FERROVIE DELLO STATO ITALIANE

PREMIUM PARTNER

People, Culture & Transformation
HR Policies, Labour Legal & Industrial Relations
Il Responsabile

Ferrovie dello Stato Italiane
UA 5/12/2025
FS-AD-PCT-PIR\A0011\P\2025\0000019

Segreterie Nazionali:
FILT-CGIL
FIT-CISL
UILTRASPORTI
UGL FERROVIERI
SLM FAST CONFSAL
ORSA FERROVIE

Loro Sedi

Oggetto: Riscontro OO.SS. richiesta formale di informazioni - Regolamento 2016/679.

Allegati: 1

Con riferimento alla nota trasmessa dalle Organizzazioni sindacali in indirizzo il 24 novembre 2025, avente ad oggetto "Richiesta formale di informazioni e atti relativi alla violazione dei dati personali – artt. 28, 32, 33 e 34 GDPR - Regolamento 2016/679", si forniscono, a nome delle funzioni competenti di Gruppo, i seguenti elementi di conoscenza, sulla base delle informazioni allo stato disponibili e in relazione all'avanzamento delle indagini in corso da parte delle Autorità competenti.

Identificazione del fornitore IT e dei responsabili del trattamento

L'evento di violazione in parola ha riguardato un sistema di archiviazione in proprietà e in uso a un fornitore esterno al Gruppo, RTI TiAKy (TIM, Almaviva e Kyndryl), di "Servizi ICT di gestione sistemistica e delle infrastrutture hardware, hosting, housing, IaaS".
Il contratto con RTI TiAKy è gestito da FS Technology, in qualità di Service Company ICT del Gruppo FS al fine di fornire alle società del Gruppo i servizi ICT a supporto dei processi aziendali.
In particolare, Ferservizi SpA - Società del Gruppo FS individuata quale Shared Services Center del Gruppo FS - eroga alle altre Società del Gruppo, i Servizi "no core" tra cui quello di "Gestione del Personale Amministrato", nell'ambito del quale cura le attività di "payroll" predisponendo le "buste paga" dei dipendenti delle Società del Gruppo.
L'affidamento dei predetti Servizi a Ferservizi è disciplinato da appositi Contratti Intercompany stipulati dalle predette Società in relazione ai quali - con apposito Accordo di Data Protection allegato a ciascun Contratto - le Società, quali Titolari del

Ferrovie dello Stato Italiane S.p.A. – Società con socio unico
Sede legale: Piazza della Croce Rossa, 1 - 00161 Roma
Cap. Soc. Euro 31.062.952.307,00
Iscritta al Registro delle Imprese di Roma
Cod. Fisc. e P. Iva 06359501001 – R.E.A. 962805

Trattamento dei dati personali, hanno nominato Ferservizi Responsabile del trattamento.
Per l'esecuzione dei citati Servizi – tra cui quello relativo alle "buste paga" – Ferservizi si avvale dei Servizi IT e dei Servizi di Cyber Security prestati, rispettivamente, dalle Società del Gruppo FSTechnology e FS Security in virtù di appositi contratti.
FS Technology e FS Security si configurano, per le rispettive attività di competenza, entrambe quali Responsabile del trattamento (per Ferservizi "Titolare") e sub-Responsabile del trattamento (per Ferservizi "Responsabile"), in forza di appositi Accordi di Data Protection.
FSTechnology presta a Ferservizi i suddetti Servizi IT di supporto al business avvalendosi di propri fornitori terzi tra i quali, in particolare - per le predette attività inerenti di archiviazione transitoria all'interno del processo di elaborazione delle buste paga - il RTI denominato TiAKy (TIM, Almaviva e Kyndryl) con il quale ha stipulato apposito contratto per l'affidamento dei "Servizi ICT di gestione sistemistica e delle infrastrutture hardware, hosting, housing, IaaS".

