GRUPPO CASSA CENTRALE
CREDITO COOPERATIVO ITALIANO

METODOLOGIA DI GRUPPO

per l'esecuzione del Data Protection Impact Assessment (DPIA)

Fonte Normativa: Metodologia

Approvato dal Consiglio di Amministrazione

Data della Delibera: 20 gennaio 2021

Owner		Autore
DPO		Servizio Data Protection
Destinatari		
Capogruppo e Società del Gruppo		
N° Versione	Data di approvazione in CdA di Capogruppo	Note
1	20 gennaio 2021	Prima versione

5. Sommario

1. Glossario

Ai fini della presente Metodologia si intende per:

Banca/Banche affiliata/e: singolarmente ovvero collettivamente le Banche di Credito Cooperativo, le Casse Rurali e/o le Casse Raiffeisen aderenti al Gruppo Bancario Cooperativo, in quanto soggette all'attività di direzione e coordinamento da parte della Capogruppo in virtù della sottoscrizione del Contratto di Coesione.

Capogruppo: Cassa Centrale Banca – Credito Cooperativo Italiano S.p.A. in qualità di Capogruppo del Gruppo Bancario Cooperativo.

Consiglio di Amministrazione (CdA): Organo con funzione di supervisione strategica.

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 o sociale;

"Data Protection Officer" o **"DPO"**: il soggetto designato dal Titolare del trattamento per assolvere funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR;

Funzioni Competente: la persona fisica, o giuridica, in possesso di informazioni e competenze utili alla risoluzione delle esigenze manifestate dal Titolare del Trattamento;

Garante: autorità garante per la protezione dei Dati personali;

GDPR: regolamento UE 2016/679 in materia di protezione dei Dati personali;

Interessati: interessati al trattamento, persona fisica o giuridica, compreso un'autorità pubblica e un organismo di diritto pubblico, che utilizza o richiede servizi di trattamento di dati;

Policy: la Policy in materia di protezione dei Dati personali;

Privacy by default: il principio che richiede al Titolare di predisporre misure tecniche e organizzative tali da garantire che, per impostazione predefinita, siano trattati esclusivamente i Dati personali necessari per ogni specifica finalità del trattamento, ad esempio riducendo la quantità di Dati

raccolti, la portata del trattamento, il periodo di conservazione e il numero di soggetti che hanno accesso ai Dati personali;

Privacy by design: il principio che prescrive al Titolare di adottare sia al momento della determinazione dei mezzi del trattamento che all'atto del trattamento stesso misure tecniche e organizzative adeguate a garantire il rispetto del GDPR e la tutela dei diritti e delle libertà degli interessati;

Referente Privacy: il soggetto interno alla realtà aziendale del Titolare che supporta il DPO nello svolgimento delle sue funzioni;

Registro: il registro adottato dal Titolare al fine di annotare tutte le attività di trattamento svolte sotto la propria responsabilità, contenenti le informazioni di cui all'articolo 30 GDPR;

Requisiti Funzionali: insieme delle caratteristiche, sia tecniche relative all'implementazione di eventuali soluzioni tecnologiche, sia organizzative, che potrebbero comprendere, a titolo esemplificativo ma non esaustivo, la descrizione del funzionamento di eventuali applicazioni, le categorie di dati personali impiegate, i protocolli di sicurezza nonché la descrizione di tutte le qualità utili per la migliore definizione del progetto stesso;

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, o altro organismo che tratta Dati personali per conto del Titolare del trattamento;

Società del Gruppo/Società: le Banche affiliate, le società da queste controllate, direttamente o indirettamente, e le altre Banche, Società prodotto, Società finanziarie, Società servizi e strumentali controllate, direttamente e/o indirettamente, dalla Capogruppo.

Soggetto Designato: la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile;

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. Ai fini della presente Procedura, il Titolare coincide con Cassa Centrale Banca Credito Cooperativo Italiano S.p.A.;

"Valutazione di impatto sulla protezione dei dati" o **"Data Protection Impact Assessment (DPIA)"**: valutazione di impatto sulla protezione dei Dati effettuata dal Titolare quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

2. Premessa

2.1. OBIETTIVI DEL DOCUMENTO

Il presente documento fornisce la metodologia per la conduzione, conforme alla Normativa Privacy, del Data Protection Impact Assessment ("DPIA")

Il DPIA è lo strumento preventivo utilizzato dal Titolare del trattamento al fine di identificare, valutare e gestire in anticipo quali sono i potenziali rischi ai quali sono esposte le persone fisiche in funzione delle attività di trattamento effettuate sui dati delle stesse. In pratica, il DPIA consente di determinare il livello di rischio che incombe sui dati degli interessati e stabilire le contromisure più appropriate per mitigare i rischi, mediante la riduzione dell'impatto e delle probabilità di accadimento delle Minacce che potrebbero avere riflessi per le libertà e i diritti degli Interessati, a un livello considerato accettabile.

2.2. ADOZIONE, AGGIORNAMENTO E DIFFUSIONE DEL DOCUMENTO

La presente metodologia e i suoi relativi aggiornamenti sono approvati dal Consiglio di Amministrazione della Capogruppo.

Il DPO verifica nel continuo e comunque con cadenza annuale la complessiva idoneità del Documento ad ottemperare a quanto previsto dalla vigente Normativa Privacy, tenendo conto, tra l'altro, delle modifiche eventualmente intervenute, degli assetti organizzativi del Titolare del Trattamento, nonché dell'efficacia dimostrata dalle procedure nella prassi applicativa.

La Metodologia si applica a tutte le Società del Gruppo/Banche affiliate ed è trasmessa alle stesse per il recepimento e la relativa attuazione.

2.3. CONTESTO NORMATIVO DI RIFERIMENTO

- Regolamento europeo 2016/679 "*General Data Protection Regulation* (GDPR)".
- Privacy Impact Assessment (PIA) 1: methodology e Privacy Impact Assessment (PIA) 3: knowledge bases: Fonte CNIL.

- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato ai sensi del regolamento 2016/679 (WP 248).
- Orientamenti sulla valutazione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) a norma del processo di revisione e valutazione prudenziale (SREP), EBA.

3. Funzioni, ruoli e responsabilità

Di seguito si riporta il dettaglio delle funzioni e dei ruoli, con le relative responsabilità, coinvolti nel processo di DPIA.

