# Regolamento del processo di governo degli accessi logici

Processo ***Gestione e controllo accessi logici***
Regolamento emesso il ***7/10/2021***
Aggiornato il 29/12/2022
Owner del processo: ***Organization & Business Continuity***

**Indice**

**INDICE** ..... **2**
**1 PREMESSA** ..... **3**
**2 AMBITO DI APPLICAZIONE** ..... **3**
2.1 RESPONSABILITÀ DEL DOCUMENTO ..... 3
2.2 OBIETTIVI DEL DOCUMENTO ..... 3
2.3 STRUTTURA DEL DOCUMENTO ..... 3
**3 GLI ATTORI COINVOLTI** ..... **4**
3.1 ORGANIZATION & BUSINESS CONTINUITY ..... 4
3.2 IT OPERATION SECURITY & GOVERNANCE ..... 5
3.3 DIREZIONE RISORSE UMANE DI BANCA MEDIOLANUM: ..... 5
3.4 RESPONSABILE DI PERSPECTIVE ..... 5
3.5 UFFICIO PRIVACY DI BANCA MEDIOLANUM ..... 5
**4 DEFINIZIONI** ..... **6**
**5 FASI DEL PROCESSO DI GOVERNO DEGLI ACCESSI LOGICI** ..... **6**
5.1 PROFILAZIONE UTENTI ..... 6
5.1.1 Definizione Permessi per Perspective ..... 6
5.1.2 Definizione Permessi Aggiuntivi per Singolo Utente ..... 7
5.1.3 Diritti di accesso privilegiato ..... 7
5.2 CONFERIMENTO ABILITAZIONI ACCESSI ..... 7
5.2.1 Attribuzione Profili ..... 7
5.3 MANUTENZIONE E CONTROLLO ACCESSI ..... 8
5.3.1 Attribuzione Nuovi Permessi a seguito di variazioni di Perspective ..... 8
5.3.2 Gestione Nuove Collaborazioni ..... 8
5.3.3 Sospensione Utente ..... 8
5.3.4 Revoca Utente ..... 9
5.3.5 Ricertificazione periodica dei permessi aggiuntivi ..... 9
5.3.6 Rivalutazione Permessi ..... 9
5.4 PRESIDIO DEL PROCESSO DI GESTIONE DEGLI ACCESSI LOGICI ..... 9
5.4.1 Ingaggio in fase di Project Design ..... 9
5.4.2 Definizione Profili Applicativi ..... 9
5.4.3 Aggiornamento Catalogo Applicazioni ..... 10
**6 NORMATIVA ESTERNA DI RIFERIMENTO** ..... **10**
**7 LE POLICY E LA NORMATIVA INTERNA DI RIFERIMENTO** ..... **10**

# 1 Premessa

Il presente Regolamento illustra i principi guida, l'architettura organizzativa e le interdipendenze alla base del processo di governo degli accessi logici ai sistemi applicativi che gestiscono i processi e le informazioni del cui trattamento ai sensi della normativa privacy vigente è Titolare Flowe società benefit S.p.A. (di seguito Flowe o la Società).

Sono esclusi i sistemi applicativi di altre società o che gestiscono informazioni di cui Flowe non è titolare ed a cui accedono i collaboratori (dipendenti o consulenti) della Società.

# 2 Ambito di Applicazione

Il processo descritto dal presente Regolamento si applica a tutte le unità organizzative (di seguito anche *Perspective*) di Flowe.

