Edizione Luglio 2023

FONDO PENSIONE PER IL PERSONALE DELLA DEUTSCHE BANK S.p.A.

FONDO PENSIONE PREESITENTE

Iscritto all'Albo tenuto dalla COVIP con il n. 1056

Istituito in Italia

Piazza del Calendario, 3 – 20126 Milano

+39 02 4024 2432

Mail: info@fondopensionedb.it
Pec: Fondopensione.db@actaliscertymail.it

www.fondopensionedb.it

REGOLAMENTO PRIVACY

Edizione luglio 2023

CORRETTA GESTIONE DEI DATI PERSONALI E DEGLI STRUMENTI DI TRATTAMENTO
FONDO PENSIONE PER IL PERSONALE DELLA DEUTSCHE BANK S.p.A.

REGOLAMENTO PRIVACY

1. SCOPO DEL PRESENTE DOCUMENTO

Lo scopo del presente documento è quello di definire un insieme di norme comportamentali cui tutti i dipendenti, i collaboratori ed eventuali terze parti che operano per il **Fondo Pensione Per il Personale della Deutsche Bank S.p.A.** (da ora Titolare o Fondo) devono uniformarsi nell'ambito delle attività che implicano un trattamento di dati ed informazioni personali e aziendali in linea con il Regolamento UE 2016/679 (General Data Protection Regulation).

2. DEFINIZIONI

«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 osociale.

«Trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

«Profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

«Pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

«Archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dalfatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

«Titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

«Responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. I trattamenti realizzati da parte di un Responsabile sono disciplinati da un contratto con cui quest'ultimo si vincola a rispettare le indicazioni del Titolare riguardo al trattamento.

«Destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabiliin materia di protezione dei dati secondo le finalità del trattamento.

«Terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il

titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

«Consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

«Violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione,la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

«Dati Particolari»: dati personali che rivelano 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 genetici»: 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.

«Dati biometrici»: 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.

«Dati relativi alla salute»: 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.

«**Dati giudiziari»:** dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

«Stabilimento principale»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento.

«Rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto …, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento.

«Impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica.

«Gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate.

3. ACCESSO AGLI UFFICI DEL FONDO

L'accesso agli Uffici del Titolare avviene attraverso badge e chiave personale, esclusivamente da personale autorizzato dal Titolare in base a precise e motivate esigenze di accesso a tali ambienti per finalità lavorative.

Le terze parti (clienti, fornitori, consulenti, visitatori, esterni) potranno avere accesso alle aree del Titolare esclusivamente se accompagnati da personale interno.

4. POSTAZIONE DI LAVORO FISICA

L'utilizzo della postazione di lavoro e il conseguente accesso agli strumenti informativi, agli atti, documenti e archivi contenenti dati personali è consentito nei limiti della propria funzione e dei propri incarichi assegnati.

Sulla propria scrivania non si devono lasciare documenti ed atti riservati e/o contenenti dati particolari sensibili senza un proprio controllo all'accesso di terzi, in momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.

5. GESTIONE DEI DATI E DELLE INFORMAZIONI PERSONALI

Ogni incaricato è responsabile dei dati e delle informazioni personali e aziendali delle quali entra in possesso per lo svolgimento della sua attività lavorativa. Deve quindi trattare i dati e le informazioni adottando ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza ed il corretto utilizzo.

Il trattamento di qualunque dato e informazione personale nell'ambito della propria attività lavorativa realizzata per il Fondo, deve prevedere da parte del collaboratore incaricato, ogni ragionevole misura per assicurare l'integrità di tali dati. I dati e le informazioni potranno essere comunicati a terze parti esclusivamente nell'ambito della propria funzione e secondo le finalità connesse alla propria attività lavorativa.

È vietata la comunicazione di dati e informazioni personali verso terzi che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale e del know-how ed alla redditività del Fondo, che possano violare i vincoli contrattuali e di legge e che possano ledere il diritto alla privacy dell'interessato.

