CONVENZIONE

tra

Il Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto per l'emergenza epidemiologica COVID -19 e per l'esecuzione della campagna vaccinale nazionale, Gen. C.A. Francesco Paolo Figliuolo, nominato con DPCM 1°- 2021, (di seguito "**Commissario**"),

e

la **SOGEI - Società Generale d'Informatica S.p.A.**, con sede legale in Roma, via Mario Carucci n. 99, iscritta al registro delle imprese di Roma al n. 02327910580, coincidente con il numero di codice fiscale, partita IVA n. 01043931003, per la quale interviene il dottor Andrea Quacivi, Amministratore Delegato, che agisce in virtù dei poteri conferitigli dal Consiglio di amministrazione come da delibere del 7 agosto 2018 e del 22 maggio 2019 (di seguito "**Società**").

Il Commissario e la Società, di seguito, singolarmente anche "**Parte**" e congiuntamente "**Parti**",

PREMESSO CHE

- il 30 gennaio 2020, il Direttore generale dell'Organizzazione mondiale della sanità (OMS) ha dichiarato il focolaio internazionale da SARS-CoV-2, denunciato dalle autorità sanitarie cinesi, un'emergenza di sanità pubblica di rilevanza internazionale (Public Health Emergency of International Concern - PHEIC), come sancito nel Regolamento sanitario internazionale (International Health Regulations, IHR, 2005);
- in seguito al diffondersi del virus sul territorio nazionale con il conseguente accertamento di casi di contagio e di diffusione di malattia denominata dall'OMS "COVID-19", in data 31 gennaio 2020 il Consiglio dei ministri ha dichiarato lo stato di emergenza sanitaria per l'epidemia da nuovo coronavirus e attivato gli opportuni strumenti normativi precauzionali;
- nei mesi successivi, a seguito del diffondersi della pandemia, con successivi provvedimenti il Governo ha adottato plurimi provvedimenti contenenti misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19, estese a tutto il territorio nazionale, con i quali sono stati limitati gli spostamenti e in parte le attività dei cittadini;
- con modifiche al decreto-legge 25 marzo 2020 n. 19, convertito con modificazioni dalla legge 22 maggio 2020 n. 35, recante "Misure urgenti per fronteggiare l'emergenza epidemiologica da COVID-19" è stato prorogato al 31 luglio 2021 il termine dello stato di emergenza;
- ai sensi dell'articolo 122, del decreto-legge 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27, con decreto del Presidente del Consiglio dei ministri 1° marzo 2021, registrato alla Corte dei conti in data 3 marzo 2021 al n. 508, il Generale di Corpo d'Armata Francesco Paolo Figliuolo è stato nominato Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto

dell'emergenza epidemiologica COVID-19 e per l'esecuzione della campagna vaccinale nazionale, in sostituzione del precedente Commissario straordinario;

CONSIDERATO CHE

- l'articolo 122 del decreto-legge 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27, statuisce che il Commissario straordinario "*attua e sovrintende a ogni intervento utile a fronteggiare l'emergenza sanitaria, organizzando, acquisendo e sostenendo la produzione di ogni genere di bene strumentale utile a contenere e contrastare l'emergenza stessa, o comunque necessario in relazione alle misure adottate per contrastarla, nonché programmando e organizzando ogni attività connessa, individuando e indirizzando il reperimento delle risorse umane e strumentali necessarie, individuando i fabbisogni"* e che *"nell'esercizio di tali attività può avvalersi di soggetti attuatori e di società in house, nonché delle centrali di acquisto*";
- la precedente Struttura Commissariale è stata sostituita dall'attuale Struttura come da Ordinanza n. 1 in data 11.03.2021 del Commissario straordinario;
- con comunicazione prot. M_D E24363 REG2021 0026329 09-03-2021 il Commissario, ha richiesto alla Società, in considerazione della consolidata esperienza maturata nel tempo, di valutare la possibilità di intraprendere le seguenti iniziative volte al:
  - trasferimento delle piattaforme, comprensive di eventuali licenze dall'attuale gestore delle stesse;
  - migrazione dei flussi dati;
  - sviluppo di specifici applicativi per l'ottimizzazione di processi di lavoro.
- al fine di verificare la fattibilità del trasferimento di tutti i dati fino ad oggi prodotti dall'architettura informatica della precedente struttura commissariale, il tutto in costanza di operatività, per consentire alle istituzioni e ai cittadini di avere continua visibilità della risposta nazionale alla pandemia;
- con comunicazione in data 11 marzo 2021, prot. n. 0010152 la Società nel riscontrare la comunicazione del Commissario ha confermato la piena collaborazione da parte della stessa con tutte le sue strutture aziendali che opereranno a supporto della organizzazione del Commissario straordinario;
- la Sogei S.p.a., ai sensi dell'art. 4, comma 1 e 5, comma 2 dello Statuto, è a totale partecipazione pubblica ed interamente partecipata dal Ministero dell'Economia e delle Finanze;
- ai sensi del comma 2 del citato art. 4, "*la Società ha, altresì, quale oggetto lo svolgimento, nel rispetto della normativa vigente, di ogni attività di natura informatica per conto della Amministrazione pubblica centrale*";
- conformemente a quanto previsto dall'art. 26, comma 5 dello Statuto, la Società, preliminarmente alla sottoscrizione della presente Convenzione per l'affidamento diretto delle attività di cui al citato art. 4, comma 2, ha provveduto alle previste comunicazioni con lettera in data 30 marzo 2021, prot. n. 13129, al fine della verifica del mantenimento

dell'equilibrio economico finanziario in relazione all'iniziativa di cui al presente Convenzione;