Richiedente	È il Responsabile della Funzione che richiede l'implementazione e quindi ha la responsabilità dell'esecuzione e della compilazione del DPIA. Se il Richiedente è diverso dall'Utente Responsabile/Focal Point, deve accordarsi con quest'ultimo per la compilazione. Il Richiedente è colui che è responsabile del trattamento oggetto del DPIA.
Utente Responsabile (Focal Point)	È la figura aziendale identificata per ciascuna Applicazione IT e che ne assume formalmente la responsabilità, in rappresentanza degli utenti e nei rapporti con con le funzioni preposte allo sviluppo e alla gestione tecnica. L'Utente Responsabile potrebbe coincidere con il Richiedente e con il Data Owner. Per un singolo progetto potrebbero essere interessati più Utenti Responsabili.
Servizio DP/Referente Privacy	La funzione che esprime un giudizio in merito allo stato di compilazione e all'adeguatezza delle informazioni raccolte, necessarie per l'esecuzione della valutazione d'impatto. I controlli di conformità vengono eseguiti dal: • Referente Privacy per i progetti eseguiti da una singola banca; • Servizio DP di Cassa Centrale Banca per i progetti eseguiti dalla capogruppo;

	• Referente Privacy di Allitude per i progetti che prevedono il coinvolgimento dei servizi IT erogati da Allitude.
DPO	Data Protection Officer che opera ai sensi del Regolamento Europeo 679/2016 e che supporta la il Richiedente e l'Utente Responsabile nella esecuzione della Valutazione d'Impatto Privacy (DPO).
Servizio Governo e Sicurezza ICT	Funzione dedicata alla sicurezza dei sistemi informativi aziendali.
Cda	Consiglio di Amministrazione della società che delibera l'approvazione della valutazione d'impatto privacy (DPIA) per i trattamenti con rischio alto/medio alto nonché delibera su un eventuale interpello del Garante.

4. Metodologia di valutazione d'impatto

La presente metodologia deve essere seguita sin dalla fase di sviluppo, progettazione o selezione di qualsiasi iniziativa di business, progetto o implementazione tecnologica, che possa implicare un trattamento di Dati personali che ricade in uno delle tipologie, descritte nella tabella riportata al Capitolo 4 "Analisi preliminare del rischio".

Le tipologie riportate nelle tabelle citate sono state ricavate prendendo a riferimento:

- l'elenco dei trattamenti soggetti a DPIA pubblicato dal Garante con provvedimento n. 467 del 11 ottobre 2018;
- i criteri individuati dal WP29 (Comitato dei Garanti privacy europei) all'interno delle Linee Guida WP248 rev. 01 del 4 ottobre 2017 in materia di valutazione d'impatto.

4.1. CRITERI DI VALUTAZIONE

Nei capitoli relativi allo svolgimento del DPIA viene chiesto, al Servizio DP per i progetti curati dalla capogruppo Cassa Centrale Banca, o al referente Privacy per le Banche Affiliate, di esprimere un giudizio in merito allo stato di compilazione delle informazioni necessarie per l'esecuzione della

valutazione d'impatto (parere). Il riquadro dedicato a riportare il giudizio dii valutazione si presenterà come segue.

Valutazione	ADEGUATA
Commento: nessuno	

Il giudizio di valutazione può assumere i seguenti valori:

- **da correggere**: le informazioni fornite non sono sufficienti per esprimere una valutazione. Qualora sia indicato questo giudizio il Richiedente sarà tenuto a integrarne il contenuto;
- **adeguata:** le informazioni fornite sono adeguate e il trattamento è conforme e protegge in modo adeguato i dati personali;
- **migliorabile:** le informazioni fornite sono sufficienti ma devono essere adottate delle azioni correttive per rendere conforme o migliorare la sicurezza del trattamento. In questo caso devono essere descritte le azioni correttive che faranno parte integrante del piano delle azioni correttive.

Questa valutazione è necessaria affinché il DPO possa esprimere il suo parere.

5. Analisi preliminare del rischio

L'analisi preliminare del rischio privacy deve essere eseguita:

- per quanto riguarda i progetti promossi dalla Capogruppo, all'interno del "Processo Demand" nella fase di analisi dei requisiti prima dell'istituzione di un nuovo trattamento;
- per quanto riguarda i progetti promossi di iniziativa dalla Società nella fase iniziale di definizione dei requisiti del progetto stesso.

Se un trattamento di dati personali utilizzando nuove tecnologie, tenendo conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, può provocare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve, **prima di procedere al trattamento**, effettuare una valutazione dell'impatto delle operazioni di trattamento (DPIA). Una singola valutazione può riguardare un insieme di operazioni di elaborazione analoghe che presentano rischi elevati simili.

Il ***Richiedente***, per valutare se il trattamento può costituire un rischio elevato per i diritti e le libertà dell'individuo, deve verificare se tale trattamento rientra in una delle tipologie, descritte nella tabella di seguito riportata, che richiede l'esecuzione della valutazione d'impatto privacy (DPIA).

Anche la presenza di un'unica corrispondenza richiede lo svolgimento di un DPIA.

Sono svolti **trattamenti valutativi o di scoring su larga scala, profilazione, attività predittive** effettuate anche on-line o attraverso app, **relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato**	☐
ESEMPI: • lo screening dei propri clienti utilizzando un database di rischio creditizio • lo screening dei propri clienti utilizzando un database per la lotta alle frodi o al riciclaggio e al finanziamento del terrorismo (AML/CTF); • creazione profili comportamentali o di marketing a partire dalle operazioni o dalla navigazione compiute sul proprio sito web; • la classificazione dei clienti in base ai loro dati personali con finalità di comunicazioni commerciali; • l'esame delle operazioni conformemente al diritto applicabile per individuare eventuali operazioni fraudolente.	
Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi);	☐
ESEMPI: • il trattamento può comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione • valutazione automatizzata del personale ("se ricadi nella decade percentile più bassa per numero di pratiche evase, riceverai una valutazione di "insoddisfacente" senza possibilità di discussione); • screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento; • un istituto finanziario o una centrale rischi per il credito che tenga conto della differenza di età fra i coniugi al fine di definire l'affidabilità creditizia (il che può ostacolare il libero esercizio del diritto; • database negativi (di esclusione rispetto a determinate prestazioni) fondamentale di contrarre matrimonio); **Eccezione**: l trattamento che produce effetti minimi o nulli su un interessato non soddisfa questo specifico criterio.	
Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci **in grado di**	☐

identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Questa tipologia di monitoraggio costituisce un criterio, ai fini della DPIA, in quanto la raccolta di dati personali può avvenire in circostanze tali da non consentire agli interessati di comprendere chi vi stia procedendo e per quali finalità.	