È assolutamente vietata la divulgazione a terzi di informazioni particolari, sensibili, giudiziaria o riservate o comunque di proprietà del Fondo, senza espressa autorizzazione del Titolare.

In caso di violazione il Titolare si riserva di avviare i relativi provvedimenti disciplinari, nonché le azioni civili e penali consentite.

6. MISURE FISICHE DI CUSTODIA DEI DOCUMENTI E ATTI CARTACEI

I dati cartacei ed i documenti necessari allo svolgimento delle attività lavorative devono essere custoditi nell'ufficio di destinazione e/o nei luoghi deputati ad archivio del Fondo. Tutti gli archivi cartacei sono ad accesso limitato, per cui è possibile accedervi nei limiti della necessità per prelevare e riporre i documenti e gli atti necessari per lo svolgimento delle proprie attività lavorativa.

Gli archivi di documenti e atti contenenti dati personali particolari sensibili dovranno essere custoditi in armadi chiusi a chiave.

L'eliminazione fisica di documenti cartacei contenenti dati e informazioni di natura particolare sensibile o riservata deve essere effettuata dopo aver distrutto/stracciato fisicamente il documento, eventualmente utilizzando l'apposito elimina- documenti.

7. ACCESSO AI DATI PERSONALI ATTRAVERSO SISTEMI INFORMATICI

L'accesso ai dati, personali attraverso i sistemi informatici del Fondo, è consentito nei limiti della propria funzione e della propria attività lavorativa. In generale il sistema informatico e sue periferiche (PC, notebook, monitor e stampante) devono essere spenti ogni sera, prima di lasciare gli uffici, a maggior ragione in caso di assenze prolungate

dall'ufficio e nel fine settimana.

È obbligatorio non lasciare incustodito o accessibile il PC o notebook durante una pausa di lavoro. Per questo motivo i dispositivi devono essere bloccati manualmente se lasciati incustoditi e devono inoltre essere dotati di uno screen saver, protetto da password, ad attivazione automatica al massimo dopo 15 minuti di inattività.

Salvo preventiva espressa autorizzazione da parte del Titolare, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC o notebook né procedere ad installare software, dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.) non autorizzati dal Titolare.

8. CREDENZIALI DI ACCESSO ALLA RETE AZIENDALE (LOGIN E PASSWORD) E POLICY PASSWORD

L'accesso alla rete aziendale attraverso i sistemi informatici può avvenire esclusivamente se preventivamente identificati ed autenticati, pervia verifica delle proprie credenziali di accesso costituiti dal login e password. Qualunque variazione delle credenziali di accesso alla rete aziendale/applicazioni/data base/archivi/cartelle/risorse dei sistemi dovrà essere concordata ed autorizzata dal Titolare. È necessario prestare la massima attenzione nell'utilizzo, gestione e conservazione delle credenziali necessarie all'accesso dei sistemi informatici.

La policy per la gestione della password deve essere applicata da ogni utente e si compone dei seguenti criteri:

- password strettamente personale;
- di almeno 8 caratteri alfanumerici;
- con modifica ogni 3 mesi come indicato dal sistema.

L'utente dovrà attenersi alle seguenti prescrizioni:

- la password non può essere comunicata a nessun altro utente/terza parte;
- la password non deve essere annotata all'interno dell'ufficio o conservarla on-line;
- in caso di dimenticanza e/o ripristino della password, dovrà essere inoltrata una richiesta all'Amministratore di sistema.

Nell'ambito della gestione delle credenziali di autenticazione e dei profili utente ricordiamo che è compito dell'Amministratore di sistema:

- verificare la correttezza degli accessi al sistema riportando eventuali abusi;
- verificare periodicamente la coerenza dei profili utente con le responsabilità/attività assegnate in collaborazione con il Titolare.

All'utente non è consentita la modifica della struttura di rete aziendale e l'uso per scopi personali.