Descrizione tecnica e giuridica della violazione

In data 13 novembre 2025, il suddetto RTI TiAKy ha comunicato che Almaviva, Società mandante, aveva segnalato la possibile violazione di alcuni apparati in scope al RTI e in uso afferenti al servizio di archiviazione documentale, ad opera di attori esterni non identificati.
Successivamente, in data 14 novembre, a valle delle necessarie analisi e verifiche svolte dalle competenti strutture di Gruppo, è stato possibile confermare l'avvenuta violazione con esfiltrazione di dati personali.
La perdita di riservatezza ha riguardato le tipologie di dati personali contenute nella busta paga del mese di settembre 2025 dei dipendenti delle seguenti società Titolari, per un totale di circa 70.000 interessati: Cremonesi Workshop Srl, Fercredit SpA, Ferrovie dello Stato Italiane SpA, Ferservizi SpA, Fondazione FS Italiane, FS International SpA, FS Park SpA, FS Security SpA, FS Sistemi Urbani SpA, FSTechnology SpA, Grandi Stazioni Rail SpA, Italcertifer SpA, Italferr SpA, Mercitalia Intermodal SpA, FS Logistix SpA, Mercitalia Rail Srl, Rete Ferroviaria Italiana SpA, Terminali Italia Srl, FS Treni Turistici Italiani Srl, Trenitalia SpA, Trenitalia Tper Scarl.
Le probabili conseguenze della violazione riguardano la potenziale perdita di riservatezza, con possibilità che i dati siano divulgati al di fuori di quanto previsto per il loro legittimo trattamento. Il livello di gravità per il potenziale impatto sugli interessati è stato identificato come alto, in considerazione delle caratteristiche della condotta malevola posta in essere dall'attaccante e in funzione dell'elevato numero di interessati, della categoria di interessati coinvolti (dipendenti) e della tipologia di dati personali oggetto della violazione.

Notifica all'Autorità Garante – Art. 33 GDPR

Il fornitore esterno ha comunicato di aver presentato notifica per esfiltrazione dati al Garante per la Protezione dei Dati Personali in data 17 novembre 2025.

Comunicazione agli interessati – Art. 34 GDPR

Ai dipendenti interessati è stata resa comunicazione ex art. 34 GDPR da parte della rispettiva società titolare tramite portale aziendale Self-service WE4ME. Il contenuto è stato reso a visualizzazione obbligatoria all'accesso al portale al fine di assicurare la presa visione da parte di ciascun dipendente della suddetta comunicazione. Con la medesima funzionalità è in corso la messa a disposizione dei dipendenti interessati anche di una raccolta di domande e risposte frequenti (FAQ - allegate alla presente).

Profili di responsabilità contrattuale e trattamento illecito – artt. 5, 24 e 28 GDPR

FSTechnology, responsabile del contratto con TiAKy si è da subito attivata formalmente richiedendo al fornitore gli elementi informativi necessari, anche al fine della valutazione di eventuali profili di responsabilità.
Il fornitore ha comunicato di avere rafforzato le configurazioni di sicurezza dei sistemi impattati dall'evento e sono in corso ulteriori verifiche tecniche.

Misure di tutela per gli interessati

Sono state adottate dal fornitore misure di protezione tecniche e organizzative per contenere la violazione e attenuarne gli effetti, nonché implementative volte a prevenire il ripetersi di violazioni analoghe.
Si è provveduto a denunciare l'evento alle Autorità competenti, nello specifico la struttura di Cyber Security del Gruppo FS ha provveduto ad effettuare apposita segnalazione dell'evento al CSIRT Italia e al Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC).
Ciascuna società del Gruppo titolare ha provveduto a presentare notifica al Garante per la Protezione dei Dati Personali.
Ai dipendenti interessati è stata fornita dalla rispettiva Società titolare comunicazione ex art. 34 GDPR, nella quale sono indicati i relativi canali di contatto aziendali dedicati per qualsiasi necessità di chiarimento per gli aspetti di data protection e di cyber security.
Infine, il Cyber Defence Center di FS Security SpA prosegue le proprie attività di monitoraggio costante, anche attraverso i propri servizi di Cyber Threat Intelligence.

Distinti saluti,

Massimiliano Loffredi

MASSIMILIANO LOFFREDI
Firmato da
MASSIMILIANO
LOFFREDI
il 05/12/2025 alle
12:54:06 CET