ESEMPI:

- Analisi del traffico Internet;
- Videosorveglianza intelligente (ossia, associata a software per il riconoscimento del volto) in luoghi pubblicamente accessibili;
- Strumenti per la prevenzione della perdita di dati
- Trattamento di metadati (tempo, natura, durata di una transazione bancaria) per scopi organizzativi o per ricavare stime di bilancio

Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza, etc.;

Trattamenti su larga scala di dati aventi carattere estremamente personale quali ad esempio i dati economico-patrimoniale o di pagamento i dati di accesso e di identificazione (username, password, customer ID, altro…), i dati di posizione/localizzazione (es. GPS) i dati oggetto di scambio di comunicazioni (mail, registrazioni telefoniche…), dati di traffico telematico, telefonico (es. log navigazione siti web, indirizzo IP), diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone :	☐

ESEMPI:

Tali dati personali sono considerati essere sensibili perché:

- sono legati ad attività a carattere personale o domestico (un datore di lavoro che acceda a documenti privati, e-mail personali, diari o appunti tratti da lettori elettronici dotati di strumenti per la presa di appunti e di proprietà del personale, oppure utilizzati dal personale per scopi sia privati sia professionali, per esempio in contesti BYOD – Bring Your Own Device).
- influenzano l'esercizio di un diritto fondamentale (un datore di lavoro che accede a informazioni strettamente personali contenute in applicazioni che registrano le attività quotidiane delle persone, oppure che utilizzi informazioni tratte dai social media in contesti che possono avere impatti significativi sugli interessati, per esempio ai fini del reclutamento occupazionale o in rapporto a colloqui di lavoro oppure i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione);
- la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti)

Eccezioni: A tale proposito, può essere pertinente la circostanza per cui i dati siano già stati resi pubblici dall'interessato ovvero da terzi. Il fatto che un certo dato personale sia disponibile

pubblicamente può essere un elemento da prendere in esame nel valutare l'aspettativa di un utilizzo ulteriore di tale dato per determinati scopi.	
Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti.	☐
Trattamenti non occasionali di dati relativi a soggetti vulnerabili:	☐
Esempio: La categoria degli interessati vulnerabili comprende anche: • i minori • i dipendenti, • quei segmenti di popolazione particolarmente vulnerabile e meritevole di specifica tutela (soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti) • ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento.	
Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;	☐
Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment) e in particolare, a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato.	☐
• Verifiche incrociate e non trasparenti delle registrazioni sugli accessi, degli accessi informatici, e delle dichiarazioni rese ai fini della compensazione oraria, per individuare casi di assenteismo; • Un'agenzia fiscale che confronti i dati delle dichiarazioni dei redditi con gli atti di proprietà relativi a imbarcazioni di pregio, al fine di individuare potenziali evasori fiscali.	
Trattamenti di categorie particolari di dati oppure di **dati relativi a condanne penali e a reati.**	☐
ESEMPI: • Dati particolari: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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 giudiziari (relativi a condanne penali o reati).	
Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento;	☐
Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	☐
Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo);	☐
Esempio IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking	

Nel caso in cui il trattamento previsto per la realizzazione del nuovo progetto/servizio non rientri in una delle casistiche sopra esposte e quindi non presenti dei rischi elevati per i diritti e le libertà degli interessati, **il *Richiedente* formalizza tale scelta** motivando le ragioni per le quali non è necessario svolgere un DPIA. Procederà comunque a supervisionare le successive fasi di esecuzione del progetto al fine di assicurare la sua conformità ai principi delineati nell'apposita procedura di Privacy by design.

Il ***Richiedente*** può comunque **consultare il *Referente Privacy/Servizio DP*,** o in alternativa il ***DPO***, per chiedere un parere in merito alla necessità o meno di condurre un DPIA in particolare quando il trattamento può presentare rischi per i diritti e le libertà degli interessati.

Nel caso in cui il *Richiedente* riscontri la necessità di eseguire un DPIA, deve redigere apposita documentazione con le modalità e contenuti indicati nel seguito.

6. Descrizione del contesto

6.1 CICLO DI VITA DEL DATO ALL'INTERNO DEL TRATTAMENTO

Al fine di valutare, anche sotto il profilo della sicurezza, se il trattamento oggetto di analisi comporta un rischio e, in particolare, un rischio elevato per i diritti e le libertà delle persone fisiche il ***Richiedente*** deve ricostruire, supportato dall'***Utente Responsabile,*** il ciclo di vita dei dati personali impiegati nel trattamento oggetto di DPIA.

In particolare, la descrizione de**l ciclo di vita** deve descrivere i seguenti punti.

6.1.1 DESCRIZIONE DEI DATI TRATTATI E DELLE MODALITÀ DI RACCOLTA

In tale sezione vanno indicate le tipologie di dati oggetto del trattamento e una descrizione delle maggiori caratteristiche. In particolare, dovranno essere indicati se i dati sono:

- **conferiti dall'interessato**: il ***Richiedente*** deve descrivere i dati personali raccolti quali ad esempio: dati anagrafici (nome, cognome, codice fiscale); altri dati accessori (quali l'indirizzo email) e le modalità con le quali sono stati raccolti (ad esempio all'atto dell'apertura dell'anagrafica, in fase di sottoscrizione della newsletter, tramite dei moduli web, moduli cartacei, campionamenti e sondaggi, registrazioni audio e video, fonti esterne o pubbliche come i social network, acquisiscono attraverso sensori, ecc.etc.);

- **osservati forniti dall'utilizzatore** tramite la fruizione di un servizio: il ***Richiedente*** deve descrivere i dati economico/finanziari; dati contenuti negli estratti conto e nelle movimentazioni bancarie relativi ai rapporti intrattenuti dalla clientela con la banca; acquisto/vendita strumenti finanziari; ordini di acquisto formulati telefonicamente;
- **dati inferenziali e derivati:** sono dati prodotti da elaborazioni di tipo statistico, matematico o altri metodi di analisi effettuate dal titolare sulla base dei dati "forniti dall'interessato". Sono ad esempio: Set di dati prodotti da elaborazioni di tipo statistico, matematico o altri metodi di analisi; Valutazione o profilazione ai fini antiriciclaggio; Valutazione (score) propensione al rischio; Valutazione (score) solvibilità creditizia; Profilazione scelte di acquisto; Profilazione relativa al nucleo familiare; Profilazione ai fini scelte di investimento; Dettagli dei segmenti nei quali l'interessato è stato inserito.

