INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI PER L'UTILIZZO DELLA PIATTAFORMA MICROSOFT 365 DELL'INFN

1. PERCHÉ QUESTA INFORMATIVA

Ai sensi del Regolamento UE 2016/679 (Regolamento nel seguito) e del Decreto Legislativo 30 giugno 2003, n. 196 e ss.mm.ii, questa informativa descrive le modalità con cui l'Istituto Nazione di Fisica Nucleare (INFN) tratta i dati personali degli utenti nell'ambito dell'accesso e dell'utilizzo della piattaforma Microsoft 365.

La piattaforma è utilizzata per supportare attività istituzionali, amministrative, lavorative e di ricerca mediante servizi di identità, comunicazione, collaborazione, gestione documentale, archiviazione, sicurezza e conformità. Il perimetro può comprendere, in funzione dei servizi assegnati, Microsoft Entra ID, Exchange Online/Outlook, Microsoft Teams, SharePoint Online, OneDrive for Business, Microsoft 365 Apps, Microsoft Purview e Microsoft Defender.

Le registrazioni e le trascrizioni delle riunioni Microsoft Teams sono disciplinate da una specifica informativa, complementare alla presente.

2. IL TITOLARE DEL TRATTAMENTO E IL RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Titolare del trattamento dei dati è Istituto Nazionale di Fisica Nucleare (INFN) Via E. Fermi n. 54, Frascati (Roma), e-mail: presidenza@presid.infn.it PEC: amm.ne.centrale@pec.infn.it.

Il Responsabile della protezione dei dati è raggiungibile all'indirizzo e-mail: dpo@infn.it.

Punto di contatto: struttura o servizio INFN competente per l'utenza o per il servizio utilizzato.

3. FINALITÀ DEL TRATTAMENTO

I dati sono trattati per le seguenti finalità:

a) creare, gestire e proteggere gli account Microsoft 365, autenticare gli utenti e controllare gli accessi;

b) fornire i servizi di comunicazione, calendario, collaborazione, gestione documentale e archiviazione assegnati;

c) consentire lo svolgimento delle attività istituzionali, amministrative, lavorative, formative e di ricerca;

d) consentire la creazione, modifica, co-redazione, archiviazione e condivisione controllata di documenti e contenuti;

e) garantire sicurezza informatica, continuità operativa, protezione delle informazioni e gestione degli incidenti;

f) effettuare logging, audit, controllo degli accessi, diagnosi tecnica e tracciamento delle operazioni;

g) adempiere a obblighi normativi, amministrativi, di conservazione e di tutela dei diritti del Titolare.

4. BASI GIURIDICHE DEL TRATTAMENTO E NATURA DEL CONFERIMENTO

Il conferimento dei dati richiesti trova le sue basi giuridiche:

a) espletamento dei compiti di interesse pubblico connessi alle funzioni istituzionali dell'INFN;

b) interesse legittimo del Titolare alla sicurezza e alla continuità dei servizi ove applicabile e, nei soli casi in cui sia necessario, nel consenso dell'interessato;

c) adempimento obblighi legali;

d) nell'esecuzione del rapporto di lavoro, collaborazione, formazione o di misure contrattuali;

e) consenso dell'interessato, ove richiesto.

Il conferimento di dati è necessario per accedere ai servizi assegnati. L'eventuale mancato conferimento può impedire l'attivazione o l'utilizzo delle funzionalità della piattaforma.

L'utilizzo ordinario della piattaforma non è finalizzato al trattamento di categorie particolari di dati ne tantomeno è intenzione del Titolare utilizzarli. Gli utenti sono invitati a non inserire tali dati se non quando strettamente necessario, autorizzato e sorretto da un'idonea base giuridica. Qualora emergano, il trattamento avverrà solo se ricorre consenso esplicito o accertamento/difesa di un diritto.

5. TIPOLOGIA DEI DATI TRATTATI

Per le finalità dell'art. 3 saranno trattati i seguenti dati:

- dati identificativi e di contatto, quali nome, cognome, username, indirizzo e-mail, struttura o sede di appartenenza;
- dati relativi all'account, ruoli, licenze, autorizzazioni, autenticazione e sessioni;
- contenuti di messaggi, calendari, rubriche, documenti, file e relative informazioni di collaborazione;
- metadati di file e attività, quali autore, proprietario, date, cronologia, permessi e operazioni effettuate;
- dati relativi a riunioni ed eventi, fermo restando quanto previsto dalla specifica informativa Teams;
- dati tecnici, diagnostici, di utilizzo, connettività e configurazione dei dispositivi;
- indirizzi IP, log di accesso, audit trail, eventi, indicatori e segnalazioni di sicurezza;
- dati forniti volontariamente nell'ambito delle richieste di assistenza tecnica.

6. DURATA DI CONSERVAZIONE

I dati sono conservati per il tempo necessario alle specifiche finalità istituzionali, amministrative, operative, di sicurezza e di conformità.

I tempi dipendono dal servizio Microsoft 365 utilizzato, dalla tipologia del contenuto, dalle configurazioni del tenant, dalle policy di conservazione applicate, dagli obblighi normativi o archivistici e da eventuali esigenze di tutela giudiziaria.

In caso di eliminazione dell'account, i dati associati sono normalmente ripristinabili entro 30 giorni dalla cancellazione.

Per i documenti OneDrive di utenti eliminati si applica il periodo configurato nel tenant, pari a 60 giorni, oltre agli eventuali tempi tecnici del cestino, salvo differenti policy di conservazione, richieste di cancellazione, blocchi conservativi o obblighi di legge.

In caso di scadenza o cessazione del contratto Microsoft, i Customer Data possono essere mantenuti in un account a funzionalità limitata per 90 giorni per consentirne l'estrazione; la cancellazione definitiva avviene entro il termine massimo previsto dalla documentazione contrattuale applicabile, salvo obblighi di legge o diversi accordi.

7. MODALITÀ DEL TRATTAMENTO

Il trattamento avviene con strumenti informatici e telematici, secondo misure tecniche e organizzative adeguate e nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione, limitazione delle finalità e protezione dei dati.

Le misure comprendono, secondo le configurazioni applicabili, autenticazione degli utenti, autenticazione a più fattori, separazione dei ruoli amministrativi, controllo degli accessi, principio del minimo privilegio, gruppi di sicurezza, cifratura in transito e a riposo, logging, audit, revisione dei permessi e monitoraggio degli eventi di sicurezza.

La condivisione anonima mediante link accessibili a chiunque è disabilitata. Le condivisioni devono essere limitate ai soli soggetti necessari e avvenire mediante i meccanismi autorizzati dall'INFN.

8. COMUNICAZIONE

I dati possono essere comunicati, in funzione delle rispettive necessità e competenze, a:

- personale autorizzato dal Titolare, amministratori di sistema e funzioni tecniche, di sicurezza e conformità;
- fornitori di servizi ICT/Microsoft 365 o soggetti esterni che agiscono quali responsabili e ad eventuali sub-responsabili indicati nei loro elenchi;
- responsabili delle strutture e dei servizi interessati, collaboratori, consulenti e fornitori autorizzati;
- soggetti esterni autorizzati con i quali sia necessario collaborare per le attività istituzionali o contrattuali;
- Microsoft Ireland Operations, Ltd., quale responsabile del trattamento ai sensi dell'art. 28 del GDPR, e agli eventuali sub-responsabili indicati nella documentazione contrattuale;
- Enti, Amministrazioni o Autorità competenti, sanitarie, assicurative e di pubblica sicurezza in esecuzione di obblighi previsti dalla legge e di un contratto;
- altri soggetti che facciano richiesta di accesso nei limiti consentiti ai sensi della Legge 7 agosto 1990, n. 241;
- forze di polizia, all'autorità giudiziaria, a organismi di informazione e sicurezza o ad altri soggetti pubblici per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o re-pressione dei reati.

Microsoft tratta i dati personali nel rispetto delle proprie policy e documentazione contrattuale, in particolare:

- Microsoft Privacy Statement: https://privacy.microsoft.com/it-it/privacystatement e https://www.microsoft.com/it-it/privacy/privacystatement;
- Microsoft Products and Services Data Protection Addendum (DPA): https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.

Microsoft adotta misure di sicurezza tecniche e organizzative adeguate, conformi agli standard internazionali (es. ISO/IEC 27001).

9. DIFFUSIONE

I dati trattati mediante Microsoft 365 non sono destinati, per impostazione generale, alla diffusione al pubblico. L'eventuale pubblicazione di contenuti avviene esclusivamente quando prevista dalle finalità istituzionali e nel rispetto della base giuridica applicabile, dei principi di minimizzazione e privacy by design e delle specifiche regole del servizio utilizzato.

10. TRASFERIMENTO DEI DATI ALL'ESTERO

I dati personali conferiti non saranno trasferiti in Paesi terzi o presso organizzazioni internazionali al di fuori dell'Unione Europea.

I dati del tenant sono ospitati nel cloud Microsoft 365 con provisioning in area UE/EFTA, così da beneficiare degli impegni di residenza dei dati e, per i servizi coperti, della EU Data Boundary di Microsoft.

Qualora per ragioni di natura tecnica, di assistenza e/o operativa di funzionalità del servizio si renda necessario avvalersi di soggetti ubicati al di fuori dell'Unione Europea, oppure si renda necessario trasferire alcuni dei dati raccolti verso sistemi tecnici e servizi gestiti in cloud e localizzati al di fuori dell'area dell'Unione Europea, il trattamento sarà regolato in conformità a quanto previ-sto dal capo V del Regolamento UE e autorizzato in base a specifiche decisioni dell'Unione Europea.

11. DIRITTI DEGLI INTERESSATI

L'interessato, direttamente o a mezzo di un proprio de-legato, ha diritto di chiedere la conferma, l'accesso, la rettifica, l'integrazione, la limitazione, la trasformazione in forma anonima, il blocco, la cancellazione e la portabilità dei dati personali trattati che lo riguardano nonché di opporsi al loro trattamento.
I diritti indicati possono essere esercitati con apposita richiesta rivolta via mail al punto di contatto del Titolare di cui all'art. 2.
L'interessato può proporre reclamo all'Autorità Garante (https://www.garanteprivacy.it) o adire l'Autorità Giudiziaria qualora ritenga che il trattamento dei dati perso-nali avvenga in violazione del Regolamento.