## 2.1 RESPONSABILITÀ DEL DOCUMENTO

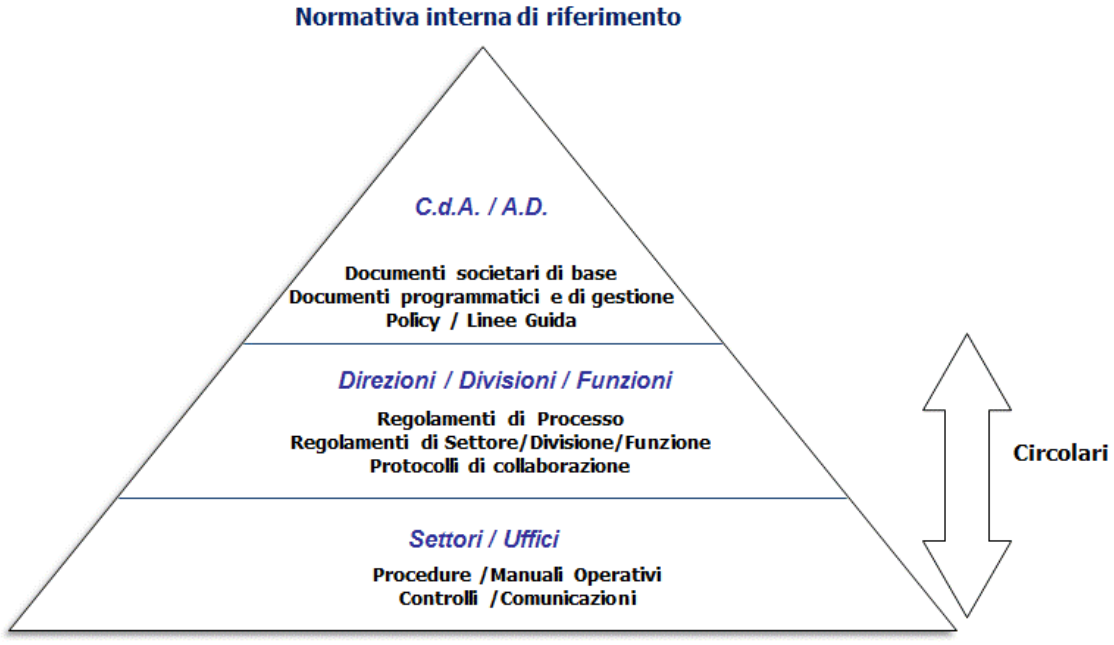
L'aggiornamento e la revisione del presente documento sono responsabilità di ***Organization & Business Continuity***.

## 2.2 OBIETTIVI DEL DOCUMENTO

Il presente documento ha l'obiettivo di:

- descrivere le diverse fasi del processo di governo degli accessi logici;
- richiamare ruoli e responsabilità degli attori coinvolti nel processo, in relazione all'assetto organizzativo di Flowe.

Con riferimento alla "*Policy di Gruppo sulle modalità di redazione, approvazione, diffusione ed aggiornamento della Normativa Interna*", il presente documento si colloca al secondo livello della piramide documentale richiamata nello schema seguente.




## 2.3 STRUTTURA DEL DOCUMENTO

Il Regolamento si compone complessivamente di 5 capitoli, oltre al presente.

Oggetto del presente documento è la regolamentazione dei principi e dei ruoli alla base della corretta gestione della sicurezza logica di Flowe.

Per sicurezza logica si intende l'insieme delle attività volte ad assicurare che le singole risorse del patrimonio della Società esposte ai rischi connessi alla gestione della sicurezza

siano accessibili esclusivamente alle persone/enti autorizzati nell'ambito delle loro competenze e secondo le *policy* aziendali e le normative vigenti.

È esclusa dal presente documento la sicurezza, sia fisica sia organizzativa, della infrastruttura dati.

Ai fini del presente documento, rientra nella categoria dei collaboratori tutto il personale interno ed esterno alla Società, inclusi ad esempio:

- i consulenti di tutte le *Perspective*;
- gli *Outsourcer* che pur non operando in sede accedono agli applicativi aziendali nell'ambito del loro incarico;
- i collaboratori occasionali quali stagisti e dipendenti interinali;
- gli ispettori / regolatori.

Di seguito sono descritte sinteticamente le principali tematiche trattate in ogni capitolo:

**Capitolo 3: Gli attori coinvolti**

Obiettivo del capitolo è descrivere e richiamare ruoli e responsabilità degli attori coinvolti nel processo oggetto del presente documento, definendo modalità di integrazione e di coordinamento previste nei casi di attività di carattere interfunzionale.

