sogei

METODOLOGIA PER LA PROTEZIONE DEI DATI E PER LA VALUTAZIONE D'IMPATTO

Strutture organizzative di competenza: SGD – F. Lazzini	*Responsabile della redazione:* SGD.SIP – E. Trasatti
Approvazioni: DZS – F. Amadei	*Ente emittente:* DZS – F. Amadei

INDICE

INDICE DELLE TABELLE

1. ELENCO DELLE MODIFICHE APPORTATE AL DOCUMENTO

Variazioni rispetto alla precedente versione				
Struttura proponente	**Pagina**	**Paragrafo**	**Descrizione modifiche**	**Motivazione**
DZS		5.7 5.10 5.11 6.2	Modifica delle modalità di applicazione delle misure di sicurezza eliminando il caso di "*misura non applicata*" Modifica dei criteri di valutazione di adeguatezza delle misure applicate Modifica dei criteri di accettazione di adeguatezza delle misure applicate	Definizione di valori di applicabilità delle misure di sicurezza necessari per mitigare i rischi.
DZS		5.4	**Rischio per l'organizzazione** valutato sia in termini di *probabilità* di accadimento dell'evento negativo che dell'impatto conseguente	Adeguamento ai criteri di valutazione del rischio per l'interessato

2. INTRODUZIONE

Il 25 maggio 2016 è entrato in vigore il "Regolamento 2016/679 del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati" (di seguito Regolamento) [2].

Il Regolamento ha l'obiettivo di garantire una disciplina sulla protezione dei dati personali uniforme e omogenea nell'Unione europea e ha una portata altamente innovativa rispetto alle precedenti normative in ambito privacy poiché sostituisce gli adempimenti di natura formale burocratica con attività sostanziali finalizzate a una maggiore responsabilizzazione e consapevolezza dei rischi.

Il Regolamento è definitivamente applicato in tutti i Paesi Ue dal 25 maggio 2018; in Italia il d.lgs 101/2018 [7], in vigore dal 19 settembre 2018, modifica il Codice per la protezione dei dati personali (d.lgs 196/2003) adeguandolo alla nuova normativa.

Il Regolamento introduce requisiti innovativi per la protezione dei dati personali, con ricadute organizzative, operative e tecnologiche che riguardano i principali processi di gestione del dato. Tra le principali novità vi è l'obbligo per il Titolare del trattamento di procedere a una valutazione d'impatto che, secondo quanto recita l'art. 35, deve essere compiuta dal titolare quando «un tipo di trattamento […] può presentare un rischio elevato per i diritti e le libertà delle persone fisiche».

2.1 SCOPO

Scopo del presente documento è descrivere la metodologia di protezione dei dati personali, ai sensi di quanto previsto dall'art. 25 del Regolamento, che si integra nel processo di produzione del software di Sogei. In tale contesto viene inoltre descritta la valutazione d'impatto, ai sensi di quanto previsto dall'art. 35 del Regolamento, per i trattamenti di dati personali che presentino un rischio elevato per i diritti e le libertà degli interessati. In tale metodologia sono integrati anche i criteri di valutazione dei rischi per l'organizzazione al fine di definire le misure di sicurezza complessive per le informazioni trattate.

2.2 CAMPO DI APPLICABILITÀ

La metodologia descritta in questo documento si applica allo sviluppo dei Servizi ICT erogati da Sogei per i Dipartimenti del MEF (Economia) e altri enti/amministrazioni (Altre convenzioni).

Tale metodologia può essere applicata anche a trattamenti di tipo cartaceo o basati su strumenti informatici di office automation, valutandone in modo analogo i rischi ma prendendo in considerazione misure di sicurezza specifiche per tali ambiti (Allegato 3 FLUSSO B.2 - VALUTAZIONE DI RISCHI E MISURE PER IL TRATTAMENTO).

2.3 STANDARD E NORMATIVE DI RIFERIMENTO

[1] D.Lgs. n. 196/03 Codice in materia di protezione dei dati personali;

[2] Regolamento Ue n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati che abroga la direttiva 95/46/CE (Regolamento Generale sulla protezione dei dati);

[3] Documento WP 243 – Linee guida sui responsabili della protezione dei dati (RPD) del 13 dicembre 2016;

[4] Documento WP 248 rev. 0.1 – 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 del 4 ottobre 2017;

[5] Standard ISO/IEC 29134:2017 Information technology -- Security techniques -- Guidelines for privacy impact assessment;

[6] Rettifiche del Regolamento, pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018;

[7] Decreto legislativo 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)*" approvato dal Consiglio dei Ministri n. 14 dell'8 agosto 2018.

2.4 DOCUMENTAZIONE CORRELATA

[8] Task Support System, pubblicato sulla intranet aziendale;

[9] IS-00-PR-05 - FOURSec - Misure per la protezione dei dati di trattamenti e Servizi ICT;

[10] IS-18-PR-01 - Misure di sicurezza e privacy del Servizio ICT.

2.5 ACRONIMI E GLOSSARIO

- **Autorità di controllo** o **Autorità Garante**: l'autorità pubblica indipendente istituita da uno Stato UE ai sensi dell'articolo 51 del GDPR;
- **Applicazione:** Collezione integrata di procedure automatizzate e dati che forniscono supporto ad un obiettivo applicativo; è formata da uno o più componenti, moduli, o sottosistemi;
- **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» (GDPR, art. 4 punto 1);
- **Danno**: conseguenza di un evento che compromette la protezione delle persone fisiche con riguardo al trattamento dei loro dati personali;
- **DPO** (*Data Protection Officer*) o **Responsabile della Protezione dei dati personali (RPD)**: il soggetto nominato dal Titolare o dal Responsabile del trattamento in presenza di trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala oppure nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati;
- **FOURSec** (*Framework to Organize Under Rules Security*): framework multicompliance costituito da 260 misure di sicurezza che sintetizzano circa 600 singoli requisiti derivati da normative, standard, istruzioni contrattuali e politiche interne [9];
- **GDPR**: *General Data Protection Regulation* o Regolamento europeo n.679/2016, di seguito anche **Regolamento** [2]
- **Impatto:** insieme delle conseguenze in termini di danni o perdite che il verificarsi di un evento ha sul pieno raggiungimento dell'obiettivo della protezione delle persone fisiche con riguardo al trattamento dei loro dati personali;
- **Interessato**: la persona fisica cui si riferiscono i dati personali;
- **Minaccia**: causa potenziale di un rischio di compromissione della protezione delle persone fisiche con riguardo al trattamento dei loro dati personali;
- **Misure di sicurezza**: insieme degli accorgimenti tecnici e organizzativi volti a ridurre al minimo il rischio che i dati vadano distrutti o persi anche in modo accidentale, che le persone non autorizzate possano avere accesso ai dati e che siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati sono stati raccolti;

- **Owner del trattamento**: la persona di riferimento per un determinato trattamento. Risponde al Titolare del trattamento;
- **Privacy by default**: il principio secondo il quale il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
- **Privacy by design**: il principio secondo il quale il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati fin dalla progettazione del trattamento per tutelare i diritti degli interessati;
- **Privacy Impact Assessment** (**PIA**) o **Valutazione d'impatto**: l'azione che il Titolare del trattamento deve effettuare prima di procedere a un trattamento di dati personali per tutelare gli interessati in caso di rischio elevato per i loro diritti e le loro libertà;
- **Probabilità**: possibilità del concretizzarsi di un evento;
- **Registro dei trattamenti**: il documento che contiene tutte le informazioni base del trattamento che deve essere redatto, secondo le rispettive responsabilità e competenze, sia dal Titolare sia dal Responsabile del trattamento ed esibito su richiesta all'Autorità di controllo;
- **Responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il Servizio ICT o altro organismo che tratta dati personali per conto del Titolare del trattamento (di seguito anche **Responsabile**);
- **Responsabile del Servizio ICT**: è il riferimento per tutto ciò che riguarda il Servizio ICT e risponde al Titolare o al Responsabile del trattamento ove designato;
- **Rischio intrinseco**: incertezza sul raggiungimento dell'obiettivo della protezione dei dati, che si verifica come combinazione dell'impatto di un evento e della probabilità del suo verificarsi;
- **Rischio residuo**: rischio intrinseco valutato dopo il suo trattamento, ovvero dopo l'applicazione delle misure di sicurezza;
- **Scenario di rischio**: descrizione generale e/o specifica di un insieme di minacce;
- **Servizio ICT**: insieme di applicazioni informatiche omogenee (identificate da uno o più kit di applicazione) e della relativa infrastruttura tecnologica, in grado di supportare lo svolgimento di un processo/sottoprocesso amministrativo – e, nei casi previsti dalla normativa (GDPR) connesso al "Trattamento" dei dati e per le quali sia comunque opportuno esercitare il controllo/monitoraggio (prestazioni, costi, consumi, ecc.) a livello di unica entità;

- **Titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il Servizio ICT o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali (di seguito anche **Titolare**);
- **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, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione» (GDPR, art. 4);
- **Valutazione del rischio**: il processo di identificazione, stima del livello di rischio, valutazione e trattamento del rischio. In ambito GDPR il processo di analisi del rischio si svolge tenuto conto della natura dei dati, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche (GDPR, art. 24.1).

3. SINTESI DELL'APPROCCIO METODOLOGICO

Il processo di valutazione dei rischi supporta il Titolare e il Responsabile del trattamento a mettere in atto misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, conformemente ai principi sulla protezione dei dati dettati dal Regolamento [2].

La presente metodologia a supporto del processo integra la valutazione dei rischi per i diritti e le libertà dell'interessato ai sensi di quanto previsto dall'art 25 del Regolamento [2] (*privacy by design*) e dall'art. 35 (*Privacy Impact Assessment* - PIA) con la valutazione dei rischi relativi alla sicurezza delle informazioni secondo lo standard ISO/IEC 27001:2013.

La metodologia descritta nel documento è stata sviluppata sulla base delle prescrizioni contenute nel Regolamento ([2]), delle linee guida del documento WP 248 [4] e tenendo conto dell'approccio descritto nello standard ISO/IEC 29134 [4].

La presente metodologia sarà fatta oggetto di revisione periodica almeno annuale, e comunque nei casi in cui se ne ravvisi la necessità in relazione a novità normative o interpretative.

Il documento è focalizzato sulla metodologia di valutazione dei rischi collegati ad asset di tipo informatico (Servizi ICT) a supporto del trattamento e, conseguentemente, è integrata nel processo di sviluppo del software. Può però essere generalizzata a trattamenti di archivi cartacei o supportati da strumenti informatici di office automation prevedendo idonee misure di sicurezza.

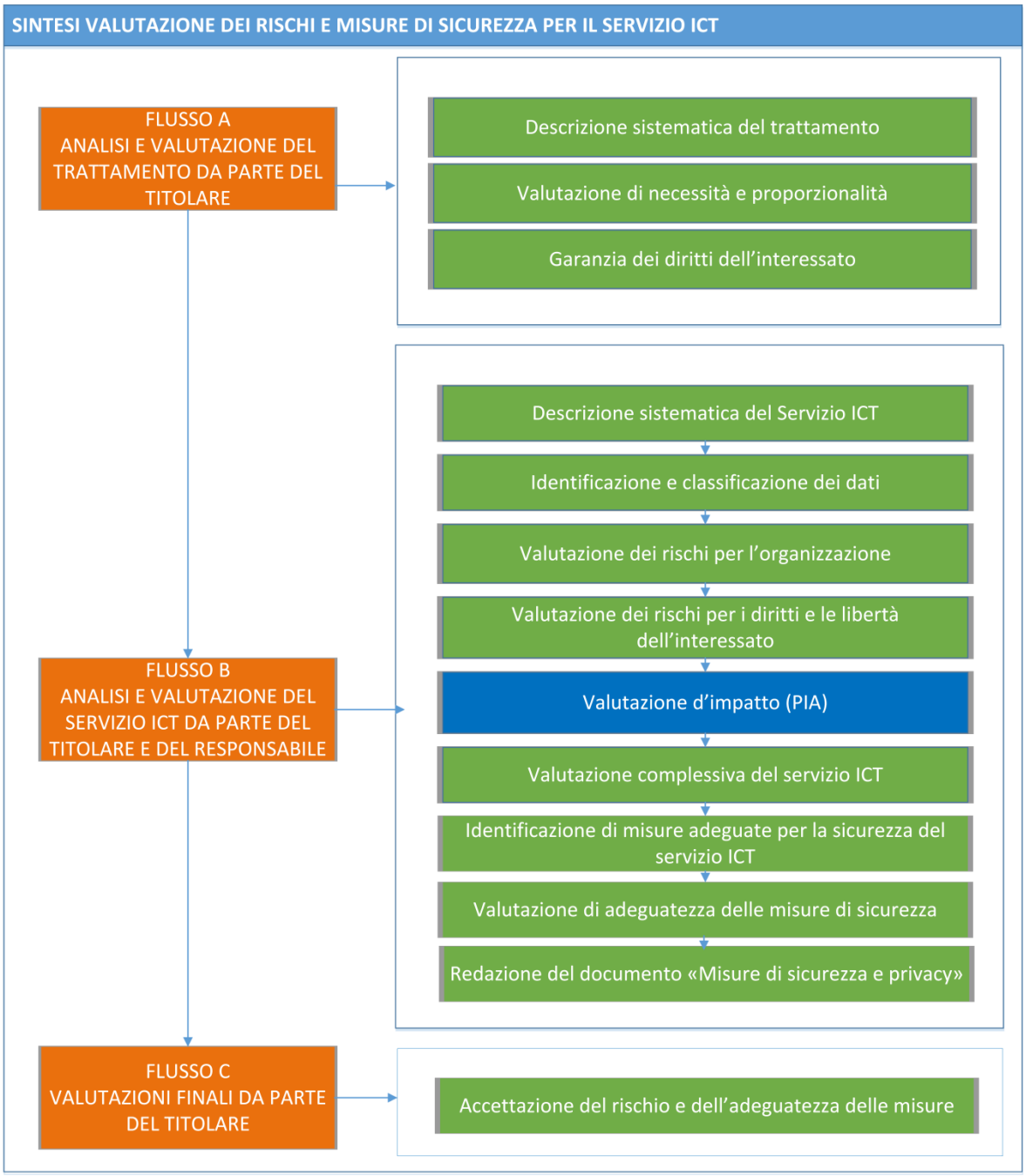
Di seguito il flusso di sintesi[1] per la valutazione dei rischi e delle misure di sicurezza per il Servizio ICT, suddiviso in tre parti:

FLUSSO A. Analisi e valutazione del trattamento da parte del Titolare

FLUSSO B. Analisi e valutazione del Servizio ICT da parte del Titolare e del Responsabile, ove designato

FLUSSO C. Valutazioni finali del Titolare.