6.1.2 DESCRIZIONE PROCESSO DI ELABORAZIONE

A seguire dovranno invece essere le descritte le varie fasi di processo del trattamento. Ogni fase deve essere descritta indicando i seguenti elementi.

A. Attività di elaborazione di dati personali

Nel documento di DPIA deve essere compilato il seguente box.

Attività del processo	Descrizione dell'operazione o insieme di operazioni eseguite su dati personali o set di dati personali, mediante procedure automatizzate o manuali; In ogni fase o nell'insieme delle fasi del ciclo di vita, vengono effettuate specifiche attività [1] necessarie a conseguire le finalità oggetto del trattamento. È importante descrivere in dettaglio tutte le attività o operazioni effettuate su dati personali con l'obiettivo di comprendere i possibili rischi a cui i dati possono essere esposti. In pratica, un trattamento può essere identificato come l'insieme di operazioni effettuate per raggiungere un determinato scopo che trova legittimazione nella stessa base giuridica. Ogni trattamento comprenderà una serie di operazioni come raccolta, registrazione, organizzazione, strutturazione, consultazione o utilizzo dei dati.

1 Un'attività o un'operazione può essere considerata, ad esempio, l'acquisizione di dati mediante un modulo web, il filtraggio delle informazioni attraverso un processo di profilazione, un processo di crittografia, cancellazione o qualsiasi attività che richieda l'elaborazione o la manipolazione dei dati.

B. Attori e ruolo

Nel documento di DPIA deve essere compilato il seguente box.

Attori e ruolo	I soggetti che prenderanno parte al trattamento in qualità di Titolare o Responsabile

C. Utilizzatori

Nel documento di DPIA deve essere compilato il seguente box.

Utilizzatori	Durante tutto il ciclo di vita dei dati potrebbero essere coinvolti numerosi attori, Individui o persone giuridiche che devono essere identificati, individualmente o collettivamente chiarendo i relativi ruoli e responsabilità. Fra i destinatari del trattamento devono essere citati, quando previsto, il personale delle funzioni deputate al trattamento designate dal Titolare, i responsabili nonché eventuali altri destinatati a cui verranno comunicati i dati che operano nella qualità di Titolari autonomi. La partecipazione dei destinatari al trattamento costituisce un fattore di rischio da rilevare all'interno del DPIA.

D. Asset che gestiscono le informazioni

Nel documento di DPIA deve essere compilato il seguente box.

Tecnologia/servizio	In questa sezione deve essere riportata la tecnologia/servizio utilizzato nella specifica fase del trattamento

E. Periodo di conservazione

Laddove applicabile, nel documento di DPIA deve essere compilato il seguente box.

Periodo di conservazione	In questa sezione deve essere riportato il periodo di conservazione dei dati presenti sulla piattaforma utilizzata per l'elaborazione.

6.1.3 MODALITÀ DI DISTRUZIONE

Quale ultimo elemento devono essere descritte le modalità con le quali i dati, che possono essere contenuti nei sistemi o nei file, saranno eliminati in modo che non possano essere

recuperati dai supporti; la cancellazione dei dati avviene secondo i criteri di conservazioni compresi quelli relativi alla detenzione obbligatori ai sensi di norme di legge e/o detenzione per fini, giustificati, stabiliti dal Titolare del Trattamento.

7. Necessità e proporzionalità del trattamento

7.1 FINALITÀ SPECIFICHE, ESPLICITE E LEGITTIME (ART. 5.1 B) DEL GDPR

Il richiedente deve attestare che i dati personali saranno raccolti per perseguire finalità:

- **Specifiche**, le motivazioni alla base della raccolta e trattamento dati devono essere chiare e circoscritte. Non sono pertanto ammesse indicazioni generiche ovvero finalità in corso di definizione, indefinite e/o illimitate.
- **Esplicite,** le finalità devono essere sufficientemente inequivocabili e chiaramente espresse in modo quindi non ambiguo. L'interessato deve, quindi, essere messo a conoscenza dei motivi per i cui i suoi dati sono trattati.
- **Legittime,** le finalità del trattamento devono essere lecite rispetto alla normativa applicabile. Non sono ammesse, ovviamente, finalità *contra legem*.

Non è vietato, in assoluto, il trattamento dei dati per finalità diverse da quelle per le quali sono stati raccolti, ma solo il loro utilizzo per finalità incompatibili con quelle originarie.

Deve essere fornita inoltre una breve descrizione delle motivazioni che supportano le affermazioni sopra effettuate.

7.2 CONDIZIONI DI LICEITÀ DEL TRATTAMENTO

Il Titolare del trattamento deve valutare la possibilità di effettuare il trattamento prima di chiedersi quali misure di sicurezza applicare. È necessario quindi si dia risposta al "perché" vengono trattati i dati personali prima di chiedersi "come" poterlo fare.

Il ***Richiedente***, supportato dal Referente Privacy, deve descrivere nel documento di DPIA le basi giuridiche su cui si fonda il trattamento. In particolare, il trattamento è lecito se è fondato su una delle seguenti basi giuridiche:

- consenso prestato dall'interessato;
- esecuzione di un'obbligazione contrattuale;
- adempimento di un obbligo legale;

- presenza di un legittimo interesse;
- salvaguardia di interessi vitali dell'interessato;
- esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Qualora non ricorra almeno una delle condizioni sopra citate, il trattamento non può essere eseguito e, di conseguenza, la procedura deve essere interrotta.

Nel caso in cui il trattamento si basi sul legittimo interesse il Richiedente, supportato dal Referente Privacy, deve fornire una breve sintesi dei criteri applicati nel bilanciamento effettuato con riferimento ai diritti fondamentali e le libertà degli interessati, così come previsto dall'art. 6, paragrafo 1, lett.f) del RGPD.

Se i dati vengono trattati sulla base del consenso degli interessati dovranno essere verificate le seguenti condizioni:

- come e quando viene ottenuto il consenso (ad es., in formato cartaceo o elettronico, da una domanda diretta o chiedendo a un individuo di spuntare una casella).
- quale prova è mantenuta dell'avvenuta prestazione del consenso (ad es., copie cartacee, log)
- come e per quanto tempo viene conservata questa prova.

il ***Referente Privacy*** verifica successivamente se il trattamento che si intende attivare/modificare, sia fondato su una delle condizioni di liceità previste dal GDPR.

