

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.

Per i servizi contrattualizzati che prevedono il trattamento di questo Perimetro di Dati sono state definite le seguenti misure ulteriori misure aggiuntive a quelle previste per il perimetro dei Dati Personali Comuni.

ID MISURA	Categoria	Testo requisito
Bck-ICT.001.1	Back-up	E' 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.

TIM S.p.A.

ID MISURA	Categoria	Testo requisito
Ris-ICT.002.1	Riservatezza	<p>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.</p> <p>In particolare la misura deve essere prevista qualora:</p> <ul style="list-style-type: none">- 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	<p>E' 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.</p>

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