**Capitolo 4: Definizioni**

Nel capitolo è stata inserita una tabella di riferimento con le principali definizioni utilizzate nel presente documento.

**Capitolo 5: Fasi processo di governo degli accessi logici**

Obiettivo del capitolo è descrivere gli aspetti di carattere organizzativo il processo e le modalità di interazione con altre *Perspective* o le entità organizzative di società terze, interne o esterne al Gruppo Mediolanum in relazione al processo oggetto di regolamentazione, gli strumenti utilizzati e gli *output* attesi dalle fasi in cui il processo è articolato.

**Capitolo 6: Normativa esterna di riferimento**

Obiettivo del capitolo è descrivere il quadro normativo di riferimento rilevante per il processo oggetto di regolamentazione.

**Capitolo 7: Le policy e la normativa interna di riferimento**

Nel capitolo sono riportati le *policy* ed i principali riferimenti normativi in merito al processo operativo già emanati o recepiti dalla Società.

# 3 Gli attori coinvolti

Il modello organizzativo adottato dalla Società prevede il coinvolgimento delle *Perspective* della Società, di opportune funzioni della Capogruppo Banca Mediolanum (che svolgono in outsourcing servizi aziendali in virtù di un apposito accordo di esternalizzazione) e delle strutture organizzative degli *Outsourcer* tecnologici, che si impegnano, per quanto di competenza, ad applicare il presente regolamento.

Oltre alla definizione dei profili relativi a nuove applicazioni o ad applicazioni preesistenti, in coerenza rispetto alle regole normative ed alle *policy* aziendali in materia di sicurezza logica, le singole unità organizzative sono coinvolte nel processo di governo degli accessi logici secondo quanto dettagliato di seguito.

## 3.1 ORGANIZATION & BUSINESS CONTINUITY

*Organization & Business Continuity*:

- definisce, in collaborazione con le diverse *Perspective*, il *set* di permessi da assegnare in relazione al ruolo ed alle esigenze operative di ciascuna funzione coerentemente agli assetti ed agli ambiti di responsabilità delle strutture aziendali e nel rispetto dei principi del "minimo privilegio" e della "*segregation of duties*";

- verifica la coerenza dei profili censiti sugli applicativi aziendali rispetto alle regole normative ed alle *policy* aziendali in materia di sicurezza logica;
  valuta preventivamente le richieste di permessi aggiuntivi avanzate dagli utenti, verificandone la coerenza con le attività svolte e validandone l'attribuzione;
- effettua periodiche campagne di ricertificazione dei permessi abilitativi attribuiti ai dipendenti ed ai collaboratori aziendali
- controlla e sollecita l'effettiva esecuzione delle ricertificazioni ai referenti delle singole *Perspective* con il supporto di specifici *report*;
- verifica con cadenza almeno annuale, che non siano presenti utenze attive intestate a dipendenti o collaboratori dimessi e l'allineamento dei profili definiti e della profilatura degli utenti sui *"sistemi target";*
-

### 3.2 IT OPERATION SECURITY & GOVERNANCE

IT Operation Security & Governance all'interno della *Perspective Augmented Intelligence*:

- in coordinamento con *Organization & Business Continuity* attribuisce ai dipendenti ed ai collaboratori aziendali i diritti di accesso richiesti;
- collabora con *Organization & Business Continuity* per la verifica di coerenza dal punto di vista della sicurezza per le nuove richieste di abilitazione degli amministratori di sistema e per la revisione annuale degli stessi

### 3.3 DIREZIONE RISORSE UMANE DI BANCA MEDIOLANUM:

La *Direzione Risorse Umane di Banca Mediolanum*:

- censisce i dipendenti nell'applicativo specifico (a tempo determinato, indeterminato, interinali, stagisti, apprendisti);
- mantiene puntualmente aggiornato, in occasione di ogni modifica occorsa, l'archivio dei dipendenti (assunzioni, dimissioni, variazioni, etc.) e le informazioni in esso contenute, con particolare riferimento alla relativa *Perspective* di appartenenza, informazione determinante al fine della corretta e tempestiva attribuzione dei permessi di accesso;
- comunica tutte le variazioni ad *Organization & Business Continuity.*

### 3.4 RESPONSABILE DI PERSPECTIVE

Il Responsabile di *Perspective*:

- Comunica ad *Organization & Business Continuity* ogni variazione che interessi l'elenco dei propri collaboratori ;
- avanza le richieste di permessi aggiuntivi ad *Organization & Business Continuity*;
- collabora con *Organization & Business Continuity* nella verifica della correttezza dei diritti di accesso dei collaboratori appartenenti o che collaborano con la propria *Perspective*;
- effettua su indicazioni di *Organization & Business Continuity* la ricertificazione dei permessi associati alle risorse appartenenti o che collaborano con la propria *Perspective*;
- comunica tempestivamente alla *Direzione Risorse Umane di Banca Mediolanum*, e ad *Organization & Business Continuity* e *IT Operation Security & Governance* l'uscita del dipendente dalla *Perspective* per la corretta gestione del processo di ridefinizione dei diritti di accesso.

### 3.5 UFFICIO PRIVACY DI BANCA MEDIOLANUM

l'*Ufficio Privacy di Banca Mediolanum*:

- effettua valutazioni di coerenza in merito all'accesso ai dati nel rispetto del principio di minimizzazione, disciplinato dalla normativa *privacy* vigente.

## 4 Definizioni

| | |
|---|---|
| Permesso o privilegio | Configurazione di accesso (transazioni informative e/o dispositive) ad un determinato applicativo. |
| Permessi minimi (o diritti di accesso o modello) | Insieme di applicazioni e diritti di accesso ai dati, associati agli utenti di una specifica Perspective, nel rispetto del principio del minimo privilegio. |
| Permessi aggiuntivi | Permessi attribuiti ad uno o più risorse di una *Perspective*, oltre ai permessi minimi della stessa *Perspective*, per specifiche esigenze di tali utenti. |
| Profilatura | L'insieme di permessi minimi ed aggiuntivi di un determinato utente che definisce il *set* di transazioni a cui lo stesso è abilitato. |
| Manager approvatore | E' il responsabile gerarchico dell'utente richiedente che approva le richieste di accesso ai dati e sistemi applicativi da parte degli utenti che ne fanno richiesta. |
| Catalogo applicazioni | Elenco dei sistemi applicativi che gestiscono i processi e le informazioni della Società. |

## 5 Fasi del processo di Governo degli Accessi logici

Il processo di governo degli accessi logici si articola nelle fasi / sotto-processi riportati nello schema sotto riportato:


### 5.1 PROFILAZIONE UTENTI

Ad ogni utente viene attribuito un *set* di permessi strettamente necessari per lo svolgimento delle proprie mansioni (nel rispetto dei principi del *need to know* e del *least privilege*).
Al fine di governare le identità digitali di ciascun utente, Flowe ha scelto di adottare un modello operativo che prevede l'attribuzione di diritti d'accesso diversificati per ogni applicazione, oltre al *minimo privilegio* assegnato a tutte le risorse Flowe e utile a poter accedere ai siti e teams aziendali istituzionali ad uso interno.

#### 5.1.1 DEFINIZIONE PERMESSI PER PERSPECTIVE

Ad ogni dipendente o collaboratore esterno è associato un permesso preventivamente definito per la *Perspective* di appartenenza.