7.3 MINIMIZZAZIONE DEI DATI

Il principio di minimizzazione, (così come previsto dall'art. 5 del GDPR) prevede che il trattamento dei dati sia effettuato rispettando i seguenti requisiti:

- **adeguatezza**, vale a dire che il trattamento deve essere proporzionale rispetto alle finalità per le quali i dati sono raccolti o, in altre parole, il minimo necessario per conseguire le finalità comunicate agli Interessati;
- **pertinenza** rispetto alle finalità precedentemente definite;
- **limitazione** e cioè rivolto esclusivamente al raggiungimento delle specifiche finalità per le quali i dati sono stati raccolti, riducendo al minimo il numero di dati personali che verranno elaborati e limitando tali dati a quanto strettamente necessario per gli scopi per i quali vengono elaborati (altrimenti non dovrebbero essere raccolti).

I dati raccolti devono essere adeguati e pertinenti rispetto al fine che si intende perseguire, non possono essere, quindi, raccolti in misura maggiore a quella necessaria.

Il presupposto per individuare correttamente il perimetro a cui applicare il principio di minimizzazione è dato dalla previa coerente individuazione delle finalità, che incide ovviamente anche sul principio di limitazione della conservazione.

È necessario evitare la raccolta di dati non necessari e/o l'utilizzazione di dati che non sono correlati alla finalità.

È quindi opportuno che in fase di redazione del DPIA sia opportunamente documentata la motivazione ad impiegare i dati sopra descritti al fine di giustificare il principio di impiego minimo dei dati.

7.4 LIMITAZIONE DELLA CONSERVAZIONE

I dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

8. Misure a tutela dei diritti degli interessati

Il ***Richiedente*** deve identificare e descrivere le misure (esistenti o pianificate), che consentono di rendere conforme il trattamento ai principi del GDPR. Tale attività deve essere svolta rispondendo alle seguenti domande:

1. Come sono informati del trattamento gli interessati (artt. 12, 13 and 14 del GDPR)?
2. Come fanno gli interessati ad esercitare i loro diritti (artt. Dal 15 al 21 GDPR)?
3. Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto (art. 28 del GDPR)?
4. In caso di trasferimento di dati al di fuori dell'Unione Europea, i dati godono di una protezione equivalente (art. dal 44 al 49 del GDPR.

9. Valutazione dei rischi per gli interessati

9.1 DESCRIZIONE ARCHITETTURA TECNOLOGIA/SERVIZI UTILIZZATI

Il ***Richiedente***, supportato dall'***Utente Responsabile***, deve compilare e verificare le Applicazioni IT censite all'interno del ciclo di vita del dato; queste sono intese come insieme di componenti tecnologiche, hardware, software e di rete che concorrono all'erogazione di un servizio informativo. Ogni Applicazione IT è considerata una entità logica, fondata su differenti elementi (componenti IT) tecnologici, organizzativi e di processo classificati e raggruppati in funzione della tipologia, o dai processi o dai presidi adottati.

Il ciclo di vita del dato potrebbe rivelare l'impiego di applicazioni o supporti non riconducibili ad una "Applicazione IT"; in questo caso vengono considerate direttamente le minacce contromisure che insistono su questo elemento del ciclo di vita del dato.

Il censimento delle fasi di elaborazione del ciclo di vita del dato, sopra descritto, è propedeutico e indispensabile per svolgere le fasi successive che consistono nell'identificare:

- le minacce alle quali sono sottoposte le risorse utilizzate;
- gli impatti potenziali sugli interessati nel caso in cui si realizzasse la minaccia;
- le vulnerabilità esistenti che potrebbero accentuare il rischio del realizzarsi della minaccia e causare un potenziale impatto sui diritti e le libertà degli Interessati. In questa fase vengono analizzate le misure di sicurezza e di controllo adottate, che contribuiscono in modo efficace ed efficiente a mitigarne nel continuo l'esposizione;
- il rischio residuo.

9.2 IDENTIFICAZIONE DEGLI SCENARI DI RISCHIO E DELLE FONTI DI RISCHIO

Il ***Richiedente, supportato dalle funzioni competenti,*** determina quali tra gli scenari descritti nei paragrafi successivi, si applicano al trattamento oggetto del DPIA.

Per ***Rischio*** si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità per i diritti e le libertà.

È opportuno sottolineare che il ***Rischio*** non si riferisce al titolare del trattamento ma alla persona fisica il c.d. soggetto interessato. Rispetto all'analisi dei rischi tradizionale quindi il Rischio è valutato dal "punto di vista dell'interessato e non del Titolare".

Di seguito vengono descritte le modalità con le quali vengono valutate le componenti elementari associate ai rischi individuati.

9.2.1 SCENARIO DI RISCHIO

Una volta individuate le informazioni e le risorse impiegate nel trattamento oggetto di analisi si deve procedere a mettere in evidenza le minacce che insistono su di esse.
Si definisce "Scenario di Rischio (o "categoria di rischio") un insieme omogeneo di Eventi di Rischio che possono essere assimilabili per la loro natura o per il comune esito dannoso che possono provocare.

Sono stati identificati **tre scenari di rischio**:

1. Accesso illegittimo (violazione Riservatezza);
2. Modifiche indesiderate (integrità);
3. Perdita dei dati (Indisponibilità).

Per ogni scenario di rischio devono essere individuati gli eventi di rischio (minacce) che insistono sui dati e sulle piattaforme oggetto del trattamento.

9.2.2 INDIVIDUAZIONI FONTI DI RISCHIO

Per ogni evento di rischio sono identificate le fonti di rischio le quali possono essere distinte in:

- **Fonti umane interne** (le motivazioni possono essere molteplici: confusione, errore, negligenza, vendetta, volontà di provocare allarme, malevolenza, possibilità di lucro, spionaggio):
  - un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione;
  - un utente o il suo entourage, negligente o malintenzionato, che ha accesso al servizio.

- **Fonti umane esterne**
  - una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio;

- un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo;
- un attaccante che prende di mira una delle società incaricate del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine;
- una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni. Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento.

- **Fonte non umana** (acqua, materiali pericolosi, virus informatici generici) che può essere all'origine di un rischio.

9.2.3 INDIVIDUAZIONE EVENTI DI RISCHIO (MINACCE)

Dopo avere individuato le informazioni e le risorse impiegate nel trattamento oggetto di analisi si deve procedere a mettere in evidenza gli eventi di rischio che insistono su di esse. Per effettuare tali attività dovranno essere seguite le indicazioni riportate nei paragrafi successivi.

Un Evento di Rischio (Minaccia) rappresenta un evento di natura dolosa o accidentale la cui manifestazione può determinare un impatto per i diritti e le libertà dell'individuo.

L'individuazione degli Eventi di Rischio è quell'attività che consiste nell'identificare le cause dei potenziali eventi dannosi. Tale analisi deve fornire un livello di dettaglio delle cause che permetta la selezione e l'attivazione di appropriati presidi di mitigazione del Rischio per diminuire la probabilità o la criticità dell'Evento di Rischio[2].

9.3 IDENTIFICAZIONE DEGLI IMPATTI POTENZIALI

Il ***Richiedente,*** supportato ***dall'Utente Responsabile,*** per ogni evento di rischio determina quale potrebbe essere l'impatto sui soggetti interessati nel caso in cui un evento di rischio si dovesse realizzare.

[2] I "processi IT" possono eventualmente essere considerati generalmente "trasversali" a tutte le componenti tecnologiche IT della catena nel caso implementino in modo uniforme le attività di gestione e governo su tutto il sistema informativo e quindi su tutte le risorse IT.

Nel seguito sono indicati i potenziali impatti sui diritti e le libertà degli Interessati e correlato indice di gravità.

Impatto	Descrizione esempi	Gravità
Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).	- impatti fisici: mal di testa passeggero impatti materiali: perdita di tempo dovuta a ripetizione delle procedure o all'attesa della loro effettuazione, riutilizzo dei dati a scopo di pubblicità mirata per beni di consumo corrente ecc. - impatti psicologici: semplice fastidio, impressione di violazione della privacy senza danno reale (intrusione commerciale) ecc.	**Trascurabile**
Gli individui possono andare incontro a disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).	- fisici: minore affezione fisica (es: malattia lieve a seguito del mancato rispetto di controindicazioni), diffamazione che dia luogo a rappresaglie fisiche, ecc - materiali: pagamenti non pianificati (ad esempio multe non dovute), negazione dell'accesso a servizi amministrativi o commerciali, pubblicità online mirata su un aspetto di vita privata che la persona voleva mantenere riservata ecc. - psicologici: disturbo psicologico minore ma oggettivo, senso di violazione della privacy senza danni irreparabili, intimidazione sui social network ecc.	**Limitata**
Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).	- fisici: grave affezione fisica che provochi danni a lungo termine (aggravamento dello stato di salute a seguito di una errata assunzione di responsabilità o del mancato rispetto di controindicazioni), alterazione dell'integrità fisica, ecc. - materiali: perdite monetarie non indennizzate, perdita di opportunità uniche e non ricorrenti (mutui immobiliari, studi, tirocini o occupazioni, interdizione da esami scolastici), perdita dell'abitazione, del posto di lavoro, ecc. - psicologici: grave disturbo psicologico (depressione, fobie), senso di violazione della privacy e di un danno irreparabile, esposizione a ricatti, cyberbullismo e molestie psicologiche, ecc	**Significativa**
Gli individui possono subire conseguenze significative o irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).	- fisici: affezione fisica a lungo termine o permanente, alterazione permanente dell'integrità fisica, decesso; - materiali: rischio finanziario, indebitamento ingente, impossibilità di lavorare, incapacità di ricollocazione, smarrimento di elementi di prova nell'ambito di un contenzioso, perdita di accesso a infrastrutture vitali (acqua, elettricità, ecc. - psicologici: disturbo psicologico a lungo termine o permanente, sanzione penale, allontanamento, perdita di legami familiari, perdita della capacità di agire, cambio di stato amministrativo e/o perdita dell'autonomia legale (tutela) ecc.	**Massimo**

9.4 DETERMINAZIONE DELLA VULNERABILITA' PROBABILE DEL TRATTAMENTO PER PROGETTI DI GRUPPO (SUSCETTIBILITA')

Data l'importanza del Sistema Informativo per il conseguimento dei propri obiettivi strategici, di business e di responsabilità sociale, anche in considerazione della criticità dei processi aziendali che da esso dipendono, la Società si è dotata, di un sistema di principi e regole, descritte all'interno del Regolamento di Gruppo per la gestione del Rischio Informatico, finalizzati a identificare e misurare i rischi in ambito IT a cui sono esposti gli Asset IT aziendali, a valutare i presidi esistenti e individuare le adeguate modalità di trattamento di tali rischi, prevedendo, ove necessario, opportuni interventi di mitigazione per ridurne i livelli ai limiti prestabiliti.

I criteri e le logiche utilizzate nel disegno e nell'implementazione del modello organizzativo per la gestione del Rischio Informatico del Gruppo si basano sulla coerenza con il più generale modello organizzativo del Gruppo e il rispetto dei vincoli e delle relazioni interne stabilite, nonché nell'ambito del più ampio processo di gestione del Rischio Operativo.

Al fine di determinare il livello di Rischio Privacy Residuo, la **Direzione Risk Management** determina il valore di suscettibilità, per ogni Applicazione IT, equivalente all'esposizione potenziale agli eventi di rischio e quindi alla sua Probabilità di accadimento, considerate le misure adottate per mitigare le minacce.

Il valore della Suscettibilità viene calcolato applicando la formula presente all'interno del "Regolamento di Gruppo per la gestione del Rischio Informatico" – allegato [A1] "Metodologia di Gruppo per l'analisi e la gestione del Rischio Informatico".

Il valore numerico di Suscettibilità rientra fra un minimo di 0 ed un massimo di 100 (in base 100); per la metodologia del DPIA viene ricondotto ad una scala da uno a 4:

- B = Bassa.
- MB = Medio bassa.
- MA = Media alta.
- A = Alta.

9.5 DETERMINAZIONE DELLA VULNERABILITA' PROBABILE DEL TRATTAMENTO PER PROGETTI DI INIZIATIVA DELLA BANCA

Il Richiedente della Banca, coadiuvato dalla **Funzione Sicurezza ICT**, al fine di velocizzare la produzione del DPIA, potrebbe impiegare, per ogni Applicazione IT, il livello di Suscettibilità (Vulnerabilità Probabile) già determinato dal fornitore del servizio tecnologico.

Il livello di Vulnerabilità Probabile (o Suscettibilità):

- è formulato da un fornitore ritenuto dal Titolare del Trattamento affidabile;
- è stabilito mediante una metodologia di analisi dei rischi condivisa con il Titolare del Trattamento;
- esprime un livello di probabilità considerate le misure per la mitigazione delle minacce già adottate dal fornitore.

Qualora il fornitore non sia in grado di garantire un livello di suscettibilità attendibile, il Richiedente, al fine di determinare la suscettibilità delle applicazioni utilizzate dalle fasi di elaborazione del progetto, può impiegare una Check-list contenente le misure di sicurezza minime che, a seconda del livello di rischio, deve adottare.

9.6 DETERMINAZIONE DEL RISCHIO RESIDUO

Per la determinazione dei rischi degli interessati, considerate le misure per la mitigazione delle minacce che insistono sul trattamento oggetto di DPIA, (Rischio Privacy Residuo) il ***Richiedente,*** supportato ***dall'Utente Responsabile,*** deve considerare esclusivamente il livello di impatto per gli Interessati e il livello maggiore di suscettibilità (worst case) delle Applicazioni IT impiegate all'interno del ciclo di vita del dato.

Rischio Residuo	**Impatto**	**Non applicabile**	**Trascurabile**	**limitato**	**significativo**	**massimo**
Suscettibilità		**0**	**1**	**2**	**3**	**4**
Non applicabile	**0**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**
Bassa	**1**	**N/A**	**B**	**B**	**B**	**B**
Medio Bassa	**2**	**N/A**	**B**	**B**	**MB**	**MA**
Medio Alta	**3**	**N/A**	**B**	**MB**	**MA**	**MA**
Alta	**4**	**N/A**	**B**	**MA**	**MA**	**A**

I valori di Rischio Residuo sono così di seguito distribuiti:

- B =Bassa.
- MB = Medio bassa.
- MA = Media alta.
- A = Alta.

Il Rischio Residuo è ritenuto accettabile se il livello è Basso o Medio Basso.

10. Valutazione conformità del DPIA alle norme privacy

Il ***Servizio DP / Referente Privacy*** deve esaminare le informazioni inserite all'interno del DPIA e valutare la conformità alla normativa privacy vigente.

11. Validazione del DPIA ed accountability

Al termine dell'esecuzione del DPIA, il ***Richiedente*** deve valutare l'attendibilità delle informazioni riportate all'interno del documento del DPIA, il livello di Rischio Residuo emerso dall'esecuzione del DPIA e sottoscrive, validandolo, il documento prodotto che descrive l'esecuzione della valutazione d'impatto privacy.

Terminate le operazioni di redazione del DPIA il ***Richiedente*** deve trasmettere il documento che descrive la valutazione d'impatto privacy al ***DPO*** per la richiesta del parere.

12. Approvazione del DPIA

Il ***Richiedente***, per l'approvazione / (non approvazione) del trattamento/progetto oggetto di DPIA, deve considerare le valutazioni, anche eventuali:

- della **Funzione Sicurezza ICT**;
- dei responsabili dei trattamenti eventualmente coinvolti;
- del DPO;
- le opinioni degli Interessati o dei loro rappresentanti (art. 35, paragrafo 9 del GDPR), se del caso; nel caso in cui il ***Richiedente*** decida di non consultare gli Interessati, deve indicare all'interno del DPIA i motivi a sostegno di tale decisione.

Esaminate le valutazioni delle funzioni coinvolte nel DPIA, se il Rischio Residuo per gli interessati emerso risulta "accettabile", considerate le misure di sicurezza applicate/applicabili, il ***Richiedente*** può approvare la valutazione d'impatto privacy (DPIA).

Il ***Richiedente***, se, ritiene insufficienti le misure per la mitigazione dei rischi privacy, può valutare la possibilità di chiedere l'adozione di ulteriori presidi di sicurezza.

Laddove il rischio residuo risulti "non accettabile" si dovranno applicare le istruzioni riportate nel capitolo successivo.

13. Consultazione del Garante

Il WP248 prescrive l'interpello dell'Autorità di controllo competente quando il Titolare del Trattamento non sia in grado di trovare misure tecnologiche sufficienti per ridurre il Rischio Privacy Residuo ad un livello ritenuto accettabile (livello basso o medio del rischio Privacy Residuo).

Sulla scorta dell'art. 36 GDPR, qualora il ***Richiedente***, considerato l'esito del DPIA ed il parere del DPO, intenda eseguire un trattamento che presenti un Rischio Residuo ritenuto non accettabile, deve avviare il processo per richiedere obbligatoriamente un parere al Garante: il *Richiedente* deve trasferire la decisione per l'interpello del Garante al ***Consiglio di Amministrazione*** del Titolare del Trattamento. Il ***Consiglio di Amministrazione*** potrà bocciare il progetto, suggerire altre misure per la mitigazione dei rischi oppure chiedere al DPO di inviare al Garante una richiesta di parere con tutte le indicazioni utili e necessarie affinché quest'ultimo possa effettuare le sue valutazioni.

Il ***DPO*** deve trasmettere al Garante Privacy tutte le informazioni relative a:

a) le rispettive responsabilità del Titolare del Trattamento e dei Responsabili del trattamento;

b) le finalità e i mezzi del trattamento previsto;

c) le misure e le garanzie previste per proteggere i diritti e le libertà degli Interessati;

d) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35 del GDPR, se eseguita;

e) ogni altra informazione richiesta dall'autorità di controllo.

Il ***Garante Privacy*** potrà esprimere il proprio parere in relazione alla richiesta valutando accettabili i rischi per gli interessati o potrà suggerire azioni di rimedio. Potrà in ogni caso esercitare tutti i poteri attribuitigli dal GDPR, tra cui quello di: richiedere informazioni, irrogare ingiunzioni, imporre divieti, disporre sanzioni, ordinare limitazioni del trattamento.

Il Garante deve fornire il proprio parere entro un termine di otto settimane (prorogabile di ulteriori sei per trattamenti complessi). Questi termini rimangono sospesi nelle more della fornitura di eventuali informazioni richieste dal Garante.

14. Privacy by Design / Default ed accountability

La presente Metodologia (compresi i tool impiegati per l'esecuzione) costituisce parte integrante dei controlli eseguiti per la conformità ai principi Privacy by Design/Default prevista dalla procedura Demand/Change del Titolare del Trattamento, per l'analisi di conformità al GDPR.

Ai sensi del principio di accountability previsti dal GDPR, le funzioni aziendali competenti, che per qualsiasi ragione valutano la conformità di un trattamento alla vigente Normativa Privacy, anche ai fini Privacy by Design/Default, descrivono e conservano la valutazione prodotta a seguito dell'applicazione del presente documento.

Allegato 1 - Criteri per una valutazione d'impatto sulla protezione dei dati accettabile

Il WP29 propone i seguenti criteri che i titolari del trattamento possono utilizzare per stabilire se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno oppure se una metodologia per lo svolgimento di una tale valutazione sia sufficientemente completa per garantire il rispetto del regolamento generale sulla protezione dei dati:

una descrizione sistematica del trattamento è fornita (articolo 35, paragrafo 7, lettera a)):	
la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);	☒
vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;	☒
viene fornita una descrizione funzionale del trattamento;	☒
sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);	☒
si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);	☒
la necessità e la proporzionalità sono valutate (articolo 35, paragrafo 7, lettera b)):	
sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):	☒
• **misure** che contribuiscono alla **proporzionalità e alla necessità** del trattamento sulla base di:	☒
– finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));	☒
– liceità del trattamento (articolo 6);	☒
– dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));	☒
– limitazione della conservazione (articolo 5, paragrafo 1, lettera e));	☒
• **misure che contribuiscono ai diritti degli interessati:**	
– informazioni fornite all'interessato (articoli 12, 13 e 14);	☒
– diritto di accesso e portabilità dei dati (articoli 15 e 20);	☒
– diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);	☒
– diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);	☒
– rapporti con i responsabili del trattamento (articolo 28);	☒
– garanzie riguardanti trattamenti internazionali (capo V);	☒
– consultazione preventiva (articolo 36).	☒
i rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c)):	☒

l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:	☒
si considerano le fonti di rischio (considerando 90);	☒
sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;	☒
sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;	☒
sono stimate la probabilità e la gravità (considerando 90);	☒
sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);	☒
le parti interessate sono coinvolte:	☒
si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);	☒
si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9).	☒

Allegato 2 – Tabella delle funzioni coinvolte per l'esecuzione del DPIA

Capitolo	Fase del DPIA	Funzione Deputata:	Funzione consultata:	Dati Input:	Dati Output
4	**ANALISI PRELIMINARE DEL RISCHIO**	Richiedente	Servizio DP, Referente Privacy; funzioni Competenti	Documentazione preliminare di progetto	Scheda Requisiti (SEZIONE PRIVACY)
5	**DESCRIZIONE DEL CONTESTO E CICLO DI VITA DEL DATO**	Richiedente, Utente Responsabile	Servizio DP, Referente Privacy; funzioni Competenti	i) Documentazione preliminare di progetto; ii) Scheda Requisiti (SEZIONE PRIVACY); iii) Manualistica o altra documentazione che consente di ricostruire il ciclo di vita del dato.	Compilazione capitolo dedicato al contesto e al ciclo di vita del dato
6	**NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO**	Richiedente per la compilazione Referente Privacy/ Servizio DP per la verifica e valutazione	Servizio DP, Referente Privacy; funzioni Competenti, DPO	i) Documentazione preliminare di progetto; ii) Scheda Requisiti (SEZIONE PRIVACY); iii) Manualistica o altra documentazione che consente di ricostruire il ciclo di vita del dato.	Compilazione capitolo dedicato alla necessità e proporzionalità del Trattamento
7	**MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI**	Richiedente per la compilazione Referente Privacy/ Servizio DP per la verifica e valutazione	Servizio DP, Referente Privacy, Utente Responsabile; funzioni coinvolte nel progetto, DPO	i) Documentazione preliminare di progetto; ii) Scheda Requisiti (SEZIONE PRIVACY); iii) Manualistica o altra documentazione che consente di ricostruire il ciclo di vita del dato.	Compilazione capitolo dedicato alla tutela dei diritti degli interessati
8.1	**VALUTAZIONE RISCHI PER GLI INTERESSATI: DESCRIZIONE ARCHITETTURA TECNOLOGICA**	**Richiedente e Utente Responsabile** per la compilazione	Servizio DP/Referente Privacy	Documentazione architetturale IT	Elenco e descrizione delle Applicazioni IT utilizzate nel ciclo di vita del trattamento
8.2	**VALUTAZIONE RISCHI PER GLI INTERESSATI: IDENTIFICAZIONE DEGLI SCENARI DI RISCHIO E DELLE FONTI DI RISCHIO**	Richiedente	Funzioni competenti	Catalogo degli Applicativi IT utilizzati; Descrizione ciclo di vita del dato; Slenco delle Categorie di Fattori di Rischio già utilizzate; Eventuali informazioni aggiuntive raccolte tramite interviste integrative.	Elenco delle Minacce che insistono sulle Applicazioni iT

8.3	**VALUTAZIONE RISCHI PER GLI INTERESSATI: IDENTIFICAZIONE IMPATTI PER GLI INTERESSATI**	Richiedente, Utente Responsabile	Servizio DP/Referente Privacy altri uffici coinvolti nel progetto	Dettaglio ciclo di vita del dato e informazioni sulla tipologia dei dati raccolti	Individuazione impatto potenziale
8.4	**DETERMINAZIONE DELLA VULNERABILITA' PROBABILE (SUSCETTIBILITA')**	Direzione Risk Management	Funzioni competenti	Catalogo delle misure di sicurezza potenziali; Eventuali questionari di valutazione su controlli adottati per ciascuna Componente IT che costituisce la Catena di Erogazione.	Catalogo delle misure di sicurezza potenziali; Eventuali questionari di valutazione su controlli adottati per ciascuna Componente IT che costituisce la Catena di Erogazione.
8.5	**IMPIEGO VULNERABILITA' PROBABILE (SUSCETTIBILITA') DEL FORNITORE**	Richiedente	Funzione Sicurezza ICT	Catalogo delle misure di sicurezza potenziali; Eventuali questionari di valutazione su controlli adottati per ciascuna Componente IT che costituisce la Catena di Erogazione.	Catalogo delle misure di sicurezza potenziali; Eventuali questionari di valutazione su controlli adottati per ciascuna Componente IT che costituisce la Catena di Erogazione.
8.6	**VALUTAZIONE RISCHI PER GLI INTERESSATI: VALUTAZIONE DEL RISCHIO RESIDUO**	Richiedente, Utente Responsabile	Servizio DP/Referente Privacy, Funzione Sicurezza ICT, altre Funzioni competenti	livello di suscettibilità e impatto	Determinazione del rischio residuo
9	**VALUTAZIONE CONFORMITA' del DPIA alle norme Privacy**	Referente Privacy, Servizio DP	Richiedente, altri uffici coinvolti nel progetto, altre Funzioni competenti, altre Funzioni competenti	Documento Esecuzione DPIA	Documento Esecuzione DPIA
10	**VALIDAZIONE DEL DPIA ED ACCOUNTABILITY**	Richiedente	Funzioni competenti	Documento Esecuzione DPIA	Documento Esecuzione DPIA sottoscritto
11	**APPROVAZIONE DEL DPIA**	Richiedente	Funzioni competenti	Documento Esecuzione DPIA	Documento Esecuzione DPIA approvato