9. SOFTWARE ANTIVIRUS

La gestione (installazione, aggiornamento, ecc.) del software antivirus è di competenza dell'Amministratore di sistema. Tuttavia, è necessario che ogni utente eviti di disabilitare, per qualsiasi motivo, il sistema antivirus.

10. SOFTWARE

Ogni utente deve utilizzare esclusivamente i software e le applicazioni di cui dispone l'organizzazione.

Non è quindi consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Titolare. Di conseguenza non è consentito all'utente installare autonomamente alcun programma informatico senza la previa autorizzazione dell'Amministratore di Sistema. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre il Fondo a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software *(Decreto Legislativo 518/92 sulla Tutela giuridica del software e Legge 248/2000 Nuove norme di tutela del diritt*

o d'autore). È inoltre vietato immettere sulla rete e server aziendali software dannoso per i sistemi o comunque non autorizzato.

11. POSTA ELETTRONICA AZIENDALE

L'assegnazione di una casella email (*personale o di gruppo*) è finalizzata all'utilizzo della stessa esclusivamente per finalità legate alla attività lavorativa. Gli utenti della posta elettronica sono responsabili del corretto utilizzo della stessa e devono mantenere un corretto comportamento nell'utilizzo dello strumento di posta elettronica, sia nei messaggi inviati internamente che esternamente.

In particolare, devono essere seguite le seguenti disposizioni:

- la casella di posta elettronica aziendale (personale o di gruppo) non deve essere utilizzata per l'invio o la ricezione di messaggi personali al di fuori dalle finalità lavorative o per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione del Titolare;
- non inviare né conservare messaggi di posta elettronica e/o allegati dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico o comunque inappropriato o illegale;
- deve essere prestata la massima attenzione nell'inoltro di mail riportanti contenuti e indirizzi email di precedenti comunicazioni;
- in caso di assenza prolungata (ferie, malattia, aspettativa, lunga attività fuori sede) l'utente deve prevedere delle opportune procedure in collaborazione con l'Amministratore di sistema, in grado di garantire la continuità delle attività.

Si avvisano gli utenti che:

- tutta la posta elettronica in entrata è controllata da un software antispam. È comunque possibile che alcune mail di spam superino i filtri impostati sul sistema centrale: quindi è necessario prestare la massima attenzione a email sospette, avvisando l'Amministratore di sistema in caso di dubbi sulla provenienza/contenuto delle stesse.
- tutti i messaggi ricevuti, spediti o salvati, potranno essere letti dal Titolare esclusivamente nei seguenti casi:
  a. in caso di improvvisa assenza dell'utente al fine di garantire una regolare continuità dell'attività lavorativa;
  b. per motivi di sicurezza informatica.

In questi casi sarà data informazione all'utente dell'accesso eseguito.

12. NAVIGAZIONE INTERNET

L'accesso ad Internet (tramite PC, tablet o smartphone aziendali) è fornito allo scopo di consentire l'accesso alle informazioni necessarie all'attività lavorativa. Essendo uno strumento di lavoro, gli utenti cui si attribuisce l'accesso, sono responsabili del suo corretto utilizzo.

Si informa che il numero, la durata ed il contenuto degli accessi ad Internet sono costantemente registrati. La consultazione di tali registrazioni può avvenire solo in forma anonima e aggregata salvo i casi previsti dalla legge. Per prevenire eventuali abusi nell'uso di Internet il sistema è provvisto di filtri d'accesso. Si devono comunque osservare le seguenti regole di navigazione della rete Internet:

- è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore, che siano essi appartenenti a persone o aziende, coperti da *copyright*, brevetto o proprietà intellettuale, ivi compresa l'installazione o la distribuzione di software che non sia specificatamente licenziato per essere utilizzato all'interno dell'azienda;
- è tassativamente vietato navigare siti e scaricare materiale vietato o aventi contenuti illegali;
- è vietato effettuare copia non autorizzata di materiale coperto da copyright compreso, ma non limitato a, digitalizzazione e distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;
- è vietato utilizzare l'infrastruttura tecnologica aziendale per procurarsi e diffondere materiale in violazione

dellenormative vigenti.

- è vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati *all'host* dell'utente (*sniffing*);
- è vietato aggirare le procedure di autenticazione o la sicurezza di qualunque *host*, rete, *account*.

13. COMUNICAZIONE DI DATI E INFORMAZIONI ATTRAVERSO SOCIAL MEDIA

È assolutamente vietato pubblicare in internet attraverso Social media personali, forum, chat, blog, siti internet, dati ed informazioni di carattere aziendale e personale *(informazioni, documenti, appunti, commenti personali o di terzi, foto, video, audio, ecc.)* non autorizzati dal Titolare.

È invece autorizzata la divulgazione di informazioni già rese pubbliche dal Titolare.

14. GESTIONE DI DATI E INFORMAZIONI ATTRAVERSO SISTEMI WEB CLOUD

È vietato il salvataggio di dati e informazioni di carattere aziendale in sistemi cloud *(per esempio Dropbox, Google+, iCloud, Evernote, ecc.)* non autorizzati dal Titolare e dall'Amministratore di sistema.

15. SISTEMI DI MONITORAGGIO RETE AZIENDALE

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/ sostituzione/ implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali *(ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.),* comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Titolare, tramite l'Amministratore di sistema, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali.

Periodicamente e in presenza di anomalie (*intervento antivirus, segnalazione di rallentamenti del computer, utilizzo aziendalmente eccessivo dell'accesso Internet, dimensione elevata della casella di posta elettronica o dello spazio disco utilizzato, etc.),* l'amministratore di sistema effettuerà verifiche di funzionalità approfondite che potranno determinare segnalazione ed avvisi generalizzati diretti ai dipendenti della funzione in cui è stata rilevata l'anomalia stessa e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

16. STAMPANTI

È vietato l'utilizzo per fini personali dei sistemi multifunzione (*sistemi di stampa, copia ed invio fax)* e dei sistemi fax e aziendali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Titolare.

Si raccomanda di non lasciare documenti incustoditi presso i suddetti dispositivi.

17. SUPPORTI DI MEMORIZZAZIONE

Al termine dell'utilizzo dei supporti di memorizzazione contenenti dati *(chiavette USB, Hard Disk interni ed esterni),* questi dovranno essere cancellati, per eliminare ogni informazione contenuta prima di autorizzarne qualunque tipo di nuovo utilizzo. In caso di smaltimento di DVD e CD è obbligo la distruzione fisica del supporto.

18. STRUMENTI INFORMATICI PORTATILI

Gli strumenti informatici portatili (*notebook, tablet, smartphone*, supporti di memorizzazione, ecc..) devono essere custoditi dall'utente con cura e diligenza, prevenendo possibili danneggiamenti che ne compromettano il corretto funzionamento, evitando di lasciarli incustoditi in ambienti pubblici (ristoranti, treni, automobili, ecc..). Inoltre, di norma, non ne deve essere consentito l'utilizzo da parte di terzi (famigliari, amici, etc.). L'utilizzo degli strumenti informatici portatili messi a disposizione del Fondo è di responsabilità dell'utente e devono avvenire attraverso l'attivazione di una password o un PIN personale (attivazione dello screen saver automatico). Si raccomanda la massima attenzione nell'utilizzo di *App* sul proprio dispositivo, in relazione all'eccessivo consumo di traffico dati ed alla sicurezza del proprio apparato.

19. PRESCRIZIONE RESIDUALE

Per dubbi ed incertezze, in merito a come debba avvenire il trattamento dei dati e delle informazioni personali e aziendali, nonché sulle modalità di utilizzo degli strumenti di trattamento, è possibile chiedere al Titolare o all'Amministratore di sistema per ricevere le opportune istruzioni.

20. SANZIONI

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari, nonché con le azioni civili e penali consentite.

21. AGGIORNAMENTO E REVISIONE

Il presente Regolamento privacy del Fondo è soggetto a revisione periodica, opportunamente comunicata al personale.