[1] Nel flusso sono rappresentate, in colore diverso, le attività che riguardano la privacy by design e la sicurezza delle informazioni (colore verde) e quelle che riguardano la valutazione di impatto (colore blu).



RUOLI E RESPONSABILITA'

Il ruolo di Titolare è assunto dall'Amministrazione per cui Sogei opera come Responsabile esterno in forza di un rapporto contrattuale o da Sogei stessa nel caso di trattamenti di propria competenza.

L'Owner del trattamento e il Responsabile del Servizio ICT operano rispettivamente per conto del Titolare e del Responsabile del trattamento, ove sia designato, ad esempio quando il Servizio ICT è erogato da Sogei per conto dell' Amministrazione.

Il DPO del Titolare fornisce, se richiesto, un parere relativamente alla valutazione di impatto (PIA) in corso e vigila sul suo svolgimento.

FLUSSO A

La prima parte del processo comprende le attività che riguardano la progettazione del trattamento, in particolare:

- descrizione sistematica del trattamento (par. 4.2);
- valutazione di necessità e proporzionalità del trattamento (par. 4.3);
- garanzie per i diritti degli interessati (par. 4.4).

Tali attività sono svolte dall'Owner del trattamento per conto del Titolare fin dalla progettazione iniziale del trattamento per consentirne una valutazione complessiva e dimostrarne la conformità al Regolamento [2] implementando gli strumenti necessari per consentire agli interessati di esercitare i loro diritti.

FLUSSO B

La seconda parte del processo comprende le attività che riguardano la progettazione del Servizio ICT a supporto del trattamento:

- descrizione sistematica del Servizio ICT (par. 5.2);
- identificazione e la classificazione dei dati (par. 5.3);
- valutazione dei rischi per l'organizzazione (par.5.4);
- valutazione dei rischi per i diritti e le libertà dell'interessato (par.5.5);
- valutazione d'impatto (PIA)
  - valutazione delle categorie di trattamento ad elevato rischio (par.5.6)
  - identificazione di misure adeguate per valutazione di impatto (par. 5.7)
  - consultazione del DPO (par. 5.8)
- valutazione complessiva dei rischi del Servizio ICT (par. 5.9)
- identificazione di misure adeguate per la sicurezza del Servizio ICT (par. 5.10)
- valutazione di adeguatezza delle misure di sicurezza (par. 5.11)
- redazione del documento "Misure di sicurezza e privacy del Servizio ICT" (par. 5.12).

Tali attività sono svolte dall'Owner del trattamento e dal Responsabile del Servizio ICT fin dalla fase di analisi dei requisiti del Servizio ICT e consistono nell'individuazione di misure di sicurezza adeguate ai rischi valutati rispetto alle caratteristiche del Servizio ICT e alla tipologia dei dati trattati.

La valutazione d'impatto (PIA) è obbligatoria a condizione che il trattamento di dati personali presenti un rischio potenzialmente elevato per i diritti e le libertà degli interessati. Ne consegue che occorre individuare i criteri per valutare la presenza di un rischio potenzialmente elevato relativo a eventi illeciti di accesso, diffusione, modifica, indisponibilità o perdita dei dati personali.

Il Gruppo di lavoro Articolo 29 per la protezione dei dati - organo consultivo della Commissione Ue su questa materia - ha emesso le linee guida WP248 [4] in tema di PIA e in esse vengono proposte 9 categorie di trattamento che individuano un potenziale rischio elevato. Il criterio utilizzato nella metodologia qui presentata valuta la presenza di un rischio potenzialmente elevato se il Servizio ICT rientra in almeno due delle categorie definite ad alto rischio dalle linee guida WP248.

Nel caso di rischio elevato per l'interessato si procede dunque con lo svolgimento di PIA individuando misure di sicurezza adeguate ai rischi.

Riguardo alla valutazione complessiva dei rischi del Servizio ICT, il calcolo viene effettuato combinando i rischi dell'organizzazione inerenti alla perdita di riservatezza, integrità e disponibilità delle informazioni e i rischi per gli interessati. Le misure di protezione adeguate al rischio complessivo del Servizio ICT sono state individuate nell'ambito del framework multicompliance FOURSec (*Framework to Organize Under Rules Security*) [9].

Una volta valutato il rischio complessivo del Servizio ICT, il Responsabile del Servizio ICT identifica le misure di sicurezza tecnicamente applicabili; l'Owner del trattamento con il Responsabile del Servizio ICT specifica se le misure di sicurezza sono da applicare nell'intervento in corso o successivamente in appositi piani di rientro.

Il Responsabile del Servizio ICT compila infine il documento "Misure di Sicurezza e Privacy del Servizio ICT" [10] per documentare le valutazioni dei rischi e della adeguatezza delle misure di sicurezza.

FLUSSO C

La terza parte del processo comprende le attività che riguardano le valutazioni finali dell'Owner del trattamento (par. 6.2) il quale può:

- approvare il documento "Misure di Sicurezza e Privacy del Servizio ICT" confermando l'adeguatezza delle misure in relazione ai rischi e autorizzare il Responsabile del Servizio ICT a procedere all'implementazione;
- non approvare il documento "Misure di Sicurezza e Privacy del Servizio ICT" e procedere alla ridefinizione degli elementi del servizio, misure di sicurezza e requisiti applicativi, eventualmente ricorrendo ad un riesame interno, coinvolgendo superiori livelli di responsabilità nell'organizzazione e, se del caso, il proprio DPO.

Oggetto di valutazione e approvazione sono in particolare i seguenti elementi:

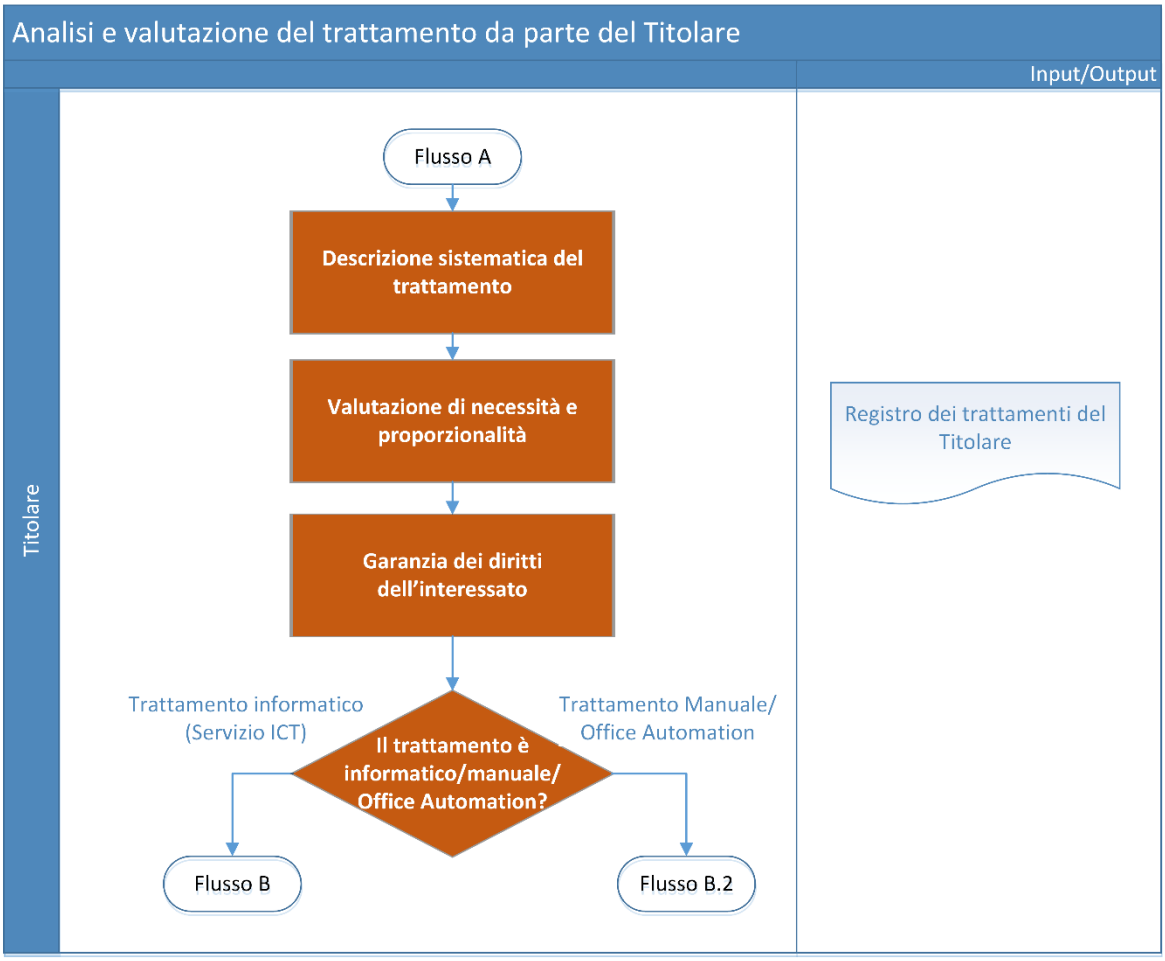
- rischi per i diritti e le libertà degli interessati - compresa la valutazione d'impatto, ove necessaria - relativi al trattamento di dati personali;
- rischi per l'organizzazione del Titolare, relativi alla sicurezza delle informazioni elaborate;
- adeguatezza delle misure di sicurezza da applicare per mitigare i rischi.

Nel caso in cui, a seguito di un'eventuale valutazione d'impatto, l'Owner del trattamento ritenga che le misure per mitigare il rischio per gli interessati non siano adeguate è necessario consultare, tramite il DPO, l'Autorità di controllo (par. 6.3), prima dell'inizio delle attività di sviluppo del Servizio ICT.

4. FLUSSO A - ANALISI E VALUTAZIONE DEL TRATTAMENTO DA PARTE DEL TITOLARE

4.1 FLUSSO E CARTA DELLE RESPONSABILITÀ

Di seguito è riportato il flusso di analisi e valutazione del trattamento di dati personali.



Le informazioni raccolte nelle diverse fasi del flusso confluiscono nel Registro dei trattamenti del Titolare.

La tabella riportata di seguito elenca le attività di analisi e valutazione di un trattamento e, per ognuna, le responsabilità secondo la matrice RACI[2] .

Nome Attività	Ruoli / Responsabilità		
	Resp. Servizio ICT	**Owner trattamento**	**DPO (Titolare/ Responsabile)**
Descrizione sistematica del trattamento	**C**	**R**	**I**
Valutazione di necessità e proporzionalità	**I**	**R**	**I**
Garanzia dei diritti dell'interessato	**I**	**R**	**I**

Tabella 1 - Flusso A: Matrice RACI

4.2 DESCRIZIONE SISTEMATICA DEL TRATTAMENTO

L'Owner del trattamento descrive le caratteristiche del trattamento, come indicato in Tabella 2, seguendo lo schema di supporto alla compilazione riportato in Tabella 3.

DATI IDENTIFICATIVI DEL TRATTAMENTO	
Processo	*Processo all'interno del quale viene realizzato il trattamento*

[2] La matrice è organizzata secondo il modello RACI che prevede quattro ruoli:
R = **Responsible**. Esegue l'attività e ne è responsabile. Per la stessa attività è ammessa una responsabilità condivisa, ossia è possibile la presenza di più "R".
A = **Accountable**. Coordina, supervisiona e approva i vari task che compongono l'attività; può eseguirne alcuni ed è responsabile anche degli aspetti economici. È unico per l'attività e deve essere individuato nel caso vi sia la presenza di più "R".
C = **Consulted.** È consultato poiché possiede informazioni e/o capacità necessarie per portare a termine l'attività.
I = **Informed**. È informato dei risultati dell'attività.

Trattamento	*Identificativo, nome, descrizione funzionale, informazioni sulla struttura referente del trattamento*
Titolare	*Soggetto che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*
Responsabile	*Informazioni sul Responsabile del trattamento (es. nome, indirizzo, contatti, etc.)*
Contitolare	*Informazioni (es. nome, indirizzo, contatti, etc.) sul soggetto che, unitamente al Titolare, determina le finalità e i mezzi del trattamento*
Strumenti	*Strumenti utilizzati per il trattamento anche in base al tipo di trattamento (es. servizi informatici, servizi informatici non software, servizi software, servizi infrastrutturali)*
IDENTIFICAZIONE E CLASSIFICAZIONE DEI DATI	
Dati	*Categorie di dati personali*
Termini di cancellazione	*Tempi o criteri di cancellazione dei dati*
CARATTERISTICHE GENERALI DEL TRATTAMENTO	
Tipologia	*Tipologia del trattamento (es. informatico, cartaceo o eseguito su postazioni di lavoro tramite strumenti di office automation)*
Finalità	*Scopo perseguito con il trattamento*
Fondamenti di liceità	*Base giuridica e contrattuale che legittima il trattamento dei dati*
Interessati	*Categorie di persone fisiche cui si riferiscono i dati*
Destinatari	*Categorie destinatari di comunicazioni e relativa descrizione*
Trasferimenti dati	*Trasferimento dati extra Ue e relative garanzie*

Tabella 2 - Informazioni descrittive del trattamento

VALORIZZAZIONE CATEGORIE	
Dati	*Dati personali comuni* *anagrafici* *contabili e fiscali, inerenti possidenze e riscossione* *inerenti il rapporto di lavoro* *tracciamenti* *dati inerenti situazioni giudiziarie civili, amministrative, tributarie*
	Dati personali specifici *geolocalizzazione* *audio/video/foto* *dati di profilazione*

VALORIZZAZIONE CATEGORIE	
	Dati personali finanziari *dati relativi all'esistenza di rapporti finanziari (coordinate bancarie, consistenze saldi, movimenti, giacenza media, etc.)*
	Dati personali sensibili *convinzioni religiose o filosofiche/opinioni politiche/origine razziale/adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale*
	Dati personali ipersensibili *stato di salute, assistenza sanitaria, orientamento/vita sessuale* *genetici*
	Dati personali giudiziari *casellario giudiziale* *qualità di indagato/imputato o altre situazioni giudiziarie (condanne penali e reati o connesse misure di sicurezza)*
	Dati personali biometrici *impronte digitali* *altre caratteristiche biometriche* *firma grafometrica*
Tipologia	*Supportato da Servizi ICT*
	Supportato da strumenti di office automation
	Supportato da archivi cartacei
Finalità	*Gestione amministrativo contabile*
	Informazione/formazione, istruzione, cultura
	Ricerca e statistica
	Settore economico
	Settore sanitario
	Settore fiscale, tributario
	Gestione della sicurezza fisica (es. sedi, locali,…)
	Applicazione contratti di lavoro
Fondamenti di liceità	*Consenso dell'interessato*
	Esecuzione di un contratto con l'interessato
	Obbligo legale per il titolare
	Salvaguardia interessi vitali dell'interessato o altra persona fisica
	Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale
	Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da regolamento UE
	Altri fondamenti connessi al trattamento di categorie particolari di dati personali - art. 9 par. 2
	Richiesta pubblica autorità
	Statuto
Interessati	*Cittadini*
	Personale dipendente e familiari

VALORIZZAZIONE CATEGORIE	
	Contraenti, offerenti e candidati
	Rappresentanti e dipendenti di enti/istituzioni (associazioni di categoria/ordini professionali, ecc.)
	Componenti organi dell'Ente
	Persone fisiche extra UE
	Visitatori
	Minorenni
	Operatori economici
	Professionisti, intermediari
	Altri soggetti - Persone fisiche
Destinatari	*Persona fisica*
	Persona giuridica
	Pubblica amministrazione
	Autorità pubblica
Trasferimenti dati	*Paese terzo o organizzazione internazionale*
	Garanzie e autorizzazioni ex art. 46 del Regolamento

Tabella 3 - Schema di supporto alla compilazione delle categorie

L'uso di codici di condotta (art. 35, par. 8 del Regolamento) non è referenziabile allo stato dell'arte, in quanto non risultano approvati, al momento, schemi o codici applicabili allo specifico contesto in cui opera Sogei (i.e. rapporti con la PA).