- le condizioni di somma urgenza dell'esecuzione delle attività di trasferimento delle piattaforme in parola impongono il ricorso alla Società in virtù della consolidata esperienza per la realizzazione e gestione di sistemi informatici per le amministrazioni pubbliche e della capacità di intervenire senza soluzione alcuna di continuità nell'erogazione dei servizi, rendendone altresì necessaria l'anticipata esecuzione con comunicazione del Commissario straordinario prot. CSEC19RM 001 REG2021 1001680 del 30/03/2021;
- sussiste dunque l'esigenza di sottoscrivere ai sensi del richiamato articolo 122 del decreto-legge 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27, tra il Commissario e la Società la presente Convenzione per disciplinare i reciproci impegni delle Parti e dettagliare i contenuti delle attività da svolgere nel periodo di durata della Convenzione medesima;

TUTTO CIÒ PREMESSO E CONSIDERATO, LE PARTI

CONVENGONO E STIPULANO QUANTO SEGUE

Art. 1

(Oggetto della Convenzione)

1. La Società, con la sottoscrizione della Convenzione si impegna nei confronti del Commissario a porre in essere tutte le attività volte alla:
   - trasferimento delle piattaforme cloud, in ambiente Microsoft Azure, comprensive di tutti gli ambienti, di produzione e sviluppo, e soluzioni, dall'attuale gestore delle stesse;
   - migrazione dei flussi e delle banche dati;
   - manutenzione correttiva ed evolutiva degli applicativi.

   come definite nel documento Allegato A alla presente Convenzione denominato "Piano Operativo".
2. Resta inteso che le attività relative a nuovi sviluppi di specifici applicativi che saranno individuate dal Commissario verranno disciplinate in specifici Accordi che definiranno, altresì, l'impegno economico nonché gli specifici livelli di servizio e le relative penali.
3. La Società opererà sulla base delle direttive ed in stretto coordinamento con la struttura del Commissario.

Art. 2

(Durata)

1. La presente Convenzione rimane efficace dalla data della sua sottoscrizione fino al 31 marzo 2023, fatto salvo la possibilità di risolvere *ipso iure* la presente convenzione, senza

necessità di ulteriori comunicazioni, con il termine dello stato di emergenza, salvo che la stessa sia prorogata anche oltre la citata scadenza, per espresso accordo fra le Parti.

2. Resta inteso che la Convenzione potrà essere risolta, consensualmente, tra le Parti in qualsiasi momento di durata della stessa, nel caso in cui l'utilizzo delle Piattaforme di cui al precedente Articolo 1 non si renda più necessario per sopravvenute disposizioni normative o regolamentari ed a seguito di specifica comunicazione del Commissario che dovrà essere inviata alla SOGEI con un preavviso di 30 giorni rispetto alla data di prevista interruzione delle attività e dei servizi collegati all'utilizzo delle citate Piattaforme.

3. Resta, inoltre, inteso che, in ogni ipotesi di risoluzione anticipata, il Commissario sarà tenuto al pagamento delle prestazioni già correttamente eseguite dalla Società, e a quelle relative ai contratti sottoscritti con i fornitori di cui al successivo articolo 4, per i quali troveranno applicazione le clausole ivi previste in materia di recesso, senza che possano essere considerati imputabili al Commissario ulteriori costi, spese, indennizzi, o richieste di risarcimento del danno.

Art. 3

(Servizi, obblighi e responsabilità della Società)

1. La Società, ai fini dell'adempimento degli obblighi di cui all'articolo 1, erogherà i servizi riportati nel "Piano operativo" di cui all'Allegato A, nel quale sono, altresì, definiti i relativi livelli di servizio ed i corrispettivi.

2. Resta inteso che i corrispettivi relativi alle attività di diretta competenza della SOGEI, saranno definiti in conformità al parere AGID numero 12/2020 reso ai sensi dell'Articolo 14 bis, comma 2, lettera f) del Decreto Legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale, rilasciato in relazione al Disciplinare fra il Dipartimento della Ragioneria generale dello Stato del Ministero dell'economia e delle finanze e la Sogei.

3. Resta inteso che le attività di cui alla presente Convenzione saranno realizzate nel rispetto del vincolo delle risorse finanziarie a disposizione, quantificate al successivo articolo 5.