All. 1

Domanda	Risposta
Tra i dati personali presenti nel cedolino è presente anche l'iban, devo effettuare una segnalazione al mio istituto di credito/banca? la Società titolare del trattamento contatterà l'istituto bancario/di credito per porre azioni a tutela della diffusione delle coordinate bancarie?	Normalmente gli istituti bancari non avallano alcuna operazione (ad es. addebito) se non attraverso i canali prestabiliti e processi con criteri autorizzativi rafforzati; tuttavia, una segnalazione può essere utile a sensibilizzare il proprio istituto di riferimento.
Devo modificare le mie credenziali per accedere ai servizi aziendali?	La modifica delle credenziali di accesso ai servizi aziendali segue le linee guida del Gruppo FS. Cambiare la password di accesso è sempre un buon deterrente per evitare rischi di accessi abusivi.
Devo rivolgermi alle Autorità?	L'azienda ha già attivato le misure di tutela previste a suo carico, informando le Autorità competenti in qualità di titolare del trattamento dei dati. L'incidente è stato regolarmente segnalato all'Autorità Giudiziaria e sono già in corso le relative indagini penali. Resta, comunque, una tua facoltà presentare personalmente una denuncia.
La comunicazione relativa all'evento che ho ricevuto dalla mia Azienda riguarda la mia posizione?	Se hai ricevuto la comunicazione in qualità di interessato, i tuoi dati sono stati oggetto di esfiltrazione. In particolare, come precisato nella predetta comunicazione, la violazione ha riguardato i dati personali contenuti nella busta paga del mese di settembre 2025. Tali dati possono includere, a titolo esemplificativo: dati anagrafici, codice fiscale, coordinate bancarie (es. IBAN), informazioni retributive e altri dati amministrativi presenti nella busta paga.
Quali conseguenze potrebbe comportare la perdita di riservatezza dei dati del cedolino?	L'evento è circoscritto alla perdita di riservatezza delle informazioni presenti nel cedolino, con la possibilità che tali dati possano essere utilizzati in modo improprio o non conforme alle finalità per cui erano stati raccolti. Normalmente gli istituti bancari non avallano alcuna operazione (ad es. addebito) se non attraverso i canali prestabiliti e processi con criteri autorizzativi rafforzati; tuttavia, una segnalazione può essere utile a sensibilizzare il proprio istituto di riferimento.
La Società titolare del trattamento ha posto in essere azioni a tutela degli interessati per risolvere la criticità rappresentata?	Le strutture preposte a garantire la sicurezza e la continuità dei servizi del Gruppo FS hanno posto in essere le azioni e le misure in coordinamento con le Autorità preposte. L'Azienda ha già attivato le misure di tutela previste, informando le Autorità competenti in qualità di titolare del trattamento dei dati. L'incidente è stato regolarmente segnalato all'Autorità Giudiziaria e sono già in corso le relative indagini penali. Resta, comunque, una tua facoltà presentare personalmente una denuncia.
La perdita di riservatezza dei dati personali da cosa sarebbe dipesa?	La perdita di riservatezza dei dati personali è stata causata da un accesso non autorizzato ai sistemi informatici gestiti dal fornitore IT esterno al Gruppo (RTI TIAKY). In questo contesto si parla di "esfiltrazione di dati", poiché le informazioni sono state illecitamente prelevate dai sistemi da attori esterni.
Quali sono le conseguenze della violazione?	Le principali conseguenze riguardano la perdita di riservatezza dei dati personali, con il rischio che le informazioni possano essere conosciute da soggetti non autorizzati ed essere utilizzate in modo improprio o comunque non conforme alle finalità per cui erano stati raccolti. L'Azienda ha già adottato le misure previste per ridurre i rischi.
Cosa devo fare dopo la comunicazione fatta dalla mia Azienda per tutelarmi?	Prestare particolare attenzione a email di phishing , messaggi sospetti o richieste di informazioni personali non qualificate. Non interagire con comunicazioni sospette e segnala eventuali anomalie. In caso di email sospette sulla casella di posta aziendale, non interagire con il contenuto della comunicazione e segnala con l'apposito pulsantino disponbile su Outlook aziendale "segnala email sospetta" o direttamente a securityincident@fsitaliane.it.
E' possibile ricevere un documento ufficiale fornito dalla mia Azienda riguardo all'evento occorso?	La comunicazione ex art. 34 del Regolamento (UE) 2016/679 inviata agli interessati (nell'area We4ME - Self Service) è il documento ufficiale fornito dall'Azienda ai dipendenti coinvolti nell'incident. La comunicazione ex art. 34 Regolamento (UE) 2016/679 è disponibile nella tua area riservata WE4me nelle sezioni "HR 4me" o "I miei Task".
Devo sporgere denuncia verso ignoti, al fine di tutelare preventivamente la mia persona rispetto ad un uso illecito dei miei dati personali? e se si, a chi?	L'incidente è già stato regolarmente segnalato all'Autorità Giudiziaria e sono già in corso le relative indagini penali. Resta, comunque, una tua facoltà presentare personalmente una denuncia.
In che periodo è avvenuto l'accesso non autorizzato e quanto è durato?	L'evento è stato segnalato dal fornitore in data 13/11/2025 e prontamente isolato. Sono in corso accertamenti da parte delle Autorità competenti per definire con precisione il periodo in cui è avvenuto l'accesso non autorizzato e la sua effettiva durata.
Chi è il fornitore IT che gestisce l'archiviazione documentale?	L'archivio fisico e transitorio per l'elaborazione delle buste paga è gestito dal fornitore esterno al Gruppo (RTI TIAKY), soggetto responsabile del servizio secondo gli accordi contrattuali vigenti.
È possibile conoscere in che modo i dati siano stati utilizzati?	I dati risultano essere stati esfiltrati, cioè sottratti da soggetti non autorizzati, e non è al momento possibile conoscerne con certezza l'utilizzo, rimane comunque il rischio che possano essere impiegati in modo improprio.
È possibile ricevere documentazione relativa all'incidente?	La documentazione relativa all'evento è trasmessa esclusivamente alle Autorità competenti nell'ambito delle procedure previste e non è divulgabile.
Quali misure sono state adottate per evitare che accada di nuovo?	Il fornitore ha comunicato di avere rafforzato le configurazioni di sicurezza dei sistemi impattati dall'evento e sono in corso ulteriori verifiche tecniche.
È necessario presentare una denuncia alla Polizia Postale?	L'incidente è stato regolarmente segnalato all'Autorità Giudiziaria e sono già in corso le relative indagini penali. Resta, comunque, una tua facoltà presentare personalmente una denuncia.
Quali azioni sta adottando il DPO/ Referente Data Protection nei confronti del fornitore?	Il DPO/Referente Data Protection ha attivato le strutture competenti che hanno già avviato un processo di verifica approfondita nei confronti del fornitore, al fine di garantire il pieno rispetto degli obblighi contrattuali e normativi. Inoltre, sta monitorando l'adozione tempestiva delle misure tecniche e organizzative necessarie per prevenire ulteriori rischi.