I permessi sono definiti da *Organization & Business Continuity* coerentemente con i ruoli e le mansioni attribuite alle diverse *Perspective*; secondo i principi contenuti nelle disposizioni emanate da EBA[1], agli utenti sono concessi i diritti di accesso alle risorse informatiche e ai loro sistemi di supporto sulla base di quanto è necessario sapere (principio del "need to

[1] Orientamenti dell'ABE sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) e di sicurezza del 28/11/2019

know") e che sono strettamente necessari per l'esecuzione dei loro compiti (principio del "least privilege"), in modo da impedire l'accesso ingiustificato a un'ampia serie di dati o l'assegnazione di combinazioni di diritti di accesso che possono essere utilizzati per aggirare i controlli (principio della "segregation of duties").

Il processo di gestione dei permessi si articola in due sotto-fasi:

- definizione permessi: *Organization & Business Continuity*, in collaborazione con il responsabile di *Perspective*, definisce i profili necessari da assegnare in relazione al ruolo ed alle esigenze operative di ciascuna funzione, coerentemente agli assetti ed agli ambiti di responsabilità delle strutture aziendali. I requisiti di ciascun responsabile di *Perspective*, vengono raccolti in un apposito template che viene valutato da *Organization & Business Continuity. In caso di dubbi sulla corretta applicazione dei requisiti in ambito, viene richiesto il supporto consulenziale,* all'*Ufficio Privacy di Banca Mediolanum* che effettua valutazioni di coerenza in merito all'accesso ai dati nel rispetto del principio di minimizzazione, disciplinato dalla normativa privacy vigente;
- creazione permessi: *IT Operation Security & Governance* in coordinamento con *Organization & Business Continuity*, sulla base dei requisiti forniti dai responsabili delle *Perspective*, individua i profili utili alla creazione dei permessi garantendo il rispetto del principio di segregation of duties.

#### 5.1.2 DEFINIZIONE PERMESSI AGGIUNTIVI PER SINGOLO UTENTE

Eventuali permessi aggiuntivi a quelli assegnati alle *Perspective* possono essere richiesti tramite messaggio e-mail dall'utente stesso o da un altro utente della stessa *Perspective*, compilando un apposito template che include i razionali della richiesta.

Il processo prevede una prima autorizzazione da parte del proprio responsabile gerarchico ed una successiva autorizzazione da parte di *Organization & Business Continuity* che verifica la coerenza con le attività svolte dalla *Perspective* a cui appartiene l'utente che ne fa richiesta.

#### 5.1.3 DIRITTI DI ACCESSO PRIVILEGIATO

Flowe controlla costantemente l'attività degli utenti in possesso di accessi privilegiati (es. amministratori di sistema) l'attività è comunque registrata in appositi log di sistema che non sono alterabili in alcun modo.

Le attività di manutenzione ordinaria e straordinaria che richiedono l'utilizzo delle abilitazioni di amministratore di sistema sono preventivamente concordate con il Responsabile di *Organization & Business Continuity* o con un suo delegato che ne verifica la coerenza, anche da un punto di vista sicurezza, in collaborazione con *IT Operation Security & Governance*.

Al fine di garantire la sicurezza delle comunicazioni e ridurre il rischio, l'accesso amministrativo da remoto è concesso esclusivamente sulla base delle esigenze conoscitive contingenti e qualora siano applicate soluzioni di autenticazione forte.

### 5.2 CONFERIMENTO ABILITAZIONI ACCESSI

È l'attività in base alla quale a ciascun utente viene assegnato il relativo profilo di accesso alle risorse aziendali per lo svolgimento dei relativi compiti operativi/decisionali.

#### 5.2.1 ATTRIBUZIONE PROFILI

L'attribuzione dei profili ad una risorsa, derivanti da permesso minimo o da richiesta di permesso aggiuntivo, viene effettuata da *IT Operation Security & Governance* in coordinamento con *Organization & Business Continuity*.