4. La Società non è in alcun modo responsabile per qualunque ritardo o impossibilità nello svolgimento delle attività alla stessa affidate, dovuti a cause ad essa non imputabili. In particolare, la Società non può essere ritenuta responsabile per eventuali danni materiali o patrimoniali, diretti o indiretti, qualora non ad essa imputabili o qualora la Società stessa abbia correttamente adempiuto alle obbligazioni di cui alla presente Convenzione ed abbia operato in aderenza alle direttive impartite; fermo restando quanto sopra e salvi i limiti inderogabili di legge.

5. Resta esclusa qualsiasi responsabilità del Commissario nel caso la Società usi, per l'esecuzione della presente Convenzione dispositivi e soluzioni di cui altri siano titolari di diritti di privativa.

6. La Società, conseguentemente, con la sottoscrizione della presente Convenzione fornisce manleva al Commissario da ogni pretesa e dagli oneri relativi ad azioni per violazione di qualsivoglia diritto di proprietà industriale o intellettuale relativo alle opere oggetto della Convenzione.

Art. 4

(Beni e servizi da acquisire)

1. Nei casi in cui la Società provveda ad acquisire, in nome proprio e per conto del Commissario, i beni ed i servizi necessari all'espletamento delle attività di cui al "Piano operativo" di cui all'Allegato A, il Commissario rimborserà alla Società gli importi da questa effettivamente corrisposti ai fornitori, quali risultanti dalla documentazione amministrativa e dalle scritture contabili della Società stessa.
2. Il Commissario prende atto che la Società per le acquisizioni di beni e servizi si avvale, per effetto dell'art. 4, comma 3-ter, del D.L. n. 95/2012, di Consip S.p.A, nella sua qualità di centrale di committenza della Società.
3. In relazione alla acquisizione dei beni o servizi, in nome proprio e per conto del Commissario, indicati nel "Piano operativo", quest'ultimo sosterrà i relativi costi eventualmente sostenuti dalla Società nei confronti di Consip nell'ambito del massimale di cui al successivo articolo 5 sulla base delle intese che saranno definite tra le Parti.

Art. 5

(Massimale della Convenzione)

1. Per le attività svolte dalla Società fino alla data di efficacia della presente Convenzione, l'importo massimale è determinato in Euro 6.965.262,32, oltre IVA.

Art. 6

(Rapporti Periodici e verifiche)

1. La Società darà conto al Commissario dei servizi erogati nell'ambito della presente Convenzione mediante appositi Rapporti Periodici quadrimestrali, che dovranno contenere:
   - il resoconto dei servizi realizzati/erogati con il relativo valore economico;
   - l'elenco dei beni e servizi acquistati con il relativo valore economico;
   - la documentazione a supporto per ciascuna delle voci di cui sopra ed in particolare, l'elenco delle fatture relative ai beni e servizi acquisite nella contabilità della Società**.**
2. I Rapporti Periodici dovranno essere inviati, per l'approvazione al Commissario entro 25 (venticinque) giorni dalla fine del quadrimestre, con sistema di posta elettronica certificata, al seguente indirizzo: commissarioemergenzacovid19@pec.governo.it ed, in copia, all'indirizzo sw@covid19.difesa.it, fermo restando che il Rapporto Periodico relativo

all'ultimo quadrimestre dell'anno verrà inviato entro 45 (quarantacinque) giorni dal termine del quadrimestre stesso.

3. Le eventuali osservazioni da parte della struttura commissariale sui Rapporti Periodici dovranno essere comunicate entro 30 (trenta) giorni dal loro ricevimento. Trascorso inutilmente tale termine, i Rapporti Periodici si intenderanno approvati ad ogni effetto.
4. Entro il termine previsto per l'invio del Rapporto Periodico relativo all'ultimo quadrimestre dell'anno di riferimento, la Società provvederà ad inviare al Commissario il consuntivo relativo ai beni e servizi acquisiti nell'anno di riferimento, le cui fatture non siano state ancora acquisite nella contabilità della Società, sul quale l'Amministrazione interessata comunicherà le proprie osservazioni entro il 28 febbraio dell'anno successivo a quello di riferimento, termine decorso il quale il consuntivo si intenderà approvato.

Art. 7

(Responsabili della Convenzione)

1. Per assicurare la corretta esecuzione delle attività ed il rispetto dei termini così come definiti nel "Piano operativo", le Parti procederanno, entro 10 giorni dalla data di sottoscrizione della presente Convenzione, alla nomina dei rispettivi Responsabili della Convenzione.