4.3 VALUTAZIONE DI NECESSITÀ E PROPORZIONALITÀ

L'Owner del trattamento esegue una valutazione formale di necessità, pertinenza e proporzionalità dei dati rispetto alle finalità del trattamento e descrive:

- perché i dati raccolti sono necessari, rispetto alle finalità del trattamento e ai fondamenti di liceità;
- perché i dati raccolti non sono eccedenti rispetto alle finalità e quindi, secondo il principio di minimizzazione, si raccolgono e trattano, per impostazione predefinita del trattamento (ovverosia *by default*) solo i dati minimi indispensabili per le finalità specifiche;
- in che modo che i dati trattati sono adeguati al raggiungimento degli obiettivi del trattamento;
- in quale modo i dati sono corretti e aggiornati;
- perché i dati sono limitati alla sola realizzazione delle finalità, nel rispetto dei tempi e dei criteri di cancellazione.

4.4 GARANZIA DEI DIRITTI DELL'INTERESSATO

L'Owner del trattamento dimostra di aver definito e di garantire i diritti degli interessati, in relazione allo specifico trattamento, al fine di fornire i mezzi per esercitarli agevolmente, specificando anche le motivazioni che eventualmente ne impediscono l'attuazione. Di seguito è elencato l'insieme di tali diritti e alcuni esempi a titolo di chiarimento:

- informazioni fornite agli interessati, ad esempio l'interessato è posto a conoscenza almeno dell'identità del titolare e delle finalità del trattamento cui sono destinati i dati (*informativa*), al fine di manifestare l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento (*consenso*);
- diritto di accesso e portabilità dei dati, ad esempio l'interessato ha il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso di ottenere l'accesso a tali dati. Inoltre l'interessato ha il diritto di ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico e, se possibile in funzione delle specificità del trattamento, di trasmettere tali dati a un altro Titolare;
- diritto di rettifica e cancellazione, ad esempio l'interessato ha il diritto di ottenere la correzione e l'integrazione dei dati personali inesatti o incompleti che lo riguardano senza ingiustificato ritardo. In casi particolari e in base alle caratteristiche specifiche del trattamento, ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano;
- diritto di opposizione e limitazione del trattamento, in casi particolari e in base alle caratteristiche specifiche del trattamento, l'interessato ha il diritto di opporsi al trattamento per motivi connessi alla sua situazione particolare e, di conseguenza, il Titolare si astiene, anche temporaneamente, dal trattare ulteriormente i dati, salvo dimostrare l'esistenza di motivi legittimi cogenti che prevalgono sui diritti e sulle libertà dell'interessato oppure per l'accertamento l'esercizio o la difesa di un diritto in sede giudiziaria;
- rapporti con i Responsabili del trattamento, ad esempio se il Titolare del trattamento designa i Responsabili, è necessario che questi presentino garanzie sufficienti per mettere in atto misure adeguate a garantire la tutela dei diritti dell'interessato;
- garanzie per i trasferimenti internazionali dei dati, ad esempio l'interessato ha diritto alla protezione dei dati personali che lo riguardano e ad appropriate garanzie, anche nel caso in cui i dati fossero trasferiti verso un Paese terzo o un'organizzazione internazionale;
- consultazione preventiva dell'Autorità di controllo (par. 6.3), ad esempio se dalla valutazione d'impatto sulla protezione dei dati risulta un rischio elevato per i diritti e le libertà delle persone fisiche, si consulta l'Autorità di controllo prima dell'inizio delle attività di trattamento. L'Autorità di controllo fornisce un

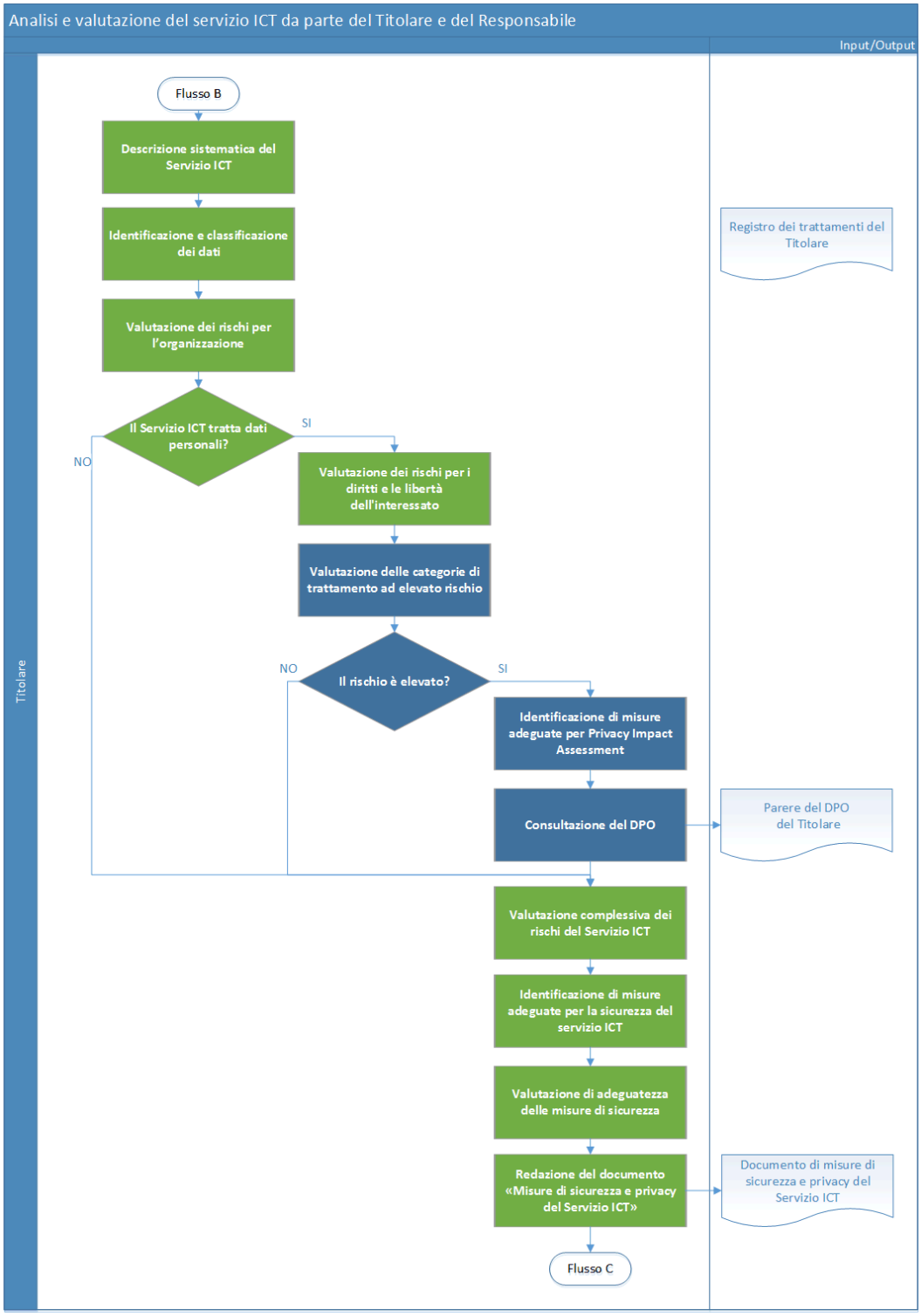
parere in merito al fine di garantire che il trattamento rispetti in ogni caso il Regolamento e può avvalersi dei propri poteri, tra cui rivolgere ammonimenti o ammonizioni, imporre limitazioni o divieti. L'Autorità di controllo, inoltre, viene notificata di eventuali violazioni di dati personali (*data breach*) e può ingiungere al Titolare di comunicare all'interessato la violazione stessa.

5. FLUSSO B - ANALISI E VALUTAZIONE DEL SERVIZIO ICT DA PARTE DEL TITOLARE E DEL RESPONSABILE

5.1 FLUSSO E CARTA DELLE RESPONSABILITÀ

Di seguito è riportato il flusso di valutazione[3], relativamente al Servizio ICT, dei rischi per i diritti e le libertà degli interessati, compresa la valutazione d'impatto (PIA), e dei rischi relativi alla sicurezza delle informazioni.

[3] Nel flusso sono rappresentate, in colore diverso, le attività che riguardano la privacy by design e la sicurezza delle informazioni (colore verde) e quelle che riguardano la valutazione di impatto (colore blu).



La tabella seguente elenca le attività e le responsabilità secondo la matrice RACI.[4]

Nome Attività	Ruoli / Responsabilità		
	Responsabile Servizio ICT	**Owner trattamento**	**DPO Titolare/ Responsabile**
Descrizione sistematica del Servizio ICT	**C**	**A**	**I**
Identificazione e classificazione dei dati	**C**	**A**	**I**
Valutazione dei rischi per l'organizzazione	**C**	**A**	**-**
Valutazione dei rischi per i diritti e le libertà degli interessati	**C**	**A**	**I**
Valutazione delle categorie di trattamento ad elevato rischio	**C**	**A**	**I**
Identificazione di misure adeguate per privacy impact assessment	**R**	**A**	**I**
Consultazione del DPO	**I**	**A**	**C**
Valutazione complessiva dei rischi del Servizio ICT	**C**	**A**	**I**
Identificazione di misure adeguate per la sicurezza del Servizio ICT	**R**	**A**	**I**
Valutazione di adeguatezza delle misure di sicurezza	**R**	**A**	**I**
Redazione del documento "Misure di sicurezza e privacy del Servizio ICT…"	**R**	**A**	**I**

Tabella 4 – Flusso B: Matrice RACI

[4] La matrice è organizzata secondo il modello RACI che prevede quattro ruoli:
R = **Responsible**. Esegue l'attività e ne è responsabile. Per la stessa attività è ammessa una responsabilità condivisa, ossia è possibile la presenza di più "R".
A = **Accountable**. Coordina, supervisiona e approva i vari task che compongono l'attività; può eseguirne alcuni ed è responsabile anche degli aspetti economici. È unico per l'attività e deve essere individuato nel caso vi sia la presenza di più "R".
C = **Consulted.** È consultato poiché possiede informazioni e/o capacità necessarie per portare a termine l'attività.
I = **Informed**. È informato dei risultati dell'attività.

Parte delle informazioni prodotte dalle attività del flusso confluiscono nei Registri dei trattamenti del Titolare e del Responsabile.

5.2 DESCRIZIONE SISTEMATICA DEL SERVIZIO ICT

Partendo dal trattamento del Titolare, l'Owner del trattamento, con il supporto del Responsabile del Servizio ICT, descrive le caratteristiche del Servizio ICT come indicato in Tabella 5, seguendo lo schema di supporto alla compilazione riportato in Tabella 6.

DATI IDENTIFICATIVI DEL SERVIZIO ICT	
Codice	*Codice del Servizio ICT*
Nome	*Nome del Servizio ICT*
Descrizione	*Descrizione funzionale del Servizio ICT*
Titolare	*Titolare del trattamento supportato dal Servizio ICT*
Interscambio dati	*Indica se il Servizio ICT permette lo scambio di dati personali tra pubbliche amministrazioni secondo il provvedimento del Garante del 2 luglio 2015*
Cloud	*Indica se vengono utilizzati servizi cloud esterni*
Numero di utenti	*Numero degli utenti del Servizio ICT*
Tipologia di utenti	*Tipologia degli utenti del Servizio ICT (cittadini, dipendenti, ecc)*
INFORMAZIONI SUL TRATTAMENTO (da riportare solo se il Servizio ICT tratta dati personali)	
Finalità	*Scopo perseguito con il trattamento*
Fondamenti di liceità	*Base giuridica e contrattuale che legittima il trattamento dei dati*
Interessati	*Categorie di persone fisiche cui si riferiscono i dati*
Destinatari	*Categorie dei destinatari di comunicazioni*
Termini di cancellazione dei tracciamenti	*Tempi o criteri di cancellazione dei tracciamenti (log)*
Trasferimenti dati	*Trasferimento dati extra Ue e relative garanzie*

Processi privacy implementati	*Procedure implementate sul Servizio ICT per garantire i diritti dell'interessato in merito ai propri dati personali (consenso, informativa, rettifica, cancellazione, …)*

Tabella 5 – Informazioni descrittive del Servizio ICT

VALORIZZAZIONE CATEGORIE	
Interscambio dati	*Interoperabilità (il Servizio ICT permette lo scambio di dati personali e viene invocato dalle amministrazioni appartenenti al SIF)*
	Cooperazione applicativa (il Servizio ICT permette lo scambio di dati personali e viene invocato da amministrazioni esterne al SIF)
	Generico (il Servizio ICT non permette lo scambio di dati personali tra pubbliche amministrazioni)
Cloud	*SI/NO*
Tipologia di utenti	*Dipendenti Sogei*
	Collaboratori Sogei (tecnici, consulenti, …)
	Dipendenti dell'amministrazione titolare per servizi di front-office
	Dipendenti dell'amministrazione titolare per servizi di Direzione Centrale
	Dipendenti dell'amministrazione titolare per servizi di back-office
	Dipendenti altre PA
	Cittadini
	Associazioni di categoria
	Professionisti
	Operatori economici
	Intermediari
	Punti di commercializzazione
	Concessionari
	Fornitori
	Collaboratori dei clienti istituzionali
	Altro (specificare)
Finalità	*Gestione amministrativo contabile*
	Informazione/formazione, istruzione, cultura
	Ricerca e statistica
	Settore economico
	Settore sanitario
	Settore fiscale, tributario

VALORIZZAZIONE CATEGORIE	
	Gestione della sicurezza fisica (es. sedi, locali,…)
	Applicazione contratti di lavoro
Fondamenti di liceità	*Consenso dell'interessato*
	Esecuzione di un contratto con l'interessato
	Obbligo legale per il titolare
	Salvaguardia interessi vitali dell'interessato o altra persona fisica
	Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale
	Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da regolamento UE
	Altri fondamenti connessi al trattamento di categorie particolari di dati personali - art. 9 par. 2
	Richiesta pubblica autorità
	Statuto
Interessati	*Cittadini*
	Personale dipendente e familiari
	Contraenti, offerenti e candidati
	Rappresentanti e dipendenti di enti/istituzioni (associazioni di categoria/ordini professionali, …)
	Componenti organi dell'Ente
	Persone fisiche extra UE
	Visitatori
	Minorenni
	Operatori economici
	Professionisti, intermediari
	Altri soggetti - Persone fisiche
Destinatari	*Persona fisica*
	Persona giuridica
	Pubblica amministrazione
	Autorità pubblica
Trasferimenti dati	*Paese terzo o organizzazione internazionale*
	Garanzie e autorizzazioni ex art. 46 del Regolamento
Termine di cancellazione dei tracciamenti	*Breve (1 anno)*
	Medio (2 anni)
	Lungo (30 anni)
	Indeterminato
	Informativa

VALORIZZAZIONE CATEGORIE	
Processi privacy implementati[5]	*Consenso*
	Data breach
	Diritto di accesso ai dati
	Diritto di opposizione/cancellazione
	Diritto di rettifica
	Diritto alla limitazione dei dati

Tabella 6 – Schema di supporto alla compilazione delle categorie

5.3 IDENTIFICAZIONE E CLASSIFICAZIONE DEI DATI

Partendo dal trattamento/processo del titolare, l'Owner del trattamento, con il supporto del Responsabile del Servizio ICT, identifica:

- i dati appartenenti al dominio in esame e ne fornisce una descrizione;
- i tempi di cancellazione dei dati, ossia il periodo massimo consentito per il trattamento. Ove possibile indica il periodo esatto oltre il quale i dati devono essere cancellati oppure descrive il criterio utilizzato per la cancellazione.