L'attribuzione può avvenire in due modalità distinte a seconda dell'applicazione/strumento:

- modalità automatica: per alcune applicazioni/strumenti, l'abilitazione avviene direttamente con l'ausilio di un "connettore" che provvede ad abilitare l'utente attraverso un flusso automatico, dopo l'approvazione di *Organization & Business Continuity*. *IT Operation Security & Governance* ha il compito di gestire eventuali 'scarti' generati dal processo di attribuzione automatico dei profili;
- modalità manuale: per le applicazioni/servizi che non prevedono l'utilizzo di un "connettore", l'abilitazione viene effettuata manualmente da *IT Operation Security & Governance,* in coordinamento con la funzione *Organization & Business Continuity di Flowe,* con l'intervento diretto sul sistema *target*, attraverso l'invio di un ticket o di un messaggio di posta elettronica al Manager Approvatore , qualora *IT Operation Security & Governance* non abbia la possibilità di intervenire direttamente sullo strumento.

## 5.3 MANUTENZIONE E CONTROLLO ACCESSI

Sono le attività mirate a garantire un costante aggiornamento dei permessi rilasciati al singolo utente, tramite i processi di:

- attribuzione di nuovi permessi a seguito della variazione della *Perspective* di appartenenza;
- ricertificazione periodica dei permessi aggiuntivi;
- rivalutazione dei permessi.

### 5.3.1 ATTRIBUZIONE NUOVI PERMESSI A SEGUITO DI VARIAZIONI DI PERSPECTIVE

Nel caso in cui un utente o un gruppo di utenti, vari la *Perspective* di appartenenza, questa lo comunica a *Organization & Business Continuity*, che dopo le opportune valutazioni richiede a *IT Operation Security & Governance* la revoca dei permessi e degli eventuali permessi aggiuntivi della *Perspective* precedente e l'attribuzione dei permessi della nuova *Perspective*.

### 5.3.2 GESTIONE NUOVE COLLABORAZIONI

In caso di collaboratori interni, per poter assegnare il set di permessi all'utente è necessario che il dipendente sia stato preventivamente censito nell'applicativo specifico da parte della *Direzione Risorse Umane di Banca Mediolanum* (a tempo determinato, indeterminato, interinali, stagisti, apprendisti).

Per i collaboratori esterni (*Outsourcer* di processo, fornitori/consulenti a progetto, consulenti occasionali) è compito del Responsabile di riferimento provvedere a richiedere il censimento/gestione dei relativi profili dei collaboratori esterni della Società.

### 5.3.3 SOSPENSIONE UTENTE

Analogamente all'inserimento, anche la sospensione di una utenza di un collaboratore interno (es. maternità) ha origine dalla registrazione dell'evento nell'applicativo specifico della *Direzione Risorse Umane di Banca Mediolanum* ed in quello della gestione dei profili di abilitazione dei collaboratori.

I privilegi di accesso alle informazioni, compresi eventuali diritti che governano funzionalità dispositive, vengono revocati e successivamente riassegnati nel momento in cui viene registrato nell'applicativo specifico della *Direzione Risorse Umane di Banca Mediolanum* il re-inserimento della risorsa nella stessa *Perspective*.

Qualora la risorsa venga assegnata ad altra *Perspective*, verrà assegnato il permesso minimo previsto dalla nuova *Perspective*.

#### 5.3.4 REVOCA UTENTE

Analogamente all'inserimento, anche la dismissione di una utenza di un collaboratore dipendente ha origine dalla registrazione dell'evento nell'applicativo specifico della *Direzione Risorse Umane di Banca Mediolanum* cui segue la registrazione sull'applicativo che gestisce i profili di abilitazione dei collaboratori o la comunicazione *a Organization & Business Continuity*.

Per i collaboratori esterni il Responsabile di riferimento deve modificare l'anagrafica direttamente sull'applicativo che gestisce i profili di abilitazione dei collaboratori o comunicandolo a *Organization & Business Continuity*, inserendo/modificando la data di fine collaborazione.

Indipendentemente dalle richieste di disabilitazione pervenute, *Organization & Business Continuity* verifica periodicamente, con cadenza almeno annuale, che non siano presenti utenze attive intestate a dipendenti o collaboratori dimessi, tracciando e conservando gli esiti delle analisi svolte.

In caso di dimissioni o di cessata collaborazione, tutti i privilegi di accesso alle informazioni, compresi i diritti che governano funzionalità dispositive, qualora presenti, vengono revocati.

#### 5.3.5 RICERTIFICAZIONE PERIODICA DEI PERMESSI AGGIUNTIVI

Con frequenza almeno annuale, viene avviato il processo di ricertificazione dei permessi aggiuntivi, attraverso il quale ciascun Responsabile conferma o modifica il perimetro dei permessi aggiuntivi associati ad ogni utente appartenente o che collabora con la propria *Perspective*.

*Organization & Business Continuity* ha il compito di avviare operativamente il processo di ricertificazione avvalendosi del supporto di *IT Operation Security & Governance*.

#### 5.3.6 RIVALUTAZIONE PERMESSI

*Organization & Business Continuity*, con il supporto di apposita reportistica, si occupa di valutare l'assetto dei permessi al fine di individuare eventuali esigenze che possono essere risolte con la modifica dei permessi associati alle singole *Perspective*.

Analogamente, la richiesta di ampliamento dei permessi può nascere dall'esigenza dei responsabili delle singole *Perspective*, qualora abbiano necessità di estendere a tutte le risorse della propria funzione l'abilitazione ad uno o più profili necessari per lo svolgimento della propria attività.

### 5.4 PRESIDIO DEL PROCESSO DI GESTIONE DEGLI ACCESSI LOGICI

Organization & Business Continuity, presidia la complessiva adeguatezza del processo di gestione degli accessi logici, attraverso il monitoraggio (con reportistica dedicata) di tutte le attività descritte nel presente documento, valutandone i rischi o le inefficienze associate (es.: i rischi operativi o in ambito *privacy* associati alla revoca di permessi legati alla precedente mansione; le inefficienze derivanti da *backlog* di attività o dalla mancata attribuzione di permessi a nuove risorse o i rischi).

#### 5.4.1 INGAGGIO IN FASE DI PROJECT DESIGN

È responsabilità dei *Project Mana*ger coinvolgere tempestivamente *Organization & Business Continuity* all'avvio di progetti di sviluppo di nuove applicazioni o nei casi di definizione di nuovi profili per applicazioni preesistenti.

#### 5.4.2 DEFINIZIONE PROFILI APPLICATIVI

*Organization & Business Continuity* definisce, dove necessario, in collaborazione con le *Perspective* coinvolte nell'operatività sulla nuova applicazione, il *set* di permessi da assegnare in relazione al ruolo ed alle esigenze operative di ciascuna unità.

### 5.4.3 AGGIORNAMENTO CATALOGO APPLICAZIONI

Nella fase di sviluppo del progetto, è responsabilità del *Project Manager* coinvolgere tempestivamente *Organization & Business Continuity* affinché si attivi per valutare ed avviare le attività necessarie per il censimento del nuovo strumento nel Catalogo Applicazioni. *Organization & Business Continuity* provvederà anche ad aggiornare il Catalogo Applicazioni in caso di dismissione di applicazioni in uso.

.

## 6 Normativa esterna di riferimento

Si riportano di seguito i principali riferimenti normativi:

- D.lgs. 196 del 30 giugno 2003 “Codice in materia di protezione dei dati personali” integrato con le modifiche introdotte dal D.lgs. del 10 agosto 2018, n. 101, recante “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)” (in G.U. 4 settembre 2018 n.205)
- Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica, provvedimento della Banca d’Italia del 23 luglio 2019;
- Regolamento (UE) n. 2016/679 - GDPR (*General Data Protection Regulation*)
- Orientamenti dell’ABE sulla gestione dei rischi relativi alle tecnologie dell’informazione e della comunicazione (*Information and Communication Technology - ICT*) e di sicurezza del 28/11/2019.

## 7 Le policy e la normativa interna di riferimento

Si riepilogano le fonti informative interne alla Società che presentano relazioni con il processo in esame:

- *Policy* di Sicurezza (approvata dal CdA di Flowe del 17/10/2022)