrafica Kyndryl Italia Spa - mandante RTI:

Fornitore	
Fornitore: Ragione Sociale	Kyndryl Italia Spa
Codice Fiscale /Partita IVA	11628710961
Rappresentante per Fornitori extra UE	
Mail Rappresentante per Fornitori extra UE	

ELENCO TIPI DATI E TRATTAMENTI PREVISTI

Elenco Tipologia Dati e Categoria dei Trattamenti oggetto della nomina				
Nome Soluzione (Tipologia soluzione Standard, Personalizzata o Custom)	**Categorie di Interessati cui i Dati sono trattati (Perimetro di Compliance)**	**Categorie di Dati Personali Trattati (Perimetro di Compliance)**	**Categorie di Trattamenti - Responsabili dei Trattamenti**	**Ubicazione piattaforma e dati trattati**
Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana Soluzione Custom	Tutti i dipendenti e gli utenti dei sistemi informativi del Titolare ospitati nel "community cloud" compresi i minori Tutti i cittadini italiani* censiti nei sistemi informativi del Titolare ospitati nel "community cloud" Tutti gli utenti* (cittadini italiani, comunitari e non) del SST - Servizio Sanitario Toscana ospitato nel "community cloud"	Dati Personali Comuni Dati particolari (già dati sensibili) e dati personali relativi a condanne penali e reati Dati particolari relativi alla Salute Dati particolari "Fascicolo Sanitario Elettronico / Dossier Sanitario" Perimetro Dati particolari biometrici o genetici Perimetro Portali Web Perimetra scambi dati tra PA Perimetro PA (Misure Agid) Perimetro Energetico Perimetro Dati di Localizzazione	Per le categorie di trattamento e i relativi Responsabili del trattamento si rimanda all'Asset Inventory	DC Regione Toscana (SCT-RT), Firenze

* i trattamenti di queste categorie di Interessati vengono effettuati su larga scala e comprendono dati di minori e categorie particolari di dati personali.

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

5. ALLEGATO TECNICO "REQUISITI DI SICUREZZA E COMPLIANCE"

GLOSSARIO: Nelle misure di sicurezza sono riferiti i seguenti ruoli:

- Gestori IT: Il Gestore è il responsabile della gestione tecnica (sviluppo, esercizio, manutenzione, aggiornamento, ecc.) di un sistema ICT
- Addetti IT: I soggetti autorizzati al trattamento, destinatari di utenze di accesso amministrativo (AdS), preposte alla gestione sistemistica o applicativa della piattaforma. Possono essere interni o esterni al Gestore IT (suoi dipendenti o Fornitori); sono sottoposti anche al rispetto del provvedimento dell'Autorità di Controllo del 27.11.2008 (G.U. n. 300 del 24.12.2008 e smi).
- End-User Autorizzati: Utilizzatori finali del servizio IT (ad es. dipendenti del Cliente) caratterizzati da utenze di accesso all'Applicativo, autorizzati al trattamento da parte del Titolare, cioè il Cliente business a compiere operazioni di trattamento sui dati gestiti dall'applicativo. Possono assumere anche il ruolo di Amministratore dell'Applicativo (AdS); in tal caso sono sottoposti anche al rispetto del provvedimento dell'Autorità di Controllo del 27.11.2008 (G.U. n. 300 del 24.12.2008 e smi).
- End-User interessati: Rappresentano i soggetti cui si riferiscono i dati personali gestiti dall'applicativo e che possono eventualmente essere anche utilizzatori finali del servizio IT; in tal caso sono assegnatari di utenze di accesso all'Applicativo di tipo non amministrativo, con profili ristretti ai dati di propria competenza. Sono i soggetti i cui diritti sono tutelati dal Regolamento UE 2016/679 (GDPR).

PERIMETRO "231/REATI INFORMATICI" E/O PERIMETRO DATI PERSONALI COMUNI

Questo perimetro è composto da piattaforme che:

- non trattano dati personali. Il Modello Organizzativo e la relativa Policy prevedono una rilevanza a medio rischio reato D.Lgs 231/01 – Reati informatici.
- 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.

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

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

ID MISURA	Categoria Mimip	Testo requisito
CdC-ICT.003.1	Canali di comunicazione	Le piattaforme e gli apparati in DC SCT sono protetti da meccanismi per la rilevazione del traffico anomalo (es. sonde di sicurezza) in grado di rilevare sia attacchi provenienti dalla rete Regione Toscana (RT) verso le piattaforme, sia attacchi uscenti dalle piattaforme 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 RT, 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).
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). **[M] 5.11.1:** **[M] 5.11.2:**
PdE-ICT.010.1	Protezione degli elaboratori	La piattaforma, e le sue componenti 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.

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

ID MISURA	Categoria Mimip	Testo requisito
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	È 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; - 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:**

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

ID MISURA	Categoria Mimip	Testo requisito
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 ciascuna 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 ciascuna 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. **[M] 5.10.2:** **[M] 5.2.1:**

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

ID MISURA	Categoria Mimip	Testo requisito
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.

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

ID MISURA	Categoria Mimip	Testo requisito
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:**
CdA-ICT.020.1 CdA-ICT.020.2	Credenziali di autenticazione	È 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	È 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:**

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

ID MISURA	Categoria Mimip	Testo requisito
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	È 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).
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:**

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

ID MISURA	Categoria Mimip	Testo requisito
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:**
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	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).