L'incidente produce effetti sulla busta paga oggetto dell'evento o su situazioni future?	L'evento è circoscritto ai cedolini relativi al mese di settembre 2025. Non ci sono stati effetti sulla tua busta paga di settembre e non emergono elementi che indichino ripercussioni su documenti o emolumenti futuri.
È possibile che siano stati trafugati ulteriori dati?	Le verifiche attuali non indicano il coinvolgimento di dati diversi da quelli presenti nei cedolini di settembre 2025.
Come verranno comunicati eventuali aggiornamenti?	Qualora emergessero elementi di rilievo, verranno prontamente comunicate agli interessati le informazioni pertinenti, attraverso il medesimo canale di comunicazione aziendale (nell'area We4ME - Self Service).
Chi è autorizzato a trattare i miei dati relativi alla busta paga?	I dati personali relativi alla busta paga sono trattati dalla società datrice di lavoro e dalle altre società del Gruppo FS che, per la loro specifica missione e service intercompany, gestiscono il payroll dei dipendenti del Gruppo FS attraverso l'utilizzo dei sistemi IT dedicati.
Esistono canali diversi dalla posta elettronica per contattarvi?	Il canale istituzionale previsto per la gestione delle tue richieste è la casella del DPO/Referente Data Protection societario come indicato nella comunicazione ricevuta.
Posso ricevere gli estremi della denuncia effettuata dall'Azienda?	Le comunicazioni rivolte alle Autorità competenti sono parte dei flussi istituzionali previsti e non sono divulgabili. L'azienda ha già attivato le misure di tutela previste, informando le Autorità competenti in qualità di titolare del trattamento dei dati. L'incidente è stato regolarmente segnalato all'Autorità Giudiziaria e sono già in corso le relative indagini penali.
Posso ricevere gli estremi della notifica effettuata dall'Azienda all'Autorità Garante per la Protezione dei Dati Personali?	Il numero di protocollo è un riferimento amministrativo interno alla procedura di notifica verso l'Autorità e non rientra tra le informazioni da divulgare.
L'Azienda prevede misure di supporto ai dipendenti interessati, come assistenza legale in caso di conseguenze dannose?	Non si rende necessario, per il caso specifico, un supporto individuale, considerato che l'eventuale azione del singolo rappresenta una facoltà personale. Il Gruppo FS ha intrapreso tutte le opportune azioni a tutela. Le azioni intraprese dall'Azienda tutelano anche i dipendenti.