Se il Servizio ICT tratta dati personali, questi devono essere classificati secondo quanto riportato in Tabella 7.

[5] Per una descrizione delle categorie di processi privacy implementabili a garanzia dei diritti dell'interessato riferirsi al par. 4.4 Garanzia dei diritti dell'interessato.

Macro categoria di dati personali	Categoria di dati personali
Dati personali comuni	anagrafici contabili e fiscali, inerenti possidenze e riscossione inerenti il rapporto di lavoro tracciamenti dati inerenti situazioni giudiziarie civili, amministrative, tributarie
Dati personali specifici	geolocalizzazione audio/video/foto dati di profilazione
Dati personali finanziari	dati relativi all'esistenza di rapporti finanziari (coordinate bancarie, consistenze saldi, movimenti, giacenza media, etc.)
Dati personali sensibili	convinzioni religiose o filosofiche/opinioni politiche/origine razziale/adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
Dati personali ipersensibili	stato di salute, assistenza sanitaria, orientamento/vita sessuale genetici
Dati personali giudiziari	casellario giudiziale qualità di indagato/imputato o altre situazioni giudiziarie (condanne penali e reati o connesse misure di sicurezza)
Dati personali biometrici	impronte digitali altre caratteristiche biometriche firma grafometrica

Tabella 7 – Classificazione privacy del dato

5.4 VALUTAZIONE DEI RISCHI PER L'ORGANIZZAZIONE

L'Owner del trattamento, con il supporto del Responsabile del Servizio ICT, valuta i rischi per l'organizzazione in termini di perdita degli attributi di riservatezza, integrità e disponibilità delle informazioni gestite.

In particolare il rischio per l'organizzazione viene valutato in termini di:

- *Impatto per l'organizzazione,* stimato sulla base del livello di gravità (trascurabile, basso, medio o alto) delle seguenti tipologie di danni:
  - perdita finanziaria;

- compromissione (rallentamento, blocco) delle attività di business;
- perdita di immagine;
- sanzioni amministrative e/o penali previste da normativa.

L'impatto è valutato come il valore massimo delle gravità dei danni indicate per ogni attributo R, I (Tabella 17 – Legenda per la valutazione del rischio di perdita di Riservatezza e Integrità) e D (Tabella 19 - Legenda per la valutazione del rischio di perdita di Disponibilità).

– *Probabilità per l'organizzazione,* (trascurabile, bassa, media o alta), stimata sulla base degli agenti interni, esterni e errori/eventi accidentali, (Tabella 22 – Legenda per la valutazione probabilità di accadimento).

Il valore del rischio intrinseco è espresso per ciascuna minaccia come combinazione dell'impatto e della probabilità di accadimento dell'evento negativo, secondo la stessa matrice utilizzata per la valorizzazione del rischio per l'interessato, (cfr. Tabella 8).

5.5 VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DELL'INTERESSATO

Per ogni Servizio ICT a supporto di un trattamento di dati personali, l'Owner del trattamento, con il supporto del Responsabile del Servizio ICT, effettua la valutazione dei rischi per l'interessato calcolando la probabilità di accadimento delle minacce applicabili e la gravità del danno, al fine di individuare le misure di sicurezza adeguate ad attenuare tale rischio.

La valutazione dei rischi sui diritti e sulle libertà dell'interessato consta delle seguenti attività:

- identificazione delle minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilità dei dati;
- individuazione degli scenari di rischio specifici relativi alle categorie di dati personali;
- valutazione dei potenziali rischi sui diritti e le libertà degli interessati. Il rischio è inteso come uno scenario descrittivo di un evento dannoso e delle relative conseguenze, stimate in termini di gravità e probabilità di accadimento.

Le minacce applicabili sono:

– accesso non autorizzato e/o trattamento illegittimo relativo a dati;

– divulgazione non autorizzata o accidentale di dati;

– modifica non autorizzata o accidentale di dati;

- perdita, distruzione accidentale o illegale di dati;
- indisponibilità temporanea o prolungata di dati.

Gli scenari di rischio specifici si ottengono applicando ogni minaccia alle differenti categorie di dati (Tabella 20 – Minacce e scenari di rischio).

Per ciascuno scenario specifico l'Owner del trattamento, con il supporto del Responsabile del Servizio ICT, valuta il livello di rischio intrinseco, espresso come combinazione dell'impatto e della sua probabilità di accadimento.

L'impatto rappresenta le conseguenze derivanti da un evento negativo. Più sono elevate le conseguenze più alto è percepito il rischio. La valutazione dell'impatto tiene conto delle seguenti tipologie di danni (Tabella 21):

- danno fisico-biologico;
- danno finanziario;
- danno reputazionale;
- danno di identità.

La valorizzazione dell'impatto segue una scala predefinita (trascurabile, basso, medio, alto), e deriva dal valore massimo di danno rispetto alle tipologie indicate.

La probabilità di accadimento segue una scala predefinita (trascurabile, basso, medio, alto) e indica quanto è probabile che si verifichi un evento negativo. Dipende dal contesto interno ed esterno del Servizio ICT e viene stimata utilizzando la Tabella 22 – Legenda per la valutazione probabilità di accadimento.

La valutazione del rischio intrinseco deve essere eseguita per ogni scenario specifico applicabile. La Tabella 23 - Stima del rischio intrinseco per i diritti e le libertà dell'interessato, rappresenta un esempio di valutazione precompilata.

Il valore del rischio intrinseco è espresso per ciascun scenario applicabile come combinazione dell'impatto e della probabilità di accadimento dell'evento negativo utilizzando la seguente Tabella 8.

Rischio intrinseco		**Probabilità di accadimento**			
		Trascurabile	***Basso***	***Medio***	***Alto***
Impatto	***Trascurabile***	Trascurabile	Trascurabile	Trascurabile	Trascurabile
	Basso	Basso	Basso	Basso	Basso
	Medio	Basso	Basso	Medio	Alto
	Alto	Basso	Medio	Alto	Alto

Tabella 8 - Matrice per la valorizzazione dei rischi per l'interessato

In caso di un nuovo Servizio ICT o di modifiche significative a un Servizio ICT esistente dovranno necessariamente essere rivalutati tutti gli scenari, apportando i dovuti aggiornamenti.

5.6 VALUTAZIONE DELLE CATEGORIE DI TRATTAMENTO A ELEVATO RISCHIO

La valutazione d'impatto (PIA) è obbligatoria qualora il trattamento presenti un rischio elevato per i diritti e le libertà dell'interessato.

Il Comitato europeo per la protezione dei dati, attraverso il documento WP 248 [4], al fine di fornire un insieme più concreto di trattamenti che richiedono una valutazione d'impatto sulla protezione dei dati in virtù del loro rischio intrinseco, suggerisce di prendere in esame le seguenti nove categorie (Tabella 24):

1. Valutazione o assegnazione di un punteggio (incluse le attività di profilazione e le analisi di tipo predittivo) riferita ad un individuo;
2. Decisioni automatizzate con significativi effetti giuridici o di analoga natura;
3. Monitoraggio sistematico di individui (es. mediante videosorveglianza);
4. Elaborazione di dati sensibili o aventi caratteristiche strettamente personali (es. giudiziari o altri tipi di dati strettamente personali il cui trattamento possa comportare alti rischi per l'interessato come la geolocalizzazione). Si assume che il Servizio ICT appartenga a questa categoria se dalla valutazione dei rischi per i diritti e le libertà degli interessati (par.5.5) emerge un rischio intrinseco alto relativamente agli scenari di rischio specifici applicabili
5. Elaborazione di dati su larga scala (es. per numero di individui coinvolti, volumi complessivi, durata o persistenza, ambito geografico);
6. Combinazione o raffronto tra banche dati provenienti da due o più operazioni di trattamento effettuati per scopi diversi;
7. Elaborazione di dati relativi a soggetti vulnerabili per cui è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento (es. minori, anziani, dipendenti);
8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
9. Impedimento all'interessato di esercitare un diritto o di avvalersi di un Servizio ICT o di un contratto.

Se il Servizio ICT rientra in almeno due tra le suddette categorie o se a giudizio dell'Owner del trattamento anche una sola categoria nel contesto di riferimento costituisce un elevato rischio per l'interessato, è necessario procedere con lo svolgimento della valutazione di impatto (PIA) identificando le misure di sicurezza

adeguate (par.5.7) prima di passare alle fasi di valutazione complessiva dei rischi e individuazione delle relative misure (par. 5.9 e 5.10).

5.7 IDENTIFICAZIONE DI MISURE ADEGUATE PER VALUTAZIONE DI IMPATTO (PIA)

Nel caso in cui il Servizio ICT rientri in almeno due categorie di trattamento ad elevato rischio per l'interessato (par. 5.6) o, se a giudizio dell'Owner, comprenda anche una sola categoria è necessario procedere con l'identificazione di misure di sicurezza PIA adeguate al livello di rischio in relazione alle singole minacce.

Tali misure sono selezionate dal framework multicompliance di Sogei, FOURSec (*Framework to Organize Under Rules Security*) [9] che associa specifiche misure di sicurezza da applicare in caso di valutazione d'impatto corrispondenti ad un elevato livello di rischio per l'interessato.

Il Responsabile del Servizio ICT indica in base ai vincoli architetturali l'insieme delle misure applicabili al contesto con la modalità di implementazione.

L'Owner del trattamento con il supporto del Responsabile del Servizio ICT valuta, tenendo conto della natura dei dati trattati, dei costi/tempi di attuazione come anche dei livelli di rischio, le misure da applicare nell'intervento in corso o successivamente in appositi piani di rientro, utilizzando la guida contenuta nella seguente Tabella 9.

Applicabilità misura	**Modalità di implementazione**
Già applicata nell'intervento (rif. Obiettivo)	*Descrivere le modalità di implementazione della misura di sicurezza*
Da applicare nell'intervento (rif. Obiettivo)	*Descrivere le modalità di implementazione della misura di sicurezza*
Da applicare successivamente - urgente	*Descrivere le azioni di miglioramento, ove possibile*
Da applicare successivamente – non urgente	*Descrivere le azioni di miglioramento, ove possibile*

Non applicabile (la misura non è tecnicamente applicabile o pertinente nel contesto di riferimento)	*Specificare le motivazioni per cui la misura non è tecnicamente applicabile o pertinente al contesto di riferimento*

Tabella 9 – Applicazione misure PIA

Nel caso in cui il Servizio ICT sia composto da Applicazioni non omogenee relativamente ai dati trattati è necessario indicare l'applicabilità delle misure di sicurezza specifiche per ognuna di tali Applicazioni.

5.8 CONSULTAZIONE DEL DPO

Tutte le misure di sicurezza ritenute tecnicamente applicabili per mitigare i rischi per l'interessato devono essere applicate.

Qualora l'Owner del trattamento ravvisi la sussistenza di rischi significativi per l'interessato, in caso di parziale adozione delle misure nell'intervento in corso, procede alla consultazione del proprio DPO.

5.9 VALUTAZIONE COMPLESSIVA DEI RISCHI DEL SERVIZIO ICT

L'Owner del trattamento, con il supporto del Responsabile del Servizio ICT, valuta i livelli complessivi di rischio intrinseco per le minacce applicabili al Servizio ICT. Tale calcolo è effettuato, come da seguente Tabella 10, sulla base di:

- rischi per i diritti e le libertà degli interessati (par.5.5);
- rischi per l'organizzazione derivanti dalla perdita di riservatezza, integrità e disponibilità delle informazioni (par.5.4).

Minaccia	Rischio intrinseco per interessato	Rischio intrinseco per organizzazione	Rischio intrinseco per Servizio ICT
Accesso non autorizzato e/o trattamento illecito relativo a dati	Valutazione dei rischi per l'interessato	Max (rischio Riservatezza, Integrità)	Max (Rischio interessato, organizz)
Divulgazione non autorizzata o accidentale di dati	Valutazione dei rischi per l'interessato	Rischio Riservatezza	Max (Rischio interessato, organizz)
Modifica non autorizzata o accidentale di dati	Valutazione dei rischi per l'interessato	Rischio Integrità	Max (Rischio interessato,organizz)

Perdita, distruzione accidentale o illegale di dati	Valutazione dei rischi per l'interessato	Rischio Disponibilità a lungo termine	Max (Rischio interessato,organizz)
Indisponibilità temporanea o prolungata di dati	Valutazione dei rischi per l'interessato	Max (Rischio Disponibilità a breve e medio termine)	Max (Rischio interessato,organizz)

Tabella 10 - Rischio intrinseco del Servizio ICT

Il rischio intrinseco complessivo del Servizio ICT è dato dal valore massimo tra il rischio intrinseco per l'interessato e il rischio intrinseco per l'organizzazione.

5.10 IDENTIFICAZIONE DI MISURE ADEGUATE PER LA SICUREZZA DEL SERVIZIO ICT

In base al livello di rischio intrinseco complessivo del Servizio ICT (par. 5.9), risultante dalla valutazione del rischio intrinseco per l'interessato e per l'organizzazione, viene estratto dal framework FOURSec [9] un elenco di misure di sicurezza in relazione ad ogni minaccia.

Il Responsabile del Servizio ICT indica in base ai vincoli architetturali l'insieme delle misure applicabili al contesto con la modalità di implementazione.

L'Owner del trattamento con il supporto del Responsabile del Servizio ICT valuta, tenendo conto della natura dei dati trattati, dei costi/tempi di attuazione come anche dei livelli di rischio, le misure da applicare nell'intervento in corso o successivamente in appositi piani di rientro, utilizzando la guida contenuta nella seguente Tabella 11.

Applicabilità misura	**Modalità di implementazione**
Già applicata nell'intervento (rif. Obiettivo)	*Descrivere le modalità di implementazione della misura di sicurezza*
Da applicare nell'intervento (rif. Obiettivo)	*Descrivere le modalità di implementazione della misura di sicurezza*
Da applicare successivamente - urgente	*Descrivere le azioni di miglioramento, ove possibile*
Da applicare successivamente – non urgente	*Descrivere le azioni di miglioramento, ove possibile*

Non applicabile (la misura non è tecnicamente applicabile o pertinente nel contesto di riferimento)	*Specificare le motivazioni per cui la misura non è tecnicamente applicabile o pertinente al contesto di riferimento*

Tabella 11 – Applicazione misure per la sicurezza del Servizio ICT

Nel caso in cui il Servizio ICT sia composto da Applicazioni non omogenee relativamente ai dati trattati, è necessario indicare l'applicabilità delle misure specifiche per ognuna di tali Applicazioni.

5.11 VALUTAZIONE DI ADEGUATEZZA DELLE MISURE DI SICUREZZA

Per ricondurre i rischi intrinseci per l'interessato e per l'organizzazione a valori trascurabili, tutte le misure di sicurezza applicabili in relazione al contesto ed ai vincoli architetturali devono essere adottate.

L'adeguatezza delle misure in relazione ai rischi è valutata in funzione delle misure da applicare nell'intervento in corso o successivamente con le relative priorità di attuazione, in particolare è espressa secondo la seguente terminologia:

- accettabile, se tutte le misure applicabili sono già applicate o sono da applicare nell'intervento in corso;
- accettabile con riserva, se per alcune misure applicabili sono previsti piani di rientro urgenti;
- da verificare, se per alcune misure applicabili sono previsti piani di rientro non urgenti.

In caso di parziale adozione delle misure di sicurezza nell'intervento in corso, il Responsabile del Servizio ICT rende evidenti all'Owner del trattamento le criticità che ne possono derivare. Tali evidenze costituiscono i razionali che supportano l'Owner del trattamento nella valutazione di adeguatezza delle misure di sicurezza per mitigare i rischi.

5.12 REDAZIONE DEL DOCUMENTO "MISURE DI SICUREZZA E PRIVACY DEL SERVIZIO ICT"

Il Responsabile del Servizio ICT compila il documento "Misure di sicurezza e privacy del Servizio ICT" [10] per documentare le valutazioni, concordate con

l'Owner del trattamento, relative ai rischi e all'adeguatezza delle misure di sicurezza.

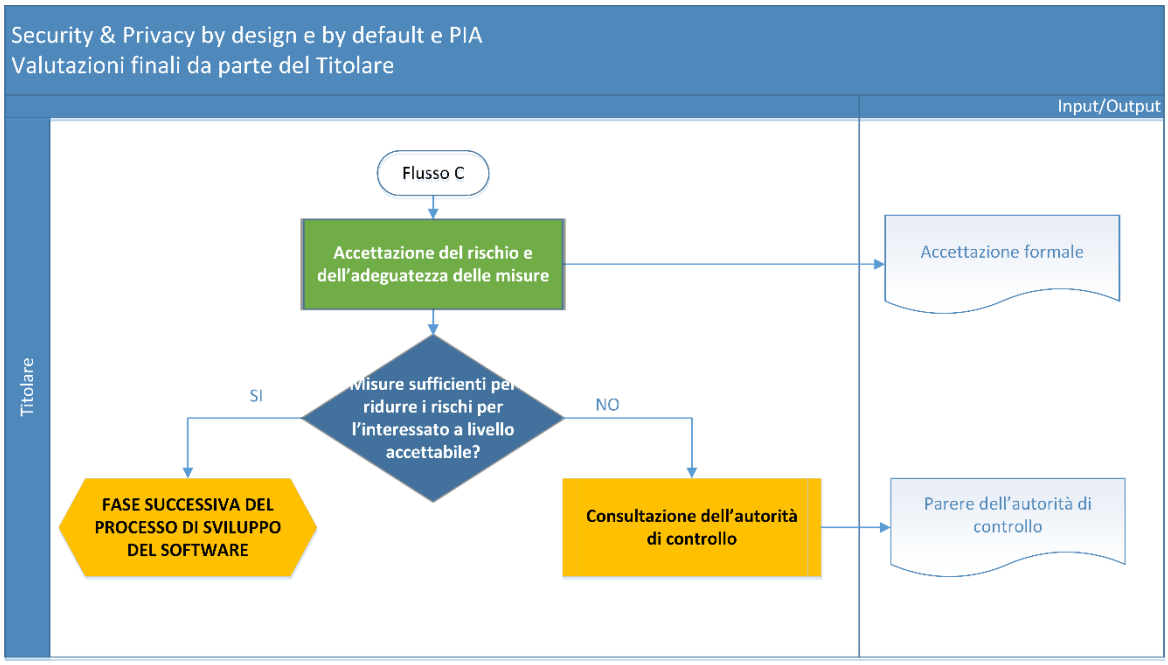
Il Responsabile del Servizio ICT invia il documento contestualmente al documento "Analisi dei Requisiti"/"Specifica di intervento" se previsto o, in caso contrario, in un momento utile a garantire comunque uno sviluppo coerente del Servizio ICT.

È richiesta l'approvazione da parte dell'Owner del trattamento del documento "Misure di sicurezza e privacy del Servizio ICT" che avverrà contestualmente all'approvazione del documento "Analisi dei Requisiti"/"Specifica di intervento", se previsto o, in caso contrario in modo specifico.

6. FLUSSO C - VALUTAZIONI FINALI DA PARTE DEL TITOLARE

6.1 FLUSSO E CARTA DELLE RESPONSABILITÀ

Di seguito è riportato il flusso[6] relativo alle valutazioni finali da parte del Titolare.



La tabella riportata di seguito elenca le attività di analisi e valutazione di un trattamento e, per ognuna, le responsabilità secondo la matrice RACI.[7] .

[6] Nel flusso sono rappresentate, in colore diverso, le attività che riguardano la privacy by design (colore verde) e quelle che riguardano la valutazione di impatto (colore blu).
[7] La matrice è organizzata secondo il modello RACI che prevede quattro ruoli:
R = **Responsible**. Esegue l'attività e ne è responsabile. Per la stessa attività è ammessa una responsabilità condivisa, ossia è possibile la presenza di più "R".
A = **Accountable**. Coordina, supervisiona e approva i vari task che compongono l'attività; può eseguirne alcuni ed è responsabile anche degli aspetti economici. È unico per l'attività e deve essere individuato nel caso vi sia la presenza di più "R".
C = **Consulted.** È consultato poiché possiede le capacità necessarie per portare a termine l'attività.
I = **Informed**. È informato dei risultati dell'attività.

Nome attività	Ruoli / Responsabilità		
	Responsabile Servizio ICT	**Owner trattamento**	**DPO Titolare**
Accettazione del rischio e dell'adeguatezza delle misure	**I**	**R**	**I**
Consultazione dell'Autorità di controllo	**I**	**R**	**C**

Tabella 12 - Flusso C: Matrice RACI

6.2 ACCETTAZIONE DEL RISCHIO E DELL'ADEGUATEZZA DELLE MISURE

L'Owner del trattamento sulla base delle informazioni raccolte può:

- approvare il documento "Misure di sicurezza e privacy del Servizio ICT", confermando l'adeguatezza delle misure di sicurezza per mitigare i rischi e autorizzare il Responsabile del Servizio ICT a procedere alla progettazione e allo sviluppo dell'applicazione;
- non approvare il documento "Misure di sicurezza e privacy del Servizio ICT", richiedendo l'applicazione di ulteriori misure di sicurezza nell'intervento in corso e autorizzare il Responsabile del Servizio ICT a procedere previa implementazione di tali misure; in tal caso il Responsabile del Servizio ICT aggiorna il documento "Misure di sicurezza e privacy", segnalando eventuali problematiche realizzative di natura tecnica, nonché eventuali costi connessi all'implementazione delle misure richieste, procedendo successivamente alla progettazione e sviluppo;
- non approvare il documento "Misure di sicurezza e privacy del Servizio ICT" e richiedere l'applicazione di minori misure di sicurezza nell'intervento in corso spostando le restanti misure applicabili in piani di rientro successivi; in tal caso il Responsabile del Servizio ICT segnala formalmente all'Owner del trattamento tutte le criticità conseguenti.

In particolare:

- nei casi in cui l'analisi contenuta nel documento "Misure di sicurezza e privacy del Servizio ICT" si concluda con una valutazione dell'adeguatezza delle misure "accettabile" in quanto è prevista l'implementazione di tutte le misure di sicurezza applicabili, l'Owner del trattamento, se valuta che siano stati

correttamente riportati e mitigati i rischi per l'organizzazione e per l'interessato, può procedere all'approvazione del documento;

- invece, nei casi in cui l'analisi contenuta nel documento "Misure di sicurezza e privacy del Servizio ICT" si concluda con una valutazione dell'adeguatezza delle misure da applicare nell'intervento in corso "accettabile con riserva" o "da verificare" e l'Owner del trattamento ravvisi la sussistenza di rischi significativi per il servizio ICT da avviare a fronte della pianificazione a breve o lungo termine delle restanti misure applicabili, l'Owner può valutare se procedere ad un riesame interno, coinvolgendo superiori livelli di responsabilità nell'organizzazione del Titolare, fino ad un eventuale coinvolgimento del proprio DPO. A seguito dell'esito di tali ulteriori valutazioni e consultazioni l'Owner del trattamento può:
  - approvare il documento "Misure di sicurezza e privacy del Servizio ICT", confermando l'adeguatezza delle misure da applicare nell''intervento in corso e le misure da applicare successivamente in appositi piani di rientro con relativo livello di urgenza;
  - non approvare il documento e ridefinire, in considerazione di tempi e costi, alcuni elementi del servizio, misure di sicurezza o requisiti applicativi, al fine di individuarne ed eliminarne i punti critici. A seguito di tale revisione si dovrà procedere alla rivalutazione dell'adeguatezza delle misure di sicurezza, aggiornando la documentazione di supporto e il documento "Misure di sicurezza e privacy ICT". Qualora, a seguito della valutazione d'impatto, l'Owner del trattamento sia del parere che rimangano elevati rischi per l'interessato, consulta preventivamente l'Autorità di controllo tramite il DPO (par. 6.3) e, se del caso, raccoglie le opinioni degli interessati o dei loro rappresentanti (art. 35, comma 9 del Regolamento).

L'Owner del trattamento può procedere analogamente anche per l'approvazione conclusiva del documento "Misure di sicurezza e privacy del trattamento" inerente a un trattamento cartaceo o supportato da strumenti di office automation, valutando la necessità di ricorrere a un riesame interno e/o a un riesame del trattamento, come sopra descritto (Allegato 3 - FLUSSO B.2 - VALUTAZIONE DI RISCHI E MISURE PER IL TRATTAMENTO DA PARTE DEL TITOLARE).

6.3 CONSULTAZIONE DELL'AUTORITÀ DI CONTROLLO

Se dalla valutazione d'impatto sulla protezione dei dati risulta che il trattamento presenta un rischio elevato per i diritti e le libertà delle persone fisiche e l'Owner del trattamento è del parere che il rischio non possa essere ragionevolmente attenuato, si consulta l'Autorità di controllo prima dell'inizio delle attività di trattamento (art. 36 del Regolamento).

L'Autorità di controllo fornisce un parere scritto e può avvalersi dei poteri stabiliti dal Regolamento, al fine di garantire il rispetto della normativa (es. può fornire consulenza notificando eventuali violazioni, rivolgere avvertimenti e ammonizioni, ingiungere di conformare i trattamenti alle disposizioni del Regolamento, imporre limitazioni o divieti al trattamento, ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali).

ALLEGATI

1. CONFORMITÀ DELLA METODOLOGIA A NORME E STANDARD

La metodologia di PIA descritta nel presente documento è stata sviluppata sulla base delle prescrizioni contenute nel Regolamento [2], delle linee guida del documento WP 248 [4] e tenendo conto dell'approccio descritto nello standard ISO/IEC 29134 [4]. Nei paragrafi seguenti si elencano i criteri di accettabilità per la PIA estratti dalle linee guida e dallo standard ISO e se ne raffrontano i contenuti rispetto alla presente metodologia.

1.1 CONFORMITÀ ALLE LINEE GUIDA WP 248 REV.01

Il Gruppo di lavoro Articolo 29 propone, all'interno del documento di linee guida WP248 ([4], Allegato 2), una serie di criteri che possono essere utilizzati per stabilire se una metodologia specifica per l'esecuzione di una valutazione di impatto comprenda gli elementi sufficienti a garantire il rispetto delle disposizioni del Regolamento.

La Tabella 13 elenca i criteri presenti nell'Allegato 2 del WP248 e, per ognuno, ne riporta la descrizione e il paragrafo del presente documento in cui sono referenziati, tenendo in considerazione che le attività di PIA sono completamente integrate all'interno del processo di produzione del software.