Art. 8

(Monitoraggio dei livelli di servizio e penali)

1. Gli eventuali livelli di servizio e le relative penali che la Società dovrà assicurare per lo svolgimento dei servizi di propria competenza nell'ambito della presente Convenzione, sono riportati nel "Piano operativo".
2. Ai fini del controllo dei suddetti livelli di servizio e della conseguente applicazione delle penali si procederà come segue:

   a) la Società darà evidenza al Responsabile della Convenzione dei livelli effettivamente conseguiti e degli eventuali scostamenti verificatisi rispetto a quelli convenuti;

   b) la Società manterrà a disposizione del Responsabile della Convenzione, per 90 (novanta) giorni dalla data di approvazione dell'ultimo Rapporto Periodico di cui all'articolo 6, comma 1, le registrazioni e/o le rilevazioni analitiche effettuate dal suddetto sistema.
3. Le penali potranno essere applicate dal Responsabile della Convenzione previa contestazione scritta dell'addebito e previa valutazione delle deduzioni al riguardo addotte dalla Società che dovranno essere presentate non oltre il termine di 30 (trenta) giorni dal ricevimento della comunicazione contenente la contestazione stessa.
4. Il Responsabile della Convenzione, valutate le predette deduzioni, potrà decidere di dare corso all'applicazione delle penali dandone comunicazione scritta alla Società.

5. La Società provvederà a riconoscere alla struttura commissariale quanto indicato nella comunicazione di cui al precedente comma 4, secondo le modalità definite al successivo articolo 9. Le Parti si danno peraltro atto che, qualora la Società ritenga di non condividere le conclusioni del Responsabile della Convenzione, il pagamento di cui sopra non potrà costituire in nessun caso riconoscimento di responsabilità e/o di debito ove la Società dia inizio alla procedura di cui al successivo articolo 11 entro 60 (sessanta) giorni dal pagamento stesso.
6. Resta inteso che, nel caso in cui gli inadempimenti siano determinati da causa di forza maggiore, nessuna pretesa risarcitoria potrà essere avanzata dal Responsabile della Convenzione nei confronti della Società stessa, ferma restando la necessità che la Società assicuri l'erogazione, senza soluzione di continuità, dei servizi previsti nella presente Convenzione.
7. Eventuali penali relative ai contratti stipulati dalla Società in nome proprio e per conto del Responsabile della Convenzione, saranno riconosciute al Responsabile della Convenzione.

Art. 9

(Fatturazione e pagamento)

1. La Società nell'ambito dell'importo complessivo di cui all'articolo 5, procederà con cadenza quadrimestrale alla fatturazione sulla base dei servizi erogati riportati nei singoli Rapporti Periodici di cui all'articolo 6, comma 1.
2. La Società procederà all'emissione delle fatture per le attività erogate di cui al comma precedente, successivamente all'approvazione dei Rapporti Periodici di cui al precedente articolo 6, comma 1.
3. Per i crediti derivanti dall'applicazione delle penali di cui al precedente articolo 8, il Responsabile della Convenzione potrà compensare il credito con quanto dovuto alla Società. La richiesta e/o il pagamento delle penali di cui al presente Convenzione non esonera in nessun caso la Società dall'adempimento dell'obbligazione per la quale il Responsabile della Convenzione ritiene si sia resa inadempiente e che ha fatto sorgere, a parere del Commissario, l'obbligo di pagamento della medesima penale.
4. Entro 30 (trenta) giorni lavorativi dal ricevimento di ciascuna fattura, il Commissario provvede ad effettuare il relativo mandato di pagamento. Il Commissario effettuerà i pagamenti, previa presentazione di fattura elettronica – codice IPA VLO40E sul conto corrente SOGEI dedicato, IBAN n. IT26J0623003205000040677976..
5. La Società, sotto la propria esclusiva responsabilità, si impegna a rendere tempestivamente note al Commissario eventuali variazioni relative alle coordinate bancarie di cui al precedente comma. In assenza di tali notificazioni, la Società esonera il Commissario da ogni responsabilità per i pagamenti eseguiti.

6. Resta inteso che la documentazione di riferimento sarà detenuta presso la sede della Società e tenuta a disposizione del Commissario per l'effettuazione di eventuali ulteriori controlli per tutto il periodo previsto dalla normativa vigente.

Art. 10

(Recesso)

1. Nell'ipotesi in cui l'assetto proprietario della Società si modifichi in misura tale da mutarne la natura di organismo di diritto pubblico ovvero nell'ipotesi della perdita della natura di società *in house*, alle Parti è riconosciuto il diritto di recedere dalla presente Convenzione con un preavviso scritto di un mese da inviarsi all'altra Parte a mezzo posta elettronica certificata
2. In caso di recesso anticipato, il Commissario si impegna a corrispondere alla Società l'importo dovuto per le spese sostenute fino a quel momento sulla base di apposita rendicontazione, secondo le modalità stabilite al precedente articolo 6, comma 1.