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

ID MISURA	Categoria Mimip	Testo requisito
PdE-ICT.005.2		
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
PdE-ICT.009.1 PdE-ICT.009.2	Protezione degli elaboratori	Per i trattamenti che prevedono l'hosting fisico dei dati all'interno del DC SCT, il sistema risiede all'interno di un Data Center, di un Service Center, di una Centrale o di un sito equivalente.
PdE-ICT.012.1 PdE-ICT.012.2	Protezione degli elaboratori	È 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	È 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 contrattuale.
Ris-ICT.009.1	Riservatezza	È 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	È 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.

ID MISURA	Categoria Mimip	Testo requisito
Ris-ICT.011.1	Riservatezza	È 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).

PERIMETRO CATEGORIE PARTICOLARI DI DATI (GIÀ DATI SENSIBILI) E DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI

Composto dalle piattaforme che trattano Dati Personali Sensibili o Giudiziari. In particolare, di seguito si riporta la definizione di tali tipologie di dati:

- Categorie particolari di dati (già dati sensibili) –dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- Dati personali relativi a condanne penali– Dati personali relativi a condanne penali e reati.

L'appartenenza di una piattaforma a tale perimetro prevede necessariamente l'inclusione della stessa anche all'interno dei Perimetri 231 e Dati Personali.

ID MISURA	Categoria Mimip	Testo requisito
Bck-ICT.001.1	Back-up	È prevista la redazione di procedure documentate di ripristino/restore dei dati (e di configurazione se previsto dal contratto). Tali procedure di ripristino dell'accesso ai dati garantiscono tempi non superiori a sette giorni qualora tutti i dati utilizzati dal sistema andassero persi.

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.
PdE-ICT.001.1	Protezione degli elaboratori	Vengono installati, almeno semestralmente, gli aggiornamenti del software di sistema operativo necessari a correggere difetti e prevenire vulnerabilità della piattaforma.
PdE-ICT.002.1	Protezione degli elaboratori	Vengono installati, almeno semestralmente, gli aggiornamenti del software di DBMS e applicativo oggetto del SaaS, necessari a correggere difetti e prevenire vulnerabilità della piattaforma.
Ris-ICT.002.1	Riservatezza	Sono previste soluzioni (es. cifratura o altre) che, considerato il numero e la natura dei dati trattati, rendono i dati sensibili o giudiziari temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. In particolare la misura deve essere prevista qualora: - rientrino nelle responsabilità della fornitura del servizio le funzionalità applicative (es. SAAS), e le finalità del servizio prevedano (in quanto sostanziale per la finalità e non occasionale) il trattamento dei dati sensibili o giudiziari; - rientrino nelle responsabilità della fornitura del servizio infrastrutturale (IAAS) e il Cliente espliciti la necessità di trattare dati sensibili o giudiziari e richieda formalmente l'espletamento di tale misura a livello infrastrutturale.
Sup-ICT.001.1	Supporti	È prevista la definizione e l'attuazione di procedure di cancellazione fisica (ad es. tramite Wiping o Degaussing) a seguito della dismissione o della diversa assegnazione d'uso (ad es. utilizzo da parte di un cliente differente) di elaboratori o supporti utilizzati, al fine di garantire l'inaccessibilità "assoluta" agli stessi.

PERIMETRO DATI PARTICOLARI RELATIVI ALLA SALUTE

Composto dalle piattaforme dedicate a clienti quali organismi sanitari o esercenti le professioni sanitarie che intendono utilizzare il servizio per trattare categorie particolari di dati (dati idonei a rivelare lo stato di salute e/o la vita sessuale degli interessati).

Per dati relativi alla salute (Rif. [4]) s'intendono i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

L'appartenenza di una piattaforma a tale perimetro prevede necessariamente l'inclusione, minima, della stessa anche all'interno del Perimetro 231, Dati Personali e Perimetro Dati Sensibili / Giudiziari.

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

ID MISURA	Categoria Mimip	Testo requisito
Ris-ICT.001.1	Riservatezza	Nella piattaforma è prevista al fine di garantire la riservatezza dei dati sanitari conservati (data-at-rest), la cifratura degli stessi o l'utilizzo di codici identificativi o di altre soluzioni che li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. In caso di trasmissione dei dati sanitari è garantita in ogni caso la cifratura dei dati.

PERIMETRO DATI PARTICOLARI "FASCICOLO SANITARIO ELETTRONICO / DOSSIER SANITARIO"

Composto dalle piattaforme che consentono il trattamento di categorie particolari di dati tramite FSE / Dossier Sanitario. Tali insiemi di dati si differiscono dal semplice dato particolare riferito alla salute in termini di condivisione delle informazioni e di titolarità dei dati, come da definizioni di seguito riportate:

- Fascicolo sanitario elettronico (Fse) – insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito (cfr. Allegato C - Definizioni alle Linee guida in materia di Dossier sanitario del 4 giugno 2015). In particolare, per Fse si intende il fascicolo formato con riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale (es. azienda sanitaria, laboratorio clinico privato operanti nella medesima regione o area geografica);
- Dossier Sanitario – insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, messi in condivisione logica dai professionisti sanitari che lo assistono, al fine di documentarne la storia clinica e di offrirgli un migliore processo di cura. Tale strumento è costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es. ospedale o clinica privata) al cui interno operino più professionisti (cfr. Allegato C - Definizioni alle Linee guida in materia di Dossier sanitario del 4 giugno 2015). In particolare, si parla di dossier sanitario qualora tale strumento sia costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es. ospedale o clinica privata) al cui interno operino più professionisti. I dossier sanitari possono anche costituire, ad esempio, l'insieme di informazioni sanitarie detenute dai singoli titolari coinvolti in una iniziativa di Fse regionale.

L'appartenenza di una piattaforma a tale perimetro prevede necessariamente l'inclusione della stessa anche all'interno del Perimetro 231, Dati Personali, Perimetro Dati particolari Sensibili / Giudiziari e Perimetro particolari relativi alla salute.

ID MISURA	Categoria Mimip	Testo requisito
Ris-ICT.014.1	Riservatezza	L'applicativo è costruito in maniera tale da permettere l'oscuramento (revocabile nel tempo) di taluni dati o documenti sanitari a seguito di richieste dell'interessato. Le informazioni oscurate sono in ogni caso rese disponibili al professionista sanitario o alla struttura interna titolare che li ha raccolti o elaborati. L'oscuramento dell'evento clinico avviene con modalità tali da garantire che i soggetti abilitati all'accesso non possano venire automaticamente a conoscenza del fatto che l'interessato ha effettuato tale scelta.
Ris-ICT.015.1	Riservatezza	L'applicativo deve essere costruito in maniera tale da permettere la gestione del consenso al trattamento da parte dell'interessato. L'applicativo consente di raccogliere le informazioni e renderle disponibili e visualizzabili esclusivamente a un sottoinsieme di utenze definito dal Cliente business. In caso di revoca dello stesso il Dossier/Fse non è ulteriormente implementato. Le informazioni sanitarie già presenti restano disponibili e visualizzabili esclusivamente alla funzione interna del Cliente che le ha raccolte (non sono più condivise con i professionisti di altri reparti).

Di seguito i requisiti aggiuntivi da valutare col cliente per adeguarsi alla normativa:

ID MISURA Circolare 263	Categoria Mimip	Testo requisito
	Log	L'applicativo è costruito in maniera tale da prevedere la possibilità di implementare meccanismi di tracciamento degli accessi e delle operazioni di trattamento del Dossier/FSE effettuate da tutte le utenze autorizzate. Tali ulteriori registrazioni, in accordo con le richieste del Cliente, sono definite contrattualmente e messe a disposizione del Cliente al fine di poter rispondere ad eventuali richieste di visione da parte degli interessati. In particolare, i file di log registrano per ogni operazione di accesso ai Dossier, almeno le seguenti informazioni: l'utenza, la data e l'ora di effettuazione delle operazioni, il codice della postazione di lavoro utilizzata, l'identificativo del paziente il cui Dossier è interessato dall'operazione e la tipologia dell'operazione compiuta. La gestione di tale tracciamento garantisce la conservazione delle registrazioni per un periodo non inferiore a 24 mesi ed avvenire in accordo alle disposizioni interne previste per tale trattamento

	Log	L'applicativo è costruito in maniera tale da prevedere la possibilità di implementare alert e meccanismi di anomaly detection che individuino comportamenti anomali o a rischio (che possano configurare trattamenti illeciti) relativi alle operazioni eseguite dagli incaricati del trattamento (ad es. relativi al numero degli accessi eseguiti, alla tipologia o all'ambito temporale degli stessi), al fine di orientare successivi ed eventuali interventi di Audit interno da parte del Cliente titolare del trattamento.
	Riservatezza	L'applicativo è costruito in maniera tale da consentire la gestione di un autonomo e specifico consenso dell'interessato al trattamento tramite Dossier/Fse di particolari tipologie di informazioni. Trattasi di informazioni relative a prestazioni sanitarie offerte a soggetti nei cui confronti l'ordinamento vigente ha posto specifiche disposizioni a tutela della loro riservatezza e dignità personale (ad es. infezioni da HIV).

PERIMETRO PORTALI WEB

Composto dalle piattaforme che realizzano Portali / Siti web che utilizzano cookies per la navigazione libera di utenti generici attraverso l'utilizzo dei browser HTTP di navigazione Internet.

I cookie (file di informazioni che i siti web memorizzano sul computer dell'utente di Internet durante la navigazione), si suddividono in:

- Cookie Tecnici – Necessari per effettuare la navigazione in rete o per fornire servizi esplicitamente richiesti dall'utente, sono da considerarsi cookie tecnici, i cookie di autenticazione (utili anche per mantenere attiva la connessione ad aree riservate durante la navigazione attraverso le pagine del sito senza la necessità di reinserire User-Id e password), quelli di sicurezza (numero di login falliti), funzionali (utilizzati per memorizzare informazioni specifiche riguardanti gli utenti stessi, tra cui le preferenze, come ad esempio la lingua, il tipo di browser e di computer usato, il contenuto del "carrello della spesa"), per bilanciare le richieste utente, di sessione (per migliorare la fruibilità del sito), per la gestione dei contenuti multimediali (per archiviare dati tecnici);
- Cookie di Profilazione – Monitorano il comportamento degli utenti durante la navigazione in rete al fine creare profili relativi all'utente (sui suoi gusti, abitudini, scelte, ecc.) e vengono utilizzati soprattutto al fine di inviare messaggi pubblicitari personalizzati;
- Cookie analytics (analitici) – Utilizzati per rilevare a livello statistico gli utenti unici e su come hanno visitato il sito. Sono assimilati ai cookie tecnici laddove utilizzati direttamente dal gestore del sito (di prima parte) ed utilizzati solo per la suddetta finalità; a queste condizioni, sono detti cookie analytics di "prima parte" per i quali valgono le stesse regole previste per i cookie tecnici (cioè è sufficiente l'informativa). Invece, per i cookie analytics di "terze parti" (es. Google analytics) è necessario fornire l'informativa e raccogliere il consenso dell'utente; il consenso non necessario solo se sono adottati strumenti che riducono il potere identificativo (anonimizzazione anche parziale dell'IP dell'internauta del cookie) e la terza parte garantisce che non incrocia le informazioni con altre di cui già dispone.

L'appartenenza di una piattaforma a tale perimetro prevede necessariamente l'inclusione della stessa anche all'interno del Perimetro 231/01 reati informatici e del Perimetro Dati Personali.

ID MISURA	Categoria Mimip	Testo requisito
AuL-ICT.002.1	Audit log	Esiste un sistema di log che riporta: - gli accessi (access log) compresi i tentativi falliti - le operazioni svolte sui dati (activity log) dagli Addetti alla gestione applicativa e dalle utenze machine to machine (in quest'ultimo caso il sistema di destinazione dovrà tracciare anche l'informazione relativa al sistema di origine)
AuL-ICT.003.1	Audit log	Esiste un sistema di log che riporta: - gli accessi (access log) compresi i tentativi falliti - le operazioni svolte sui dati (activity log) dagli Addetti alla gestione del Database e dalle utenze machine to machine (in quest'ultimo caso il sistema di destinazione dovrà tracciare anche l'informazione relativa al sistema di origine)
AuL-ICT.004.1	Audit log	La piattaforma prevede la registrazione degli accessi e delle operazioni effettuate sui dati da parte degli End User Autorizzati, comprese le utenze machine to machine (in quest'ultimo caso il Sistema di destinazione dovrà tracciare l'informazione relativa al Sistema di origine).
AuL-ICT.005.1	Audit log	È garantita la completezza, l'immodificabilità e la possibilità di verificare l'autenticità e la conservazione per un periodo non inferiore a 6 mesi delle registrazioni dei log relativi agli accessi ed alle operazioni svolte dagli Addetti IT e dagli End User Autorizzati tramite l'invio degli stessi a sistemi di Log Collecting centralizzati.
AuL-ICT.006.1	Audit log	I log relativi agli accessi e alle operazioni degli Addetti IT e delle utenze machine to machine dovranno almeno consentire di identificare: - le operazioni svolte sui dati e le attività di amministrazione sul sistema; - l'utenza, la data e l'ora di effettuazione delle operazioni.
AuL-ICT.007.1	Audit log	I log relativi agli accessi e alle operazioni degli End User Autorizzati e delle utenze machine to machine dovranno almeno consentire di identificare: - le operazioni svolte sui dati e le attività di amministrazione sul sistema; - l'utenza, la data e l'ora di effettuazione delle operazioni.
CdC-ICT.010.1	Canali di comunicazione	È assicurata l'implementazione di meccanismi crittografici di robustezza adeguata (ad es. HTTPS) volti a garantire la protezione dell'autenticazione degli End User Autorizzati dal rischio di intercettazione delle credenziali.
CdC-ICT.011.1	Canali di comunicazione	Nel caso la piattaforma preveda l'utilizzo di web application esposte su rete pubblica, i server sono dotati di certificati SSL Publicly Trusted.

CoA-ICT.011.1	Controllo accessi	L'applicativo è costruito in maniera tale da prevedere l'impostazione di soglie relative al numero di utenze degli End User Autorizzati con privilegi di accesso. La valorizzazione di tali soglie è resa disponibile al Cliente PA attraverso funzionalità applicative assegnabili a profili caratterizzati da massimi privilegi (ad es. amministratore di applicativo o profili di gestione utenze).
CoA-ICT.012.1	Controllo accessi	L'applicativo prevede, tramite controlli automatici, la sospensione delle credenziali di autenticazione a seguito di 10 tentativi falliti di accesso, a meno di differenti accordi con il Cliente PA. Al fine di riattivare le utenze così sospese sono previste funzionalità di riabilitazione delle utenze assegnabili a specifici profili (ad es. amministratore di applicativo profili di gestione utenze).
CoA-ICT.013.1	Controllo accessi	L'applicativo prevede meccanismi di limitazione degli accessi degli End User Autorizzati per intervalli temporali o di data predeterminati. La valorizzazione di tale soglia è resa disponibile al Cliente PA attraverso funzionalità applicative assegnabili a specifici profili.
Doc-ICT.011.1	Documentazione	In presenza di personale TIM (interno od esterno) autorizzato al trattamento nonché all'accesso ai dati personali trattati dalla piattaforma, il Gestore garantisce l'esistenza di procedure di comunicazione verso la PA Cliente dell'elenco aggiornato di tali nominativi.
Ris-ICT.020.1	Riservatezza	Sono adottate misure tecniche volte ad impedire funzionalità di estrazione massiva dei dati dalle banche dati da parte degli End User Autorizzati, al fine di proibire la creazione di autonome banche dati.
Ris-ICT.021.1	Riservatezza	Sono adottate misure volte a permettere la valorizzazione di un campo con il numero di riferimento della pratica (ad es. numero del protocollo o del verbale) ogni volta che vengono effettuate consultazioni da parte degli End User Autorizzati.

PERIMETRO PUBBLICHE AMMINISTRAZIONI (MISURE AGID)

Ad aprile 2017 AgiD ha pubblicato nella Gazzetta Ufficiale (GuRI) le Misure Minime di Sicurezza per la PA, un documento che contiene le Misure minime di sicurezza ICT per le Pubbliche Amministrazioni le quali costituiscono parte integrante delle Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni.

Le misure minime Agid sono indicate con 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**).

L'appartenenza di una piattaforma a tale perimetro prevede necessariamente l'inclusione della stessa anche all'interno del Perimetro 231/01 reati informatici e del Perimetro Dati Personali.

ID MISURA	Categoria Mimip	Testo requisito

PdE-ICT.013.1 PdE-ICT.013.2	Protezione degli elaboratori	È previsto che venga applicata una protezione crittografica sui dati rilevanti (aventi particolari requisiti di riservatezza). Per le soluzioni custom condividere contrattualmente con il cliente quali sono i dati rilevanti. **[M] 13.1.1:**
Doc-ICT.012.1	Documentazione	È prevista l'implementazione di un inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, che registra almeno l'indirizzo IP, da aggiornare quando nuovi dispositivi approvati vengono collegati in rete. **[M] 1.1.1:** **[M] 1.3.1:** **[M]1.4.1:** **[M]1.4.1:**
PdE-ICT.014.1	Protezione degli elaboratori	È prevista la redazione di un elenco di software autorizzati, con relative versioni, necessari per ciascun tipo di sistema, compresi server e al contempo non è consentita l'installazione di software non compreso in tale elenco. E' prevista l'esecuzione di regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato. [**M] 2.1.1:** **[M] 2.3.1:**
Bck-ICT.004.1	Back-up	Su server e per la protezione dei sistemi operativi, sono definite, impiegate e ripristinate (nel caso vengano compromessi) configurazioni standard. Le immagini d'installazione sono memorizzate offline. **[M] 3.1.1:** **[M] 3.1.1:** **[M] 3.2.1:** **[M] 3.2.2:** **[M] 3.3.1:**
PdE-ICT.015.1	Protezione degli elaboratori	È assicurato che gli strumenti di scansione delle vulnerabilità (anche per i sistemi separati dalla rete) siano regolarmente aggiornati adottando misure di sicurezza adeguate al livello di criticità. Inoltre, è periodicamente verificato che le vulnerabilità emerse dalle scansioni siano state risolte, documentando e accettando in caso opposto un ragionevole rischio. A ciascuna azione utile per la risoluzione delle vulnerabilità è assegnato un livello di priorità in base al rischio associato. Ad ogni modifica significativa della configurazione deve essere eseguita la ricerca delle vulnerabilità con strumenti automatici che forniscano report con indicazioni delle vulnerabilità più critiche. **[M] 4.1.1:** **[M] 4.4.1:** **[M] 4.5.2:** **[M] 4.7.1:** **[M] 4.8.2:**
PdE-ICT.016.1	Protezione degli elaboratori	Vengono scaricati automaticamente e installati le patch e gli aggiornamenti del software di sistema operativo necessari a correggere difetti e prevenire vulnerabilità della piattaforma. L'installazione avviene automaticamente qualora

		non preveda un'interruzione o una forte limitazione dell'operatività. In particolare, sono applicate le patch per le vulnerabilità a partire da quelle più critiche. **[M] 4.5.1:** **[M] 4.7.1:** **[M] 4.8.2:**
PdE-ICT.017.1	Protezione degli elaboratori	Vengono scaricati automaticamente e installati le patch e gli aggiornamenti del software di DBMS e applicativo oggetto del SaaS, necessari a correggere difetti e prevenire vulnerabilità della piattaforma. L'installazione avviene automaticamente qualora non preveda un'interruzione o una forte limitazione dell'operatività. In particolare, sono applicate le patch per le vulnerabilità a partire da quelle più critiche. **[M] 4.5.1:** **[M] 4.7.1:** **[M] 4.8.2:**
CoA-ICT.015.1	Controllo accessi	Vengono completamente distinte utenze privilegiate e non privilegiate degli amministratori (alle quali devono corrispondere credenziali diverse), mentre è consentito l'utilizzo delle utenze amministrative anonime (ad esempio “root” di UNIX o “Administrator” di Windows) solo per le situazioni di emergenza; queste vengono gestite in modo da garantire la disponibilità e la riservatezza e in modo da assicurare l’imputabilità di chi ne fa uso. **[M] 5.10.1:** **[M] 5.10.3:**
PdE-ICT.018.1	Protezione degli elaboratori	Sulle piattaforme non sono consentite l’esecuzione automatica dei contenuti, dinamici e non, e l'anteprima automatica dei contenuti dei file, anche al momento della connessione dei dispositivi removibili e l'apertura automatica dei messaggi di posta elettronica. Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali. **[M]8.3.1:** **[M] 8.7.1:** **[M] 8.7.2:** **[M] 8.7.3:** **[M] 8.7.4:**
PdE-ICT.019.1	Protezione degli elaboratori	Qualsiasi supporto removibile utilizzato è automaticamente soggetto ad una scansione anti-malware, inoltre sono adottati e configurati adeguati strumenti di web filtering e nel caso di posta elettronica antispamming bloccando nella posta elettronica e nel traffico web i file potenzialmente pericolosi la cui tipologia non è strettamente necessaria per l’organizzazione. **[M] 8.8.1:** **[M] 8.9.1:** **[M] 8.9.2:** **[M] 8.9.3:**
CdC-ICT.013.1	Canali di comunicazione	Le operazioni di amministrazione remota di server, dispositivi di rete e analoghe apparecchiature sono eseguite per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).

		[M] 3.4.1:
CdC-ICT.014.1	Canali di comunicazione	È prevista la possibilità di bloccare il traffico da e verso url presenti in una blacklist. **[M] 13.8.1:**
Ris-ICT.013.1	Riservatezza	Risulta garantita l'applicazione delle misure di sicurezza derivanti dalle analisi del rischio (Piano di Sicurezza) relative alla piattaforma a supporto del servizio erogato. **[M] 4.8.1:**

PERIMETRO SCAMBI DATI TRA PA

L'appartenenza di una piattaforma a tale perimetro prevede necessariamente l'inclusione della stessa anche all'interno del Perimetro 231/01 reati informatici e del Perimetro Dati Personali.

ID MISURA	Categoria Mimip	Testo requisito
AuL-ICT.001.1	Audit log	Esiste un sistema di log che riporta: - gli accessi (access log) compresi i tentativi falliti - le operazioni svolte sui dati (activity log) dagli Addetti alla gestione del Sistema Operativo e dalle utenze machine to machine (in quest'ultimo caso il sistema di destinazione dovrà tracciare anche l'informazione relativa al sistema di origine)
AuL-ICT.002.1	Audit log	Esiste un sistema di log che riporta: - gli accessi (access log) compresi i tentativi falliti - le operazioni svolte sui dati (activity log) dagli Addetti alla gestione applicativa e dalle utenze machine to machine (in quest'ultimo caso il sistema di destinazione dovrà tracciare anche l'informazione relativa al sistema di origine)
AuL-ICT.003.1	Audit log	Esiste un sistema di log che riporta: - gli accessi (access log) compresi i tentativi falliti - le operazioni svolte sui dati (activity log) dagli Addetti alla gestione del Database e dalle utenze machine to machine (in quest'ultimo caso il sistema di destinazione dovrà tracciare anche l'informazione relativa al sistema di origine)
AuL-ICT.004.1	Audit log	La piattaforma prevede la registrazione degli accessi e delle operazioni effettuate sui dati da parte degli End User Autorizzati, comprese le utenze machine to machine (in quest'ultimo caso il Sistema di destinazione dovrà tracciare l'informazione relativa al Sistema di origine).

AuL-ICT.005.1	Audit log	È garantita la completezza, l'immodificabilità e la possibilità di verificare l'autenticità e la conservazione per un periodo non inferiore a 6 mesi delle registrazioni dei log relativi agli accessi ed alle operazioni svolte dagli Addetti IT e dagli End User Autorizzati tramite l'invio degli stessi a sistemi di Log Collecting centralizzati.
AuL-ICT.006.1	Audit log	I log relativi agli accessi e alle operazioni degli Addetti IT e delle utenze machine to machine dovranno almeno consentire di identificare: - le operazioni svolte sui dati e le attività di amministrazione sul sistema; - l'utenza, la data e l'ora di effettuazione delle operazioni.
AuL-ICT.007.1	Audit log	I log relativi agli accessi e alle operazioni degli End User Autorizzati e delle utenze machine to machine dovranno almeno consentire di identificare: - le operazioni svolte sui dati e le attività di amministrazione sul sistema; - l'utenza, la data e l'ora di effettuazione delle operazioni.
CdC-ICT.010.1	Canali di comunicazione	È assicurata l'implementazione di meccanismi crittografici di robustezza adeguata (ad es. HTTPS) volti a garantire la protezione dell'autenticazione degli End User Autorizzati dal rischio di intercettazione delle credenziali.
CdC-ICT.011.1	Canali di comunicazione	Nel caso la piattaforma preveda l'utilizzo di web application esposte su rete pubblica, i server sono dotati di certificati SSL Publicly Trusted.
CoA-ICT.011.1	Controllo accessi	L'applicativo è costruito in maniera tale da prevedere l'impostazione di soglie relative al numero di utenze degli End User Autorizzati con privilegi di accesso. La valorizzazione di tali soglie è resa disponibile al Cliente PA attraverso funzionalità applicative assegnabili a profili caratterizzati da massimi privilegi (ad es. amministratore di applicativo o profili GGU).
CoA-ICT.012.1	Controllo accessi	L'applicativo prevede, tramite controlli automatici, la sospensione delle credenziali di autenticazione a seguito di 10 tentativi falliti di accesso, a meno di differenti accordi con il Cliente PA. Al fine di riattivare le utenze così sospese sono previste funzionalità di riabilitazione delle utenze assegnabili a specifici profili (ad es. amministratore di applicativo o GGU).
CoA-ICT.013.1	Controllo accessi	L'applicativo prevede meccanismi di limitazione degli accessi degli End User Autorizzati per intervalli temporali o di data predeterminati. La valorizzazione di tale soglia è resa disponibile al Cliente PA attraverso funzionalità applicative assegnabili a specifici profili.
Doc-ICT.011.1	Documentazione	In presenza di personale (interno od esterno) autorizzato al trattamento nonché all'accesso ai dati personali trattati dalla piattaforma, il Gestore garantisce l'esistenza di procedure di comunicazione verso la PA Cliente dell'elenco aggiornato di tali nominativi.
Ris-ICT.020.1	Riservatezza	Sono adottate misure tecniche volte ad impedire funzionalità di estrazione massiva dei dati dalle banche dati da parte degli End User Autorizzati, al fine di proibire la creazione di autonome banche dati.
Ris-ICT.021.1	Riservatezza	Sono adottate misure volte a permettere la valorizzazione di un campo con il numero di riferimento della pratica (ad es. numero del protocollo o del verbale) ogni volta che vengono effettuate consultazioni da parte degli End User Autorizzati.

PERIMETRO DATI PARTICOLARI BIOMETRICI O GENETICI

Per dati biometrici (Rif. [4]) s'intendono i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Per dati genetici (Rif. [4]) s'intendono i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Per tali tipologie di dato si propone al Titolare del Trattamento di avviare la DPIA coinvolgendo il Responsabile dello Sviluppo e della Gestione Applicativa per indirizzare eventuali misure specifiche.

PERIMETRO ENERGETICO

Composto dalle piattaforme relative a soluzioni per clienti operanti nei settori dell'energia elettrica e del gas, in particolare:

- soggetti di diritto italiano che operano in una o più attività dei settori dell'energia elettrica e/o del settore del gas naturale e/o distribuzione, misura e/o vendita di altri gas a mezzo reti;
- soggetti di diritto estero che operano in una o più attività dei settori dell'energia elettrica e del gas naturale in Italia, anche per mezzo di sedi secondarie o di unità locali;
- soggetti di diritto italiano o estero appartenenti ad un gruppo che opera in una o più attività dei settori dell'energia elettrica e del gas naturale, che intrattiene rapporti economici o patrimoniali funzionali allo svolgimento delle attività degli esercenti di cui sopra.

L'appartenenza di una piattaforma a tale perimetro prevede necessariamente l'inclusione della stessa anche all'interno del Perimetro 231/01 reati informatici.

ID MISURA	Categoria Mimip	Testo requisito
CoA-ICT.001.1	Controllo accessi	Nel caso il contratto con il Cliente includa il rispetto dei requisiti del Testo Integrato di Unbundling (Delibera AEEG n. 11/07) istituito dall'Autorità per l'Energia elettrica ed il gas, è prevista l'esistenza di un elenco aggiornato delle utenze degli Addetti IT che hanno accesso alle informazioni commercialmente sensibili (prevista contrattualmente).

CoA-ICT.002.1	Controllo accessi	Nel caso il contratto con il Cliente includa il rispetto dei requisiti del Testo Integrato di Unbundling (Delibera AEEG n. 11/07) istituito dall'Autorità per l'Energia elettrica ed il gas, è prevista l'inibizione dell'accesso ai dati trattati dalla piattaforma da parte di eventuali soggetti terzi (ad es. Fornitori o Partner) estranei al rapporto contrattuale con il Cliente.

PERIMETRO DATI DI LOCALIZZAZIONE

In termini tecnici, la "localizzazione" consiste nell'individuazione della posizione geografica di oggetti, persone o mezzi sia in posizione da fermo sia in movimento, attraverso l'impiego di diverse tecnologie, ad esempio le funzionalità della rete mobile (GSM/UMTS/LTE), la tecnologia satellitare GPS, informazioni derivate dal servizio di connettività a Internet via WiFi pubblico, ecc..

L'appartenenza di una piattaforma a tale perimetro prevede necessariamente l'inclusione della stessa anche all'interno del Perimetro Dati Personali.

ID MISURA	Categoria Mimip	Testo requisito
CoA.079.1	Controllo accessi	L'estrazione dei dati di localizzazione dalla piattaforma e la memorizzazione su Postazioni di Lavoro da parte degli Addetti IT può essere svolta eccezionalmente e a seguito di autorizzazione da parte del Responsabile Gerarchico (privilegiando in alternativa la conservazione temporanea dei dati sui sistemi stessi) solo per la gestione di anomalie con l'obiettivo di ripristinare a regime e/o di assicurare con modalità provvisoria la funzionalità del sistema ICT.
CoA.054.1	Controllo accessi	I dati di localizzazione, ad esclusione di quelli gestiti per finalità di erogazione del servizio di comunicazione elettronica o per ottemperare a obblighi di legge, sono trattati in forma anonima o aggregati in modo irreversibile. In caso contrario, prima di iniziare i trattamenti, è stata verificata (anche a mezzo dichiarazione del titolare o addendum contrattuale) la fornitura una specifica informativa agli interessati ed ottenuto il relativo consenso specifico per la localizzazione.
PdE.046.1	Protezione degli elaboratori	Sono adottati sulla piattaforma metodi di sincronizzazione a riferimenti temporali standard che garantiscono la completezza e la correttezza delle informazioni temporali associate ai trattamenti svolti sui dati di di localizzazione.

Bck.008.1	Back-up	La piattaforma conserva i dati di localizzazione solo per il periodo strettamente necessario alla fornitura del servizio e, se non esplicitamente indicata nel consenso raccolto dal titolare del trattamento, non può essere superiore a 2 mesi dalla generazione del dato allo scadere dei quali i dati (contenuti in DB/Sistemi elaborazione/Backup) devono essere cancellati/anonimizzati nei minimi tempi tecnicamente compatibili e comunque non oltre 30 giorni solari. Le operazioni di cancellazione sono documentate, anche tramite il tracciamento in un file di log della corretta esecuzione delle procedure automatiche di cancellazione.
AuL.001.2	Audit log	Esiste un sistema di log che riporta tutte le operazioni svolte (audit log) sui dati di localizzazione dagli Addetti IT (deputati alla gestione del Database e alla gestione applicativa del sistema) e dalle utenze machine to machine. Il tracciamento generato della piattaforma è garantito indipendentemente dalla tipologia di accesso (es. accessi diretti o mediati). Nel caso di documentata impossibilità, i file di tracciamento sono prodotti tramite sistemi intermedi o piattaforme di mediazione degli accessi; per le utenze che accedono in tale modalità è quindi garantita l'impossibilità dell'accesso diretto alla componente.
AuL.031.1	Audit log	Il sistema registra un log di tutte le operazioni svolte (audit log) sui dati di localizzazione, da tutte le utenze (End User Autorizzati e Addetti IT), comprese quelle machine to machine (in quest'ultimo caso la piattaforma di destinazione dovrà tracciare l'informazione relativa alla piattaforma di origine). Nel caso di documentata impossibilità, i file di tracciamento sono prodotti tramite sistemi intermedi o piattaforme di mediazione degli accessi; per le utenze che accedono in tale modalità è quindi garantita l'impossibilità dell'accesso diretto alla componente.
AuL.002.3	Audit log	Esiste un sistema di log che riporta tutte le operazioni svolte (audit log) sui dati di localizzazione dagli Addetti IT (deputati alla gestione del Sistema Operativo) e dalle utenze machine to machine. Nel caso di documentata impossibilità, i file di tracciamento sono prodotti tramite sistemi intermedi o piattaforme di mediazione degli accessi; per le utenze che accedono in tale modalità è quindi garantita l'impossibilità dell'accesso diretto alla componente.

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

cod. doc. TLC23MFHATCS Data: 25/10/2023

AuL.042.1	Audit log	Nel caso di documentata impossibilità tecnica a generare i tracciamenti relativi ai trattamenti massivi sui dati di localizzazione eseguiti tramite programmi di elaborazione automatica, è previsto che: • gli autorizzati al trattamento non possano utilizzare utenze application to application per eseguire direttamente accessi e attività sul sistema; • la modifica e/o lo sviluppo di tali programmi avviene solo in seguito a processi autorizzati di software change.
AuL.004.1	Audit log	I log relativi alle operazioni svolte dagli Addetti IT e dalle utenze machine to machine, sui dati di localizzazione, dovranno almeno consentire di identificare: • il sistema target e l'eventuale applicazione acceduta; • il riferimento dell'utente che ha eseguito le attività; • l'eventuale dettaglio delle caratteristiche o dei parametri di accesso; • i riferimenti temporali di esecuzione delle singole attività; • l'indicazione delle tipologie e delle caratteristiche delle attività eseguite
AuL.005.1	Audit log	I log relativi alle operazioni svolte (audit log) dagli End User Autorizzati e dalle utenze machine to machine, sui dati di localizzazione, dovranno almeno consentire di identificare: • il sistema target e l'eventuale applicazione acceduta; • il riferimento dell'utente che ha eseguito le attività; • l'eventuale dettaglio delle caratteristiche o dei parametri di accesso; • i riferimenti temporali di esecuzione delle singole attività; • l'indicazione delle tipologie e delle caratteristiche delle attività eseguite
AuL.010.1	Audit log	E' garantita la completezza, l'immodificabilità e l'autenticità delle registrazioni dei log relativi alle operazioni svolte sui dati di localizzazione dagli addetti IT e dalle utenze machine to machine, (ad es. tramite l'invio dei log ai sistemi di Log Collecting centralizzati), e sono conservati per 12 mesi e successivamente cancellati nei minimi tempi tecnicamente compatibili e comunque non oltre 30 giorni solari.
AuL.034.1	Audit log	E' garantita la completezza, l'immodificabilità e l'autenticità delle registrazioni dei log relativi alle operazioni svolte sui dati localizzazione dagli End User Autorizzati e dalle utenze machine to machine (ad es. tramite l'invio dei log ai sistemi di Log Collecting centralizzati) dove sono conservati per 12 mesi e successivamente cancellati nei minimi tempi tecnicamente compatibili e comunque non oltre 30 giorni solari.

Allegato Tecnico di Compliance - Progettazione, realizzazione e gestione del sistema Cloud Toscana, il community Cloud per la Pubblica Amministrazione in Toscana per il Cliente AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

Doc.017.1	Documentazione	I profili autorizzativi che consentono il trattamento dei dati di localizzazione devono essere evidenziati sulla documentazione relativa alla politica di gestione Utenze e matrice profili/funzioni del sistema e adeguatamente aggiornati.