Criterio WP 248	Descrizione criterio WP 248	Paragrafo di riferimento
Descrizione sistematica del trattamento (art. 35, par. 7, lettera a)	• *si tiene conto della natura, dell'ambito, del contesto e delle finalità del trattamento (considerando 90);* • *sono indicati i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi;* • *si dà una descrizione funzionale del trattamento;* • *si specificano gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);* • *si tiene conto dell'osservanza di codici di condotta approvati (art. 35, par. 8)*	Par. 4.2 Descrizione sistematica del trattamento

Criterio WP 248	Descrizione criterio WP 248	Paragrafo di riferimento
valutazione di necessità e proporzionalità del trattamento (art. 35, par. 7, lettera b)	• *si definiscono le misure previste per rispettare il regolamento (art. 35, par. 7, lettera d) e considerando 90) tenendo conto di quanto segue:* ▪ *misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:* – *finalità specifiche, esplicite e legittime (art. 5(1), lettera b));* – *liceità del trattamento (art. 6);* – *dati adeguati, pertinenti e limitati a quanto necessario (art. 5(1)c));* – *periodo limitato di conservazione (art. 5(1), lettera e));*	Par. 4.3 Valutazione di necessità e proporzionalità Cap. 3 Flusso B.2 - Valutazione di rischi e misure per il trattamento da parte del titolare
	▪ *misure che contribuiscono ai diritti degli interessati:* – *informazioni fornite agli interessati (artt. 12, 13, 14);* – *diritto di accesso e portabilità dei dati (artt. 15 e 20);* – *diritto di rettifica e cancellazione (artt. 16, 17, 19);* – *diritto di opposizione e limitazione del trattamento (artt. 18,19, 21);* – *rapporti con responsabili del trattamento (art. 28);* – *garanzie per i trasferimenti internazionali di dati (Capo V);*	Par. 4.3 Valutazione di necessità e proporzionalità Cap. 3 Flusso B.2 - Valutazione di rischi e misure per il trattamento da parte del titolare
	– *consultazione preventiva (art. 36)*	Par. 6.3 Consultazione dell'Autorità di controllo

Criterio WP 248	Descrizione criterio WP 248	Paragrafo di riferimento
gestione dei rischi per i diritti e le libertà degli interessati (art. 35, par. 7, lettera c)	• *Si determinano l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati:* ▪ *si tiene conto delle fonti di rischio (considerando 90);* ▪ *si identificano gli impatti potenziali sui diritti e le libertà degli interessati in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilità dei dati;* ▪ *si identificano le minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilità dei dati;* ▪ *si stimano probabilità e gravità (considerando 90);*	Par 5.5 Valutazione dei rischi per i diritti e le libertà dell'interessato Par 5.6 Valutazione delle categorie di trattamento ad elevato rischio
	• *si stabiliscono le misure previste per gestire i rischi di cui sopra (art. 35, par. 7, lettera d) e considerando 90);*	Par 5.7 Identificazione di misure adeguate per valutazione di impatto (PIA) Par 5.10 Identificazione di misure adeguate per la sicurezza del Servizio ICT Par 5.11 Valutazione di adeguatezza delle misure di sicurezza
coinvolgimento dei soggetti interessati	• *si chiede consulenza al RPD/DPO (art. 35, par. 2);*	Par 5.8 Consultazione del DPO (ruolo e responsabilità del DPO)
	• *si sentono gli interessati o i loro rappresentanti (art. 35, par. 9), se del caso.*	Par. 6.2 Accettazione del rischio e dell'adeguatezza delle misure

Tabella 13 - Criteri di accettabilità per la PIA secondo WP 248

Rispetto ai criteri riportati nel WP 248, si precisa e si osserva quanto segue:

- l'art. 35, par. 8 del Regolamento relativo all'uso di codici di condotta non è referenziabile allo stato dell'arte, in quanto non risultano approvati, al momento, schemi o codici applicabili allo specifico contesto in cui opera Sogei (i.e. rapporti con la PA);
- se un trattamento è necessario per adempiere ad un obbligo di legge o per l'esecuzione di un compito di interesse pubblico ed è già stata condotta una valutazione di impatto per lo specifico trattamento, non è necessario per il titolare rieseguire nuovamente la PIA (art. 35, par. 10 del Regolamento);
- al momento non sono noti schemi di PIA applicabili al settore in cui opera Sogei; in ogni caso il Regolamento non indica una procedura specifica da seguire ai fini della PIA, lasciando ai titolari la definizione dello schema;
- la descrizione delle misure che "*contribuiscono alla proporzionalità e alla necessità del trattamento"* (artt. 5 e 35, par. 7, lett. b), del Regolamento) è principalmente di tipo concettuale;
- l'opportunità per il titolare di "*raccogliere le opinioni degli interessati o dei loro rappresentanti se del caso"* (art. 35, par. 9 del Regolamento) è contemplata come ipotesi, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti; il titolare dovrebbe comunque documentare le motivazioni della mancata consultazione, qualora decidesse di non attuarla.

1.2 CONFORMITÀ ALLO STANDARD ISO/IEC 29134:2017

Lo standard ISO/IEC 29134, basato sulla ISO/IEC 31000 (che rappresenta lo standard di riferimento per la gestione del rischio), definisce il processo per la valutazione d'impatto e il riesame periodico, fornendo un esempio per la stima degli impatti e uno specifico modello da utilizzare per il rapporto di valutazione.

L'approccio proposto dallo standard declina la valutazione d'impatto in diverse fasi operative, che vanno dalla preparazione della PIA al follow-up, ciascuna delle quali articolata in attività specifiche. La Tabella 14 elenca le fasi e, per ognuna, ne riporta le attività e il paragrafo del presente documento in cui sono referenziate, tenendo in considerazione che le attività di PIA sono completamente integrate all'interno del processo di produzione del software.

ISO/IEC 29134:2017 Fase	ISO/IEC 29134:2017 Attività	Paragrafo di riferimento
Fase 1 Preparazione della PIA	Necessità Team Pianificazione Stakeholder	Par 4.1 Flusso e Carta delle responsabilità Par 5.3 Identificazione e classificazione dei dati

ISO/IEC 29134:2017 Fase	ISO/IEC 29134:2017 Attività	Paragrafo di riferimento
Fase 2 Esecuzione della PIA	Flussi informativi	Par 5.1 Flusso e Carta delle responsabilità
	Casi d'uso	Par 5.5 Valutazione dei rischi per i diritti e le libertà dell'interessato Par 5.6 Valutazione delle categorie di trattamento ad elevato rischio
	Contromisure esistenti	5.7 Identificazione di misure adeguate per valutazione di impatto (PIA)
	Valutazione del rischio	Par 5.5 Valutazione dei rischi per i diritti e le libertà dell'interessato Par 5.6 Valutazione delle categorie di trattamento ad elevato rischio
	Trattamento del rischio	5.11 Valutazione di adeguatezza delle misure di sicurezza (valutazione di adeguatezza delle misure di sicurezza specifiche di PIA)
Fase 3 Follow up	Report	IS-18-PR-01 - Misure di sicurezza e privacy del Servizio ICT.
	Implementazione del piano	Fase di progettazione e realizzazione del Servizio ICT
	Audit	Fase di progettazione e realizzazione del Servizio ICT
	Gestione dei cambiamenti alla PIA	IS-18-PR-01 - Misure di sicurezza e privacy del Servizio ICT.

Tabella 14 – Analisi dei requisiti dello standard ISO/IEC 29134

2. FOURSEC

FOURSec (*Framework to Organize Under Rules Security*) [9] è un framework di misure di sicurezza volto alla protezione delle informazioni e dell'infrastruttura tecnologica di Sogei. Ogni misura è il risultato di una integrazione e omogeneizzazione di requisiti di sicurezza derivanti da normative nazionali ed europee (GDPR, provvedimenti del Garante), standard (ISO/IEC 27001:2013), framework di riferimento per la cybersecurity (Framework nazionale per la cybersecurity, NIST Cybersecurity Framework), istruzioni contrattuali delle Amministrazioni e politiche aziendali di sicurezza e privacy.

Ai fini della metodologia per la protezione dei dati e per la valutazione d'impatto viene utilizzato un estratto delle circa 260 misure di sicurezza in esso contenute, applicabile ai trattamenti di dati personali effettuati con l'ausilio di Servizi ICT o con il supporto di strumenti di office automation o di documenti cartacei. La selezione delle misure adeguate per ogni trattamento/ Servizio ICT viene effettuata sulla base della minaccia e del livello di rischio ad esse associato.

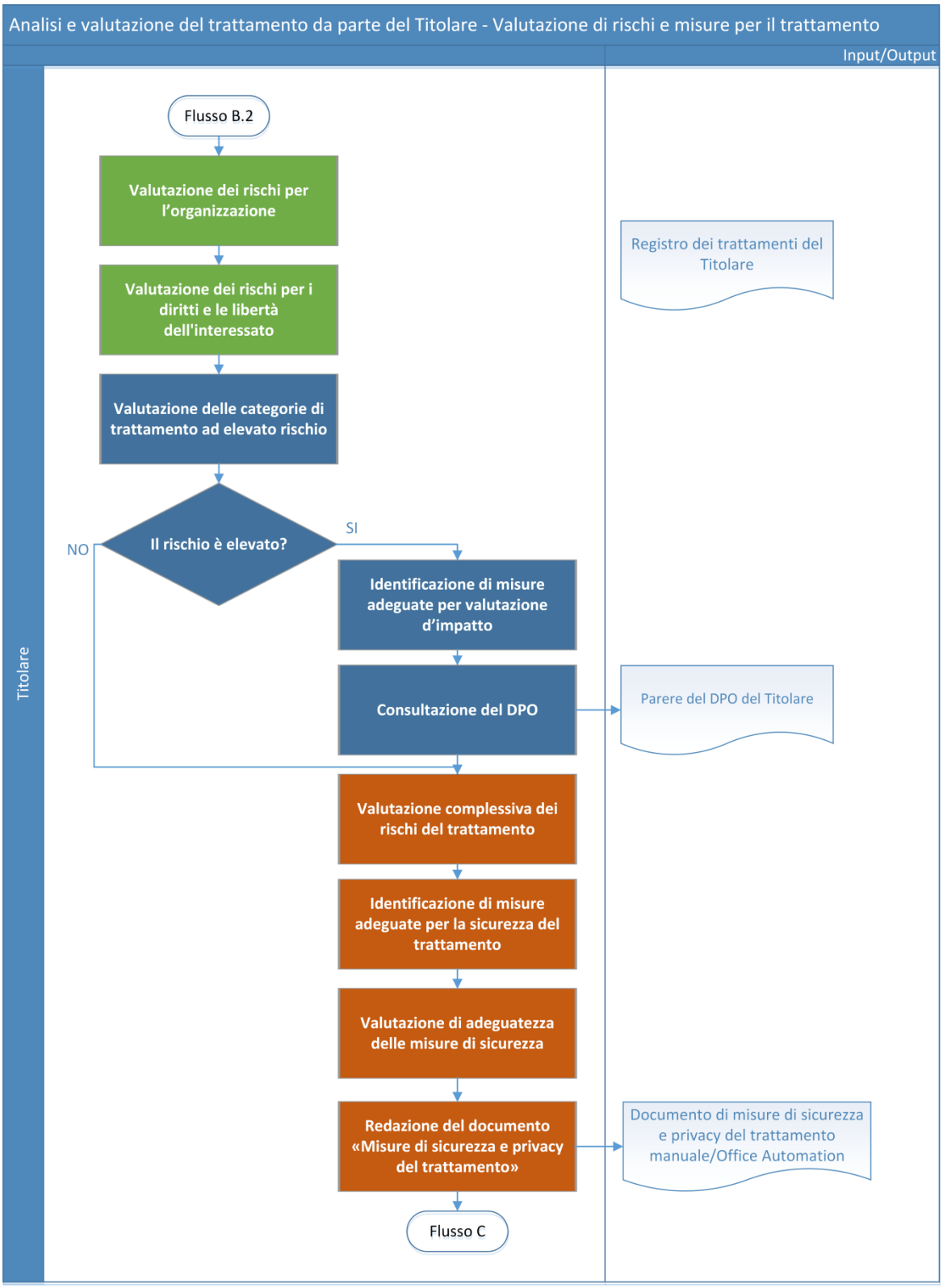
Oltre alle misure selezionate sulla base del profilo di rischio del trattamento/ Servizio ICT, Sogei protegge tutte le informazioni che tratta in qualità di Titolare o di Responsabile con un set di misure infrastrutturali elencate in specifici allegati ai registri dei trattamenti.

3. FLUSSO B.2 - VALUTAZIONE DI RISCHI E MISURE PER IL TRATTAMENTO DA PARTE DEL TITOLARE

3.1 FLUSSO E CARTA DELLE RESPONSABILITÀ

Di seguito è riportato il flusso di valutazione[8], relativamente alle attività di trattamento cartaceo o supportato da strumenti informatici di office automation, dei rischi per i diritti e le libertà dell'interessato, compresa la valutazione d'impatto (PIA), e dei rischi relativi alla sicurezza delle informazioni.

[8] Nel flusso sono rappresentate, in colore diverso, le attività relative ai trattamenti (colore arancio), quelle che riguardano la privacy by design e la sicurezza delle informazioni (colore verde) e quelle che riguardano la valutazione di impatto (colore blu).



La tabella riportata di seguito elenca le attività del flusso riportando per ognuna le responsabilità secondo la matrice RACI.[9]

Nome Attività	Ruoli / Responsabilità	
	Owner Trattamento	**DPO Titolare**
Valutazione dei rischi per l'organizzazione	**R**	**-**
Valutazione dei rischi per i diritti e le libertà degli interessati	**R**	**I**
Valutazione delle categorie di trattamento ad elevato rischio	**R**	**I**
Identificazione di misure adeguate per privacy impact assessment	**R**	**I**
Consultazione del DPO	**R**	**C**
Valutazione complessiva dei rischi del Servizio ICT	**R**	**I**
Identificazione di misure adeguate per la sicurezza del Servizio ICT	**R**	**I**
Valutazione di adeguatezza delle misure di sicurezza	**R**	**I**
Redazione del documento "Misure di sicurezza e privacy del trattamento …"	**R**	**I**

Tabella 15 – Flusso B2: Matrice RACI

[9] La matrice è organizzata secondo il modello RACI che prevede quattro ruoli:
R = **Responsible**. Esegue l'attività e ne è responsabile. Per la stessa attività è ammessa una responsabilità condivisa, ossia è possibile la presenza di più "R".
A = **Accountable**. Coordina, supervisiona e approva i vari task che compongono l'attività; può eseguirne alcuni ed è responsabile anche degli aspetti economici. È unico per l'attività e deve essere individuato nel caso vi sia la presenza di più "R".
C = **Consulted.** È consultato poiché possiede informazioni e/o capacità necessarie per portare a termine l'attività.
I = **Informed**. È informato dei risultati dell'attività.

3.2 DESCRIZIONE SINTETICA DELLE ATTIVITÀ

L'approccio per la valutazione dei rischi e per l'individuazione di misure adeguate al trattamento, nel caso in cui il trattamento sia eseguito su supporti cartacei o tramite strumenti di office automation, è del tutto analogo a quanto descritto relativamente ai trattamenti supportati da Servizi ICT (cap. 5, FLUSSO B - ANALISI E VALUTAZIONE DEL SERVIZIO ICT DA PARTE DEL TITOLARE E DEL RESPONSABILE).

Le principali differenze si sostanziano in:

- conduzione delle attività descritte a cura dell'Owner del trattamento, con l'eventuale supporto dei responsabili/esperti della sicurezza fisica o dei servizi di office automation dell'organizzazione;
- identificazione e valutazione di misure di sicurezza specifiche per l'ambito dei trattamenti cartacei o effettuati con strumenti di office automation;
- redazione ed approvazione, da parte dell'Owner del trattamento, del documento di "Misure di sicurezza e privacy del trattamento".

4. VALUTAZIONE DI RISERVATEZZA E INTEGRITA' PER SERVIZI ICT

Area d'analisi	Impatto	Perdita Finanziaria	Compromissione (rallentamento, blocco, …) delle attività di business	Perdita di immagine	Sanzioni amministrative e/o penali previste da normative[10]
Riservatezza	Che impatto ha l'accesso non autorizzato[11] ai dati da parte di personale interno o esterno?	*Nullo, Basso Medio, Alto*	*Nullo, Basso Medio, Alto*	*Nullo, Basso Medio, Alto*	*Nullo, Basso Medio, Alto*
Integrità	Che impatto ha un'alterazione non autorizzata[12] dei dati?	*Nullo, Basso Medio, Alto*	*Nullo, Basso Medio, Alto*	*Nullo, Basso Medio, Alto*	*Nullo, Basso Medio, Alto*

Tabella 16 – Valutazione del rischio per perdita di Riservatezza e Integrità

Valutazione Impatto[13]	Perdita Finanziaria[14]	Compromissione (rallentamento, blocco, …) delle attività di business[15]	Perdita di immagine	Sanzioni amministrative e/o penali previste da normative[16]
Trascurabile	Perdita finanziaria nulla (n.a.)	Nessun impatto sui processi e/o sugli utenti	Nessuna perdita d'immagine	Non esiste normativa specifica applicabile al trattamento dei dati

[10] Violazione degli obblighi di legge relativi alla normativa privacy o ad altre normative specifiche applicabili al trattamento del dato
[11] Per dolo, colpa, errore, malfunzionamento.
[12] Per dolo, colpa, errore, malfunzionamento.
[13] La valutazione dell'impatto va effettuata sul singolo evento più grave che presumibilmente può accadere.
[14] La perdita finanziaria è stimata sui processi di business del cliente nel caso si tratti di servizi informatici erogati per conto dell'Amministrazione (in particolare nel caso in cui il Servizio ICT tratti direttamente transazioni finanziarie, come servizi di pagamento allo sportello o giocate su eventi sportivi) o sui processi di business aziendali nel caso si tratti di servizi informatici interni.
[15] La compromissione (rallentamento e/o blocco delle attività di business) sono stimate sui processi di business del cliente nel caso si tratti di servizi informatici erogati per conto dell'Amministrazione o sui processi di business aziendali nel caso si tratti di servizi informatici interni.
[16] Violazione degli obblighi di legge relativi al codice privacy o ad altre normative specifiche applicabili al trattamento del dato

Valutazione Impatto[13]	Perdita Finanziaria[14]	Compromissione (rallentamento, blocco, …) delle attività di business[15]	Perdita di immagine	Sanzioni amministrative e/o penali previste da normative[16]
Basso	Perdita finanziaria trascurabile	Impatto operativo di bassa entità in quanto i dati interessano, ad esempio, un solo processo e/o un numero molto limitato di utenti	Perdita d'immagine di bassa rilevanza in quanto i dati interessano un limitato bacino di utenza e/o la compromissione degli stessi può interessare la stampa locale	Esiste normativa specifica applicabile al trattamento dei dati gestiti che non prevede sanzioni amministrative e/o penali
Medio	Impatto finanziario di media rilevanza in quanto i dati sono riconducibili a Servizi ICT che trattano indirettamente "movimentazioni economiche" (es. consuntivazioni, budget, …)	Impatto operativo di media entità in quanto i dati interessano, ad esempio, un numero medio di processi e/o di utenti	Perdita di immagine di media rilevanza in quanto i dati sono d'interesse per alcune categorie di utenti esterni e/o la compromissione degli stessi può generare: -news negative su media a diffusione nazionale -richiesta di informativa dell'azionista e degli organi di controllo	Esistono sanzioni previste dalla normativa privacy, in quanto sono trattati dati personali (ma non sensibili o giudiziari) Esistono sanzioni amministrative previste da altra normativa specifica applicabili al trattamento dei dati in oggetto (es. D. Lgs. 231/01 per processi aziendali)
Alto	Impatto finanziario di elevata rilevanza in quanto i dati sono riconducibili a Servizi ICT che gestiscono direttamente "movimentazioni economiche" (es. pagamenti, giocate, …)	Impatto operativo di alta entità in quanto i dati interessano, ad esempio, un numero consistente di processi e/o di utenti	Perdita di immagine di elevata rilevanza in quanto i dati sono d'interesse per gran parte degli utenti esterni e/o la compromissione degli stessi può generare: -interventi negativi sulla stampa nazionale interventi dell'azionista e degli organi di controllo - interventi politici	Esistono sanzioni previste dalla normativa privacy, in quanto sono trattati dati personali sensibili e/o giudiziari Esistono sanzioni penali previste da altra normativa specifica applicabili al trattamento dei dati in oggetto

Tabella 17 – Legenda per la valutazione del rischio di perdita di Riservatezza e Integrità

5. VALUTAZIONE DI DISPONIBILITA' PER SERVIZI ICT

Area d'analisi	Impatto	Perdita Finanziaria	Compromissione (rallentamento, blocco, …) delle attività di business	Perdita di immagine	Sanzioni amministrative e/o penali previste da normative[17]
Disponibilità[18]	Che impatto ha l'indisponibilità a breve (inferiore a 1 ora) del Servizio ICT?	*Nullo, Basso Medio, Alto*	*Nullo, Basso Medio, Alto*	*Nullo, Basso Medio, Alto*	*Nullo, Basso Medio, Alto*
	Che impatto ha l'indisponibilità media (tra 1 e 4 ore) del Servizio ICT?	*Nullo, Basso Medio, Alto*	*Nullo, Basso Medio, Alto*	*Nullo, Basso Medio, Alto*	*Nullo, Basso Medio, Alto*
	Che impatto ha l'indisponibilità prolungata (superiore a 4 ore) del Servizio ICT?	*Nullo, Basso Medio, Alto*	*Nullo, Basso Medio, Alto*	*Nullo, Basso Medio, Alto*	*Nullo, Basso Medio, Alto*

Tabella 18 – Valutazione del rischio per perdita di Disponibilità

[17] Violazione degli obblighi di legge relativi alla normativa privacy o ad altre normative specifiche applicabili al trattamento del dato
[18] Si applicano i criteri previsti per la Business Impact Analysis

Valutazione Impatto[19]	**Perdita Finanziaria**[20]	**Compromissione (rallentamento, blocco, …) delle attività di business**[21]	**Perdita di immagine**	**Sanzioni amministrative e/o penali previste da normative**[22]
Trascurabile	Perdita finanziaria nulla (n.a.)	Nessun impatto sui processi e/o sugli utenti	Nessuna perdita d'immagine	Non esiste normativa specifica applicabile al trattamento dei dati
Basso	Perdita finanziaria trascurabile	Impatto operativo di bassa entità in quanto i dati interessano, ad esempio, un solo processo e/o un numero molto limitato di utenti	Perdita d'immagine di bassa rilevanza in quanto i dati interessano un limitato bacino di utenza e/o la compromissione degli stessi può interessare la stampa locale	Esiste normativa specifica applicabile al trattamento dei dati gestiti che non prevede sanzioni amministrative e/o penali
Medio	Impatto finanziario di media rilevanza in quanto i dati sono riconducibili a Servizi ICT che trattano indirettamente "movimentazioni economiche" (es. consuntivazioni, budget, …)	Impatto operativo di media entità in quanto i dati interessano, ad esempio, un numero medio di processi e/o di utenti	Perdita di immagine di media rilevanza in quanto i dati sono d'interesse per alcune categorie di utenti esterni e/o la compromissione degli stessi può generare: - news negative su media a diffusione nazionale - richiesta di informativa dell'azionista e degli organi di controllo	Esistono sanzioni previste dalla normativa privacy, in quanto sono trattati dati personali (ma non sensibili o giudiziari) Esistono sanzioni amministrative previste da altra normativa specifica applicabili al trattamento dei dati in oggetto (es. D. Lgs. 231/01 per processi aziendali)

[19] La valutazione dell'impatto va effettuata sul singolo evento più grave che presumibilmente può accadere.
[20] La perdita finanziaria è stimata sui processi di business del cliente nel caso si tratti di servizi informatici erogati per conto dell'Amministrazione (in particolare nel caso in cui il Servizio ICT tratti direttamente transazioni finanziarie, come servizi di pagamento allo sportello o giocate su eventi sportivi) o sui processi di business aziendali nel caso si tratti di servizi informatici interni.
[21] La compromissione (rallentamento e/o blocco delle attività di business) sono stimate sui processi di business del cliente nel caso si tratti di servizi informatici erogati per conto dell'Amministrazione o sui processi di business aziendali nel caso si tratti di servizi informatici interni.
[22] Violazione degli obblighi di legge relativi alla normativa privacy o ad altre normative specifiche applicabili al trattamento del dato

Valutazione Impatto[19]	**Perdita Finanziaria[20]**	**Compromissione (rallentamento, blocco, …) delle attività di business[21]**	**Perdita di immagine**	**Sanzioni amministrative e/o penali previste da normative[22]**
Alto	Impatto finanziario di elevata rilevanza in quanto i dati sono riconducibili a Servizi ICT che gestiscono direttamente "movimentazioni economiche" (es. pagamenti, giocate, …)	Impatto operativo di alta entità in quanto i dati interessano, ad esempio, un numero consistente di processi e/o di utenti	Perdita di immagine di elevata rilevanza in quanto i dati sono d'interesse per gran parte degli utenti esterni e/o la compromissione degli stessi può generare: - interventi negativi sulla stampa nazionale - interventi dell'azionista e degli organi di controllo - interventi politici .	Esistono sanzioni previste dalla normativa privacy, in quanto sono trattati dati personali sensibili e/o giudiziari
				Esistono sanzioni penali previste da altra normativa specifica applicabili al trattamento dei dati in oggetto

Tabella 19 - Legenda per la valutazione del rischio di perdita di Disponibilità

6. VALUTAZIONE DEI RISCHI PER GLI INTERESSATI RELATIVI AI DATI TRATTATI

6.1 MINACCE E SCENARI DI RISCHIO

Minacce	Scenari di rischio specifici
Accesso, trattamento non autorizzato o illegittimo relativo a dati	Accesso, trattamento non autorizzato o illegittimo relativo a dati personali comuni
	Accesso, trattamento non autorizzato o illegittimo relativo a dati personali sensibili
	Accesso, trattamento non autorizzato o illegittimo relativo a dati personali ipersensibili
	Accesso, trattamento non autorizzato o illegittimo relativo a dati personali specifici
	Accesso, trattamento non autorizzato o illegittimo relativo a dati personali giudiziari
	Accesso, trattamento non autorizzato o illegittimo relativo a dati personali biometrici
Divulgazione non autorizzata o accidentale di dati	Divulgazione non autorizzata o accidentale di dati personali comuni
	Divulgazione non autorizzata o accidentale di dati personali sensibili
	Divulgazione non autorizzata o accidentale di dati personali ipersensibili
	Divulgazione non autorizzata o accidentale di dati personali specifici
	Divulgazione non autorizzata o accidentale di dati personali giudiziari
	Divulgazione non autorizzata o accidentale di dati personali biometrici
Modifica non autorizzata o accidentale di dati	Modifica non autorizzata o accidentale di dati personali comuni
	Modifica non autorizzata o accidentale di dati personali sensibili
	Modifica non autorizzata o accidentale di dati personali ipersensibili
	Modifica non autorizzata o accidentale di dati personali specifici
	Modifica non autorizzata o accidentale di dati personali giudiziari
	Modifica non autorizzata o accidentale di dati personali biometrici
Perdita, distruzione accidentale o illegale di dati	Perdita, distruzione accidentale o illegale di dati personali comuni
	Perdita, distruzione accidentale o illegale di dati personali sensibili
	Perdita, distruzione accidentale o illegale di dati personali ipersensibili
	Perdita, distruzione accidentale o illegale di dati personali specifici

Minacce	Scenari di rischio specifici
	Perdita, distruzione accidentale o illegale di dati personali giudiziari
	Perdita, distruzione accidentale o illegale di dati personali biometrici
Indisponibilità temporanea o prolungata di dati	Indisponibilità temporanea o prolungata di dati personali comuni
	Indisponibilità temporanea o prolungata di dati personali sensibili
	Indisponibilità temporanea o prolungata di dati personali ipersensibili
	Indisponibilità temporanea o prolungata di dati personali specifici
	Indisponibilità temporanea o prolungata di dati personali giudiziari
	Indisponibilità temporanea o prolungata di dati personali biometrici

Tabella 20 – Minacce e scenari di rischio

6.2 CRITERI PER LA VALUTAZIONE DELL'IMPATTO

Danno	Descrizione
Danno fisico-biologico	La lesione di attività vitali quali: la modificazione all'aspetto esteriore di una persona; la riduzione dalla capacità di relazionarsi con altri individui; la riduzione della capacità lavorativa e/o dell'attitudine di una persona a lavorare; la perdita di chance lavorative; la perdita della capacità sessuale; il danno psichico.
Danno finanziario	Inteso come la perdita economica che colpisce direttamente l'individuo limitandone le capacità di attendere alle proprie incombenze (i.e. perdita dello stipendio).
Danno reputazionale	Inteso come la perdita della considerazione che un individuo gode nell'ambiente sociale in cui vive.
Danno di identità	Inteso come il furto che un individuo può subire della propria identità digitale con conseguenze, nei casi più gravi, anche di natura penale.

6.3 VALUTAZIONE DELL'IMPATTO

Legenda per la compilazione della matrice dell'impatto

Impatto	Danno fisico-biologico	Danno finanziario	Danno reputazionale	Danno di identità
Trascurabile	La persona fisica/interessato non ha subito una lesione nel fisico o nella psiche. Non ci sono ripercussioni negative, di carattere non patrimoniale, della lesione psicofisica	la persona fisica/ interessato non ha subito una perdita economica e/o un mancato guadagno tali da comprometterne dignità e libertà	la persona fisica/ interessato non subisce nessun tipo di danno che possa lederne dignità, immagine e reputazione	la persona fisica/ interessato non subisce nessuna lesione della propria identità digitale
Bassa	La persona fisica può subire una lesione di lieve entità nel fisico o nella psiche. Probabili ripercussioni negative, di carattere non patrimoniale, della lesione psicofisica che possono portare ad una liquidazione del danno biologico, da parte del giudidce di lieve entità (i.e. invalidità temporanea che consiste nel numero di giorni necessari per la guarigione e per il ritorno alla normale attività)	la persona fisica/ interessato ha subito una perdita economica e/o un mancato guadagno classificabile come lieve (i.e. tempo dedicato allo svolgimento di pratiche burocratiche, mancata possibilità di pagare le utenze in tempo utile per non incorrere in sanzioni per il blocco dei sistemi informatici (riscossione/pagamento)	la persona fisica/ interessato subisce un semplice fastidio a causa di informazioni di carattere non sensibile divulgate e/o ricevute in maniera difforme rispetto la realtà (i.e. attribuzione di titoli scolastici diversi, indicazioni di condizioni di tipo familiare non coerenti)	la persona fisica/ interessato subisce un semplice fastidio dovuto a informazioni ricevute o richieste nel caso di omonimia (richiesta di pagamenti/tasse/imposte, mancata risposta a chiarimenti e/o istanze)

Impatto	Danno fisico-biologico	Danno finanziario	Danno reputazionale	Danno di identità
Media	La persona fisica ha subito una lesione di media entita nel fisico o nella psiche. Ripercussioni negative, di carattere non patrimoniale, della lesione psicofisica che portano ad una liquidazione da parte del giudice del danno biologico (i.e. invalidità temporanea che consiste nel numero di giorni necessari per la guarigione e per il ritorno alla normale attività: invalidità permanente determinata in base all'età del danneggiato e dal grado di invalidità permanente calcolato sui "c. d. punti")	la a persona fisica/ interessato ha subito una perdita economica e/o un mancato guadagno che può comportare: pagamenti imprevisti (multe e/o imposte dovuti per calcoli errati), costi aggiuntivi (spese bancarie, spese legali), mancato accesso a servizi amministrativi o commerciali, aumento dei costi (ad esempio prezzi assicurativi aumentati), promozione di carriera persa	la persona fisica/ interessato subisce l'invio di messaggi di tipo pubblicitario o promozionale che possono svelare un aspetto della propria vita riservato e risultare lesive della sua dignità (gravidanza, trattamento farmacologico, disoccupazione, difficoltà economiche, patologie mediche)	la persona fisica/ interessato subisce un'illecita intrusione nella propria sfera personale da parte di soggetti terzi con scopi discriminatori (razzismo, sessismo, intimidazione politica e/o sociale)
Alta	La persona fisica ha subito una grave lesione nel fisico o nella psiche. Evidenti Ripercussioni negative, di carattere non patrimoniale, della lesione psicofisica. La liquidazione da parte del giudice del danno biologico comporta un esborso economico molto oneroso (i.e. invalidità temporanea che consiste nel numero di giorni necessari per la guarigione e per il ritorno alla normale attività: invalidità	la persona fisica/ interessato ha subito una perdita economica e/o un mancato guadagno che può comportare: elevate difficoltà finanziarie con obbligo di richiesta di prestiti, perdita di proprietà e/o alloggi, mancata possibilità di adempiere ad obbligazioni contrattuali per indisponibilità di denaro, perdita di occupazione/tirocini /impiego (anche a tempo determinato), impossibilità di	la persona fisica/ interessato subisce gravi conseguenze per la propria dignità e che portano alla perdita di onorabilità/danni all'immagine (notizie su TV, stampa o social media), perdita/ impossibilità occupazionale, lesione della propria posizione creditizia/economica	la persona fisica/ interessato subisce conseguenze irreversibili quali sanzioni di tipo penale, perdita di diritti/status amministrativo/autonomia (i.e. procedura di interdizione, inabilitazione, disconoscimento della patria potestà)

Impatto	Danno fisico-biologico	Danno finanziario	Danno reputazionale	Danno di identità
	permanente determinata in base all'età del danneggiato e dal grado di invalidità permanente calcolato sui "c. d. punti")	proseguire il percorso di studio/abilitazione/ perfezionamento intrapreso		

Tabella 21 – Legenda per la valutazione impatto

6.4 VALUTAZIONE DELLA PROBABILITÀ DI ACCADIMENTO

Legenda per la valutazione della probabilità di accadimento

T	Agenti INTERNI	Un potenziale attaccante interno non otterrebbe vantaggi signifi-cativi (es. a seguito di compromissione dei dati o del servizio).
		Il clima dell'organizzazione in relazione all'ambito in analisi (es. opinioni, pareri, …) è positivo.
	Agenti ESTERNI	Il servizio non risulta di interesse sociale, economico, politico e mediatico.
		Un potenziale attaccante esterno non otterrebbe vantaggi significativi (es. a seguito di compromissione dei dati o del servizio).
	Errori/eventi ACCIDENTALI	Il contesto di riferimento (es. normativa di riferimento, tipologie di soggetti coinvolti, complessità operativa, ...) non è complesso.
		La frequenza di accadimento degli eventi accidentali registrati è molto bassa.
B	Agenti INTERNI	Un potenziale attaccante interno potrebbe otterrebbe lievi vantaggi (es. a seguito di compromissione dei dati o del servizio).
		Il clima dell'organizzazione in relazione all'ambito in analisi è o potrebbe essere influenzato da criticità non significative (es. opinioni contrarie, incertezze, ...).
	Agenti ESTERNI	Il servizio risulta di scarso interesse sociale, economico, politico e mediatico.
		Un potenziale attaccante esterno potrebbe ottenere lievi vantaggi (es. a seguito di compromissione dei dati o del servizio).
	Errori/eventi ACCIDENTALI	Il contesto di riferimento (es. normativa di riferimento, tipologie di soggetti coinvolti, complessità operativa, ...) è di bassa complessità.
		La frequenza di accadimento degli eventi accidentali registrati è bassa.
M	Agenti INTERNI	Un potenziale attaccante interno potrebbe ottenere vantaggi (es. a seguito di compromissione dei dati o del servizio).
		Il clima dell'organizzazione in relazione all'ambito in analisi è o potrebbe essere parzialmente negativo (es. dissensi, opposizioni).

	Agenti ESTERNI	Il servizio è di interesse sociale, economico, politico e mediatico o risulta significativo per le attività di determinate categorie di utenti esterni (es. professionisti, fornitori, ...).
		Un potenziale attaccante esterno potrebbe ottenere vantaggi (es. a seguito di compromissione dei dati o del servizio).
	Errori/eventi ACCIDENTALI	Il contesto di riferimento (es. normativa di riferimento, tipologie di soggetti coinvolti, complessità operativa, ...) è di ordinaria complessità.
		La frequenza di accadimento degli eventi accidentali registrati è media.
A	Agenti INTERNI	Un potenziale attaccante interno potrebbe ottenere grandi vantaggi (es. a seguito di compromissione dei dati o del servizio).
		Il clima dell'organizzazione in relazione all'ambito in analisi è o potrebbe essere fortemente negativo (es. forti dissensi, proteste).
	Agenti ESTERNI	Il servizio risulta di grande interesse sociale, economico, politico e mediatico (es. pubblicizzato sulla stampa nazionale) e l'ambito in cui si colloca è in particolare fermento.
		Un potenziale attaccante esterno potrebbe ottenere grandi vantaggi (es. a seguito di compromissione dei dati o del servizio).
	Errori/eventi ACCIDENTALI	Il contesto di riferimento (es. normativa di riferimento, tipologie di soggetti coinvolti, complessità operativa, ...) presenta una elevata complessità.
		La frequenza di accadimento degli eventi accidentali registrati è alta.

Tabella 22 – Legenda per la valutazione probabilità di accadimento

6.5 VALUTAZIONE DEL RISCHIO INTRINSECO PER DIRITTI E LIBERTÀ DELL'INTERESSATO

Si riporta un esempio di valutazione e compilazione della tabella dei rischi per i diritti e le libertà degli interessati, in relazione alle categorie di dati trattati.

Minacce	Rischio Intrinseco per scenario specifico	Probabilità di accadimento	Gravità Danno Fisico-Biologico	Gravità Danno Finanzia-rio	Gravità Danno Reputazio-nale	Gravità Danno Identità	Rischio Intrinseco (max per scenario specifico)	Rischio Intrinseco relativo alla minaccia
Accesso, trattamento non autorizzato o illecito relativo a dati	Accesso, trattamento non autorizzato o illecito relativo a dati personali comuni	M	M	M	M	M	**M**	Max dei rischi intrinseci sugli scenari applicabili
	Accesso, trattamento non autorizzato o illecito relativo a dati sensibili	A	M	A	A	A	**A**	
	Accesso, trattamento non autorizzato o illecito relativo a dati ipersensibili	A	A	A	A	A	**A**	
	Accesso, trattamento non autorizzato o illecito relativo a dati specifici	A	M	A	A	A	**A**	
	Accesso, trattamento non autorizzato o illecito relativo a dati giudiziari	A	M	A	A	A	**A**	
	Accesso, trattamento non autorizzato o illecito relativo a dati biometrici	A	M	M	A	A	**A**	
Divulgazione non autorizzata o accidentale di dati	Divulgazione non autorizzata o accidentale di dati personali comuni	M	M	M	M	M	**M**	Max dei rischi intrinseci sugli scenari applicabili
	Divulgazione non autorizzata o accidentale di dati sensibili	A	M	A	A	A	**A**	
	Divulgazione non autorizzata o accidentale di dati ipersensibili	A	A	A	A	A	**A**	
	Divulgazione non autorizzata o accidentale di dati specifici	A	M	A	A	A	**A**	
	Divulgazione non autorizzata o accidentale di dati giudiziari	A	M	A	A	A	**A**	
	Divulgazione non autorizzata o accidentale di dati biometrici	A	M	A	A	A	**A**	
Modifica non autorizzata o accidentale di dati	Modifica non autorizzata o accidentale di dati personali comuni	M	M	M	M	M	**M**	Max dei rischi intrinseci sugli scenari applicabili
	Modifica non autorizzata o accidentale di dati sensibili	A	M	A	A	A	**A**	
	Modifica non autorizzata o accidentale di dati ipersensibili	A	A	A	A	A	**A**	

Minacce	Rischio Intrinseco per scenario specifico	Probabilità di accadimento	Gravità Danno Fisico-Biologico	Gravità Danno Finanzia-rio	Gravità Danno Reputazio-nale	Gravità Danno Identità	Rischio Intrinseco (max per scenario specifico)	Rischio Intrinseco relativo alla minaccia
	Modifica non autorizzata o accidentale di dati specifici	A	M	A	A	A	**A**	
	Modifica non autorizzata o accidentale di dati giudiziari	A	M	A	A	A	**A**	
	Modifica non autorizzata o accidentale di dati biometrici	A	M	A	A	A	**A**	
Perdita, distruzione accidentale o illecita di dati	Perdita, distruzione accidentale o illecita di dati personali comuni	M	M	M	M	M	**M**	Max dei rischi intrinseci sugli scenari applicabili
	Perdita, distruzione accidentale o illecita di dati sensibili	M	M	A	M	A	**A**	
	Perdita, distruzione accidentale o illecita di dati ipersensibili	M	A	A	M	A	**A**	
	Perdita, distruzione accidentale o illecita di dati specifici	M	M	A	M	A	**A**	
	Perdita, distruzione accidentale o illecita di dati giudiziari	M	M	A	M	A	**A**	
	Perdita, distruzione accidentale o illecita di dati biometrici	M	M	M	M	A	**A**	
Indisponibilità temporanea o prolungata di dati	Indisponibilità temporanea o prolungata di dati personali comuni	M	M	M	M	M	**M**	Max dei rischi intrinseci sugli scenari applicabili
	Indisponibilità temporanea o prolungata di dati sensibili	M	M	A	M	A	**A**	
	Indisponibilità temporanea o prolungata di dati ipersensibili	M	A	A	M	A	**A**	
	Indisponibilità temporanea o prolungata di dati specifici	M	M	A	M	A	**A**	
	Indisponibilità temporanea o prolungata di dati giudiziari	M	M	A	M	A	**A**	
	Indisponibilità temporanea o prolungata di dati biometrici	M	M	M	M	A	**A**	

Tabella 23 - Stima del rischio intrinseco per i diritti e le libertà dell'interessato

7. VALUTAZIONE DEI RISCHI PER GLI INTERESSATI RELATIVI ALLE CATEGORIE DI TRATTAMENTO

Criteri per individuazione di trattamenti ad alto rischio per diritti e libertà dell'interessato	Esempi di trattamento
Valutazione o assegnazione di un punteggio (incluse le attività di profilazione e le analisi di tipo predittivo) riferita ad un individuo	Il trattamento prevede: - l'uso di database per la valutazione del rischio creditizio, per la lotta alle frodi o al riciclaggio e al finanziamento del terrorismo (AML/CTF); - test genetici offerti direttamente ai consumatori per finalità predittive del rischio di determinate patologie o in generale per lo stato di salute; - la creazione di profili comportamentali o marketing a partire dalle operazioni o dalla navigazione compiute sul sito web del Titolare.
Decisioni automatizzate con significativi effetti giuridici o di analoga natura	Il trattamento può comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione. Il trattamento che produce effetti minimi o nulli su un interessato non soddisfa questo specifico criterio.
Monitoraggio sistematico di individui (es. mediante videosorveglianza)	Il trattamento prevede il monitoraggio sistematico in termini di controllo e sorveglianza di soggetti interessati, anche in spazi pubblici (ad es. videosorveglianza di stazioni, aeroporti, aree di grandi dimensioni)
Elaborazione di dati sensibili o dati aventi carattere altamente personale	Il trattamento prevede l'uso di categorie di dati particolari (stato di salute, opinioni politiche, credo religioso, etc.) o che possano accrescere i rischi per i diritti e le libertà degli interessati (dati di localizzazione, finanziari, dati strettamente personali e confidenziali, etc.) di cui agli artt. 9 e 10 del RGPD
Elaborazione di dati su larga scala (es. per numero di individui coinvolti, volumi complessivi, durata o persistenza, ambito geografico)	Il trattamento prevede che siano elaborati dati su larga scala in termini di : - numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; - volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; - durata, o persistenza, dell'attività di trattamento; - ambito geografico dell'attività di trattamento.
Combinazione o raffronto tra banche dati provenienti da due o più operazioni di trattamento effettuati per scopi diversi	Il trattamento prevede che siano per esempio utilizzati dati derivanti da due o più trattamenti ma svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato (ad es. dati raccolti per finalità di erogazione di servizi a famiglie associati a dati riferiti alle possibilità di spesa sulla base di condizioni reddituali)

Elaborazione di dati relativi a soggetti vulnerabili per cui è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento (es. minori, anziani, dipendenti)	Il trattamento prevede l'elaborazione di dati e di informazioni riferite a minori o a persone che non siano in grado di opporsi o acconsentire, in modo consapevole e ragionato, al trattamento dei propri dati personali (i soggetti con patologie psichiatriche, i richiedenti asilo, gli anziani, i pazienti) e ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento.
Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative	il trattamento prevede l'associazione di tecniche dattiloscopiche (digitazione del PIN) con il riconoscimento del volto per migliorare il controllo degli accessi fisici oppure il trattamento l'utilizzo di applicazioni legate al c.d. "Internet delle cose" (biomedicale, monitoraggio, servizi ai cittadini riferibili alle smart city)
Impedimento all'interessato di esercitare un diritto o di avvalersi di un servizio o di un contratto	Il trattamento non prevede il diritto alla portabilità dei dati o la cancellazione dei dati

Tabella 24 - Categorie trattamento ad alto rischio per diritti e libertà interessato