Art. 11

(Controversie)

1. Nel caso di controversie di qualsiasi natura che dovessero insorgere tra il Responsabile della Convenzione e la Società in ordine alla interpretazione od all'applicazione della presente Convenzione, o comunque direttamente od indirettamente connesse alla Convenzione, ciascuna parte comunicherà per iscritto all'altra l'oggetto ed i motivi della contestazione.
2. Al fine di comporre amichevolmente la controversia il Responsabile della Convenzione e la Società si impegnano ad esaminare congiuntamente la questione, entro il termine massimo di 5 (cinque) giorni dalla data di ricezione della contestazione, ed a pervenire ad una composizione entro il successivo termine di 5 (cinque) giorni.
3. In caso di esito negativo del tentativo di composizione di cui al precedente comma 2, la questione verrà rimessa al Foro di Roma territorialmente competente in via esclusiva.
4. Resta, peraltro, inteso che le controversie in atto non pregiudicheranno in alcun modo la regolare esecuzione delle attività della presente Convenzione, né consentiranno alcuna sospensione delle prestazioni dovute dall'una e dall'altra parte, fermo restando che riguardo alle questioni oggetto di controversia, le Parti si impegnano a concordare di volta in volta, in via provvisoria, le modalità di parziale esecuzione che meglio garantiscano il pubblico interesse ed il buon andamento dell'attività amministrativa.

Art. 12

(Sicurezza)

1. Attesa la specificità dei dati e delle informazioni trattate, la Società dovrà operare attraverso l'adozione di idonee misure organizzative, tecniche ed operative, per la protezione dei dati e delle informazioni gestite.
2. La Società con esclusivo riferimento ai servizi di propria competenza, si obbliga espressamente a manlevare e tenere indenne il Commissario da tutte le conseguenze derivanti dalla eventuale inosservanza delle norme e prescrizioni tecniche vigenti in materia di sicurezza.
3. Le Parti si danno atto che in relazione alla erogazione di servizi cloud, acquisiti dalla Società in nome proprio e per conto del Commissario in ottemperanza a quanto previsto al precedente articolo 4, troveranno applicazione i livelli di servizio e le misure di sicurezza adottate dal fornitore dei medesimi servizi rimanendo la Società esonerata da qualsiasi responsabilità in merito a tali attività.

Art. 13

(Tutela dei dati personali e della riservatezza)

1. Nell'esecuzione della presente Convenzione il Commissario e la Società potranno trovarsi nella condizione di dover trattare dati personali riferibili a dipendenti e/o collaboratori dell'altra parte.
2. Il Commissario e la Società si impegnano a condurre le suddette attività di trattamento di dati personali sulla base dei principi di correttezza, liceità, trasparenza e tutela della riservatezza dei soggetti interessati e per il solo ed esclusivo fine di perseguire le finalità di cui alla presente Convenzione, nonché degli eventuali obblighi di legge allo stesso connessi.

   I dati suindicati saranno trattati da ciascuna Parte limitatamente al periodo di tempo necessario al perseguimento delle finalità di cui sopra e saranno resi accessibili alle persone autorizzate che, in ragione della propria funzione e/o attività, abbiano la necessità di trattarli per le finalità suindicate.
3. La Società prende atto ed acconsente che, in adempimento agli obblighi di legge che impongono la trasparenza amministrativa, i dati e/o la documentazione che la legge impone di pubblicare siano pubblicati e diffusi tramite il sito internet del Commissario, nella sezione relativa alla trasparenza.
4. Per la fornitura dei Servizi di cui alla presente Convenzione, la Società tratterà, in qualità di responsabile del trattamento ai sensi dell'art. 28 del GDPR, dati personali per conto del Commissario.
5. A tal fine il Commissario attribuisce alla Società, con specifico documento di cui all'Allegato B della presente Convenzione, il ruolo e gli obblighi di cui all'art. 28 del Regolamento UE 2016/679.

Art. 14

(Modifiche alla presente Convenzione)

1. Qualunque modifica alla presente Convenzione dovrà essere concordata e approvata per iscritto tra le Parti.

Art. 15

(Comunicazioni)

1. Tutte le comunicazioni relative alla Convenzione dovranno essere formulate per iscritto ed inviate, a mezzo posta elettronica certificata, ai seguenti soggetti ed indirizzi:

   – Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto per l'emergenza epidemiologica COVID -19 e per l'esecuzione della campagna vaccinale nazionale: commissarioemergenzacovid19@pec.governo.it;

   – Sogei s.p.a.: protocollosogei@pec.sogei.it.

Art. 16

(Codice Etico)

1. 1. Le Parti dichiarano di conformarsi ai principi contenuti nel D. Lgs. 8 giugno 2001 n. 231 e nel D.P.R. 16 aprile 2013 n. 62 e, nell'attuazione della presente Convenzione, si impegnano reciprocamente ad improntare i rispettivi comportamenti a principi di trasparenza e correttezza ed alla più stretta osservanza del Decreto sopra citato, non ammettendo né intraprendendo alcuna forma di corruzione, e dichiarano, altresì, di non essere sino ad ora mai incorse nella commissione di uno dei reati nello stesso contemplati.
2. Le Parti convengono che l'inosservanza da parte di una di esse di una qualsiasi delle previsioni del citato D.P.R. configurerà un grave inadempimento degli obblighi di cui alla presente Convenzione e, conseguentemente, legittimerà l'altra Parte a risolvere lo stesso con effetto immediato, ai sensi e per gli effetti di cui all'art. 1456 Cod. Civ.

Art. 17

(Clausola Fiscale)

1. La presente Convenzione è soggetta ad imposta di bollo ai sensi della normativa vigente. I relativi oneri di registrazione e imposta di bollo, ove dovuti, sono a carico della Società.

Art. 18

(Esonero della cauzione)

1. Atteso che lo stato, mediante il Ministero dell'Economia e delle Finanze, detiene direttamente la partecipazione totalitaria nella Sogei, essa è esonerata dal prestare cauzione.

Art. 19

(Valore degli allegati)

2. La presente Convenzione si compone di n. 19 articoli e di n. 2 allegati che, sottoscritti dalle Parti, ne costituiscono parte integrante e sostanziale.
3. Alla presente Convenzione viene allegato:
   - Allegato A "Piano operativo";
   - Allegato B "Atto di attribuzione del ruolo e degli obblighi di cui all'art. 28 del Regolamento UE 2016/679"

Il Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto per l'emergenza epidemiologica COVID -19 e per l'esecuzione della campagna vaccinale nazionale

Gen. C.A. Francesco Paolo Figliuolo

(*f.to digitalmente*)

L'Amministratore delegato di Sogei S.p.A.

Dott. Andrea Quacivi

(*f.to digitalmente*)

ALLEGATO A - PIANO OPERATIVO

INDICE

1. PREMESSA

Il presente documento, denominato "Allegato A – Piano operativo", costituisce parte integrante e sostanziale della Convenzione tra il Commissario Straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto per l'emergenza epidemiologica COVID -19 e per l'esecuzione della campagna vaccinale nazionale, Gen. C.A. Francesco Paolo Figliuolo, nominato con DPCM 1°- 2021, (di seguito "Commissario") e la SOGEI - Società Generale d'Informatica S.p.A. (di seguito "Società")

In particolare la Società erogherà i servizi di seguito riportati:

- Acquisizione di sottoscrizioni Cloud - Microsoft Azure per ospitare i sistemi infologistici in uso alla struttura commissariale e software di collaboration;
- Assistenza per la migrazione dei sistemi infologistici a supporto della struttura commissariale per la gestione dell'Emergenza COVID dalla infostruttura insita nel Tenant attestato ad INVITALIA al Tenant appositamente realizzato per la Struttura Commissariale;
- Gestione di un First Line Support (FLS) funzionante 24x7x365 comprensivo di capacità di intervento di primo livello;
- Gestione di un Security Operation Center per gli aspetti di integrità, disponibilità e riservatezza dei sistemi gestiti;
- Assistenza tecnica di tipo correttivo, adattativo ed evolutivo sui sistemi infologistici gestiti;
- Consulenza specialistica per gli aspetti di privacy legati all'utilizzo dei sistemi;

Alcune di queste attività sono di natura "una tantum", altre saranno erogate a corpo, e soggette al pagamento di un canone mensile, altre ancora saranno quantificate in fase esecutiva in quanto erogate "a consumo". Resta inteso che le attività relative a sviluppi di nuovi applicativi, non sono comprese e, se necessarie, verranno disciplinate in specifici addendum alla presente convenzione.

L'analisi oggetto del presente documento è stata redatta utilizzando i servizi, i relativi corrispettivi ed i livelli di servizio, così come congruiti con parere AGID 12/2020 reso ai sensi dell'Articolo 14 bis, comma 2, lettera f) del Decreto Legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale, rilasciato in relazione al Disciplinare fra il Dipartimento della Ragioneria generale dello Stato del Ministero dell'Economia e delle Finanze e la SOGEI. Per quanto attiene acquisizioni di beni e servizi, si è fatto ricorso a contratti già in essere, o da

concludere, da parte di Consip s.p.a., nella sua qualità di centrale di committenza di Sogei s.p.a, ai sensi dell'art. 4 comma 3-ter del D.L. n. 95 del 6 luglio 2012, il cui dettaglio è riportato in Suballegato 1.

Per quanto attiene la fase esecutiva, oltre alla figura di cui all'art. 7 della Convenzione, il Commissario straordinario nominerà un Direttore dell'Esecuzione contrattuale (di seguito DEC), in qualità di principale riferimento per la Società.

1.1. SISTEMI INFOLOGISTICI

Di seguito sono riportati i sistemi infologistici in uso alla Struttura Commissariale a cui ci si riferirà nel seguito del documento:

Sistema	**Descrizione sintetica**
Monitoraggio Somministrazione Vaccini	Il sistema raccoglie, organizza e pubblica le informazioni relative alle somministrazioni vaccinali e dosi consegnate alle regioni. Gli Output sono sia sul sito governativo che sulle dashboard della cabina di regia.
Analisi Distribuzione Aiuti	Il sistema effettua la raccolta dei fabbisogni delle regioni e gestisce la comunicazione relativa agli "aiuti" resi disponibili. È un ausilio alla pianificazione degli aiuti stessi, e fornisce la certificazione, da parte delle regioni degli aiuti ricevuti.
Logistica Vaccini	Il sistema completa, con informazioni legate alla Logistica distributiva dei vaccini Moderna ed Astrazeneca, la piattaforma gestita da Poste per la gestione puntuale delle somministrazioni dei vaccini, nelle regioni che hanno adottato il sistema, e dell'hub di Pratica di Mare, per lo smistamento delle dosi.
Personale Vaccini	Il sistema gestisce il reclutamento del personale Sanitario (Medico ed infermieristico) a cura della struttura commissariale al fine di renderlo disponibile alle regioni che ne fanno richiesta.
Rete Ospedaliera	Il sistema gestisce le informazioni relative al potenziamento della rete ospedaliera sul territorio nazionale per far fronte all'emergenza pandemica.

Delivery to Pay	Il sistema supporta le fasi esecutive dei contratti stipulati dalla Struttura Commissariale per le forniture di materiale distribuito direttamente "a domicilio" dei beneficiari (scuole, enti,etc.).
Dyn for Finance	Il sistema gestisce le procedure di affidamento degli appalti e la logistica degli approvvigionamenti.

2. SERVIZI A SUPPORTO DELLA STRUTTURA COMMISSARIALE

In questa sezione sono descritte le attività ed i servizi erogati da SOGEI per il supporto della Struttura Commissariale per l'Emergenza COVID19.

2.1SOTTOSCRIZIONI CLOUD - MICROSOFT AZURE E SOFTWARE DI COLLABORATION

La tecnologia utilizzata dall'attuale soluzione si basa su Cloud Azure mentre le applicazioni per la logica a basso contenuto di codice e le automazioni dei flussi e analisi dei dati, sono realizzate con tecnologia Microsoft O365, Sharepoint online e PowerPlatform. Questa situazione, unitamente all'urgenza e alle esigenze di continuità dei servizi, richiede l'acquisizione di specifici prodotti.

A questi prodotti si aggiunge la necessità della sottoscrizione di un prodotto per il *backup* completo dei dati di Office 365 (es Sharepoint).

Descrizione	**Costo Stimato**	**Dettagli**
Fornitura di sottoscrizione di servizi Cloud per ospitare i sistemi infologistici a supporto della struttura commissariale.	25.299,00€/mese (stimato)	saranno forniti i servizi di: - Sottoscrizione Azure I servizi sono a consumo, la stima è quindi indicativa essendo il contratto definito in modalità "pay-as-you-go" La durata minima del servizio è pari a 12 mesi dettaglio dei costi e delle tariffe in Suballegato 1
Fornitura di sottoscrizione di servizi Cloud per ospitare i sistemi infologistici a supporto della struttura commissariale. Componente Dynamics PowerBI, PowerAPPS.	31.296,13 €/mese	In particolare saranno forniti: - piattaforme Dynamics Finance and operation - PowerBI&PowerAPPS Il costo potrebbe essere soggetto a variazione qualora si superasse la

		quota di spazio oggi previsto se dovessero aumentare le utenze o li istanze definite. La durata minima del servizio è pari a 12 mesi [1] dettaglio dei costi e delle tariffe in Suballegato 1
Prodotti di Collaboration	4.926/mese	In particolare saranno fornite: n. 200 licenze di Microsoft Office 365 La durata minima del servizio è pari a 26 mesi
Prodotti di backup	2.840/anno	In particolare sarà fornita: n. 1 licenza VEEAM Backup for Microsoft Office 365 La durata minima del servizio è un anno.

Note per la fatturazione.

Saranno utilizzati i seguenti Contratti:

- Contratto CSQT210090 Fornitore Telecom Italia S.p.A. - Ai fini del pagamento del corrispettivo contrattuale l'Impresa potrà emettere fattura in rate trimestrali posticipate, successivamente alla relativa "Data di accettazione del servizio".
- Contratto CSQG200192 Fornitore Telecom Italia S.p.A. - per tutte le altre componenti (per subscription, licenze e relativa SA) a decorrere "Data di accettazione della fornitura";
- Il Contratto CREM200217 Fornitore Novanext S.r.l., prevede che il fornitore potrà emettere fattura per l'intero importo entro 30 giorni dalla fornitura delle subscription.- Da verificare se i prodotti da acquistare sono previsti nel contratto, altrimenti nuovo affidamento.

Gli importi delle fatture dei Fornitori saranno presentati alla struttura del Commissario in concomitanza con l'invio dei rapporti periodici previsti dalla Convenzione. La fattura sarà emessa all'approvazione del rapporto periodico.

2.2 ASSISTENZA PER LA MIGRAZIONE DEI SISTEMI INFOLOGISTICI

L'assistenza afferisce alle attività da porre in essere al fine di spostare tutti i sistemi (architetture, applicativi, database, dati, servizi e connessioni) garantendo la disponibilità senza soluzione di continuità di tutti i servizi erogati dalla infrastruttura informatica della precedente struttura commissariale. Dovranno altresì essere rese fruibili, nella nuova infrastruttura, le piattaforme di sviluppo, test e controllo di configurazione per ognuno dei sistemi in produzione.

Descrizione	**Costo**	**Dettagli**
Assistenza specialistica per la migrazione dei sistemi infologistici.	195.438 € (una tantum) di cui: – 151.680 relativo a prestazioni di tecnici SOGEI – 43.758 relativo a prestazioni di tecnici AGIC TECH	n. 60 giorni/uomo di servizio coordinamento (€ 800/g) n. 120 giorni/uomo di servizio specialistico (€ 502/g) n. 120 giorni/uomo di servizio operativo (€ 362/g) giornate di supporto specialistico AGICTECH in ambito Dynamics-dettaglio dei costi e delle tariffe in Suballegato 1.
Supporto Microsoft alla migrazione dal tenant - Architect Microsoft Azure	214.656 € (a corpo)	assistenza per la realizzazione e la configurazione degli ambienti.

Gli importi relative alle Società esterne rappresentano un massimale i cui dettagli saranno consolidati successivamente e approvati dal DEC.

Note per la fatturazione.

All'atto del primo Rapporto periodico sarà fornito il consuntivo delle attività; la fattura sarà emessa all'approvazione del rapporto periodico.

Le attività saranno concluse entro il 12 maggio; al rispetto di tale scadenza si applica il seguente livello di servizio:

Livelli di Servizio	Soglia	Penale
Mantenimento data di consegna		€ 250,00 per ogni giorno di ritardo successivo al decimo e sino al trentesimo giorno

	10 giorni dalla data di consegna	€ 500,00 per ogni giorno di ritardo successivo al trentesimo e sino al sessantesimo giorno
		€ 750,00 per ogni giorno di ritardo successivo al sessantesimo

2.3 FIRST LINE SUPPORT (FLS)

La Società, dovrà predisporre un FLS attivo 24 ore al giorno, 7 giorni su 7, 365 giorni l'anno che concorrerà alla gestione dei sistemi e fungerà da punto di assistenza per l'utenza.

In particolare il FLS dovrà:

- occuparsi della conduzione delle risorse Cloud e collaboration a servizio della Struttura Commissariale;
- monitorare costantemente il funzionamento dei sistemi e segnalare, registrare e risolvere eventuali anomalie/disservizi;
- gestire allarmi e attivazioni;
- effettuare aggiornamenti e manutenzioni programmate ove previsto;
- effettuare operazioni di accounting e configurazione utente;
- fornire assistenza e supporto all'utenza per ogni problematica di natura tecnica sui sistemi gestiti;
- effettuare interventi di primo livello di manutenzione.

Tale servizio dovrà essere svolto attraverso meccanismi che ne favoriscano la fruizione da parte dell'utenza, in particolare:

- Ticket System;
- Casella E-mail;
- Numero di telefono dedicato.

Per ogni richiesta, il personale del supporto dovrà soddisfare, ove possibile, la richiesta con interventi di primo livello. Qualora si ravvisi che una richiesta non afferisca a questioni di natura tecnica, la stessa dovrà essere inoltrata all'Area Operativa competente della Struttura Commissariale, su indicazione del DEC.

Laddove si riscontrassero anomalie di funzionamento particolarmente complesse, di concerto con il DEC sarà compilata un'apposita scheda lavoro.

In particolare, il servizio reso dal personale del centro di supporto dovrà:

- assicurare una comunicazione efficace con l'utenza con metodi sincroni (telefono) e asincroni (e-mail);
- provvedere all'accoglimento ed alla ordinata registrazione delle richieste di intervento;
- risolvere con immediatezza i problemi più ricorrenti e di complessità non elevata;

Periodicamente, il DEC ed il Referente della Società devono congiuntamente:

- controllare i processi di risoluzione attivati e verificarne gli esiti;
- verificare il rendiconto dello stato degli interventi;

Inoltre, dovrà essere reso disponibile un sistema di ticketing attraverso cui si possano tracciare tutte le attività dall'apertura di un ticket alla sua risoluzione.

In fine, dovrà essere esteso ad interventi di secondo livello, il servizio di assistenza per i seguenti sistemi critici (sistemi il cui mancato funzionamento, anche per qualche ora, potrebbe arrecare danni alla gestione della Struttura Commissariale):

- Monitoraggio Somministrazione Vaccini;
- Analisi Distribuzione Aiuti;
- Logistica Vaccini.

Descrizione	**Costo**	**Dettagli**
Servizio di First Line Support Esteso	134.416,00 €/mese così composti: - 82.882,00 €/mese per I livello - 51.534,00 €/mese per II livello su tutto lo stack tecnologico e di sicurezza e 3 servizi	In particolare saranno forniti: - Servizio di assistenza 24x7x365; - Interventi di I° Livello; - Interventi di II° Livello su tutto lo stack tecnologico e sui sistemi critici 5x8 - Ticket System. Possono rientrare in questo ambito, per il primo mese di servizio, quota parte delle attività di migrazione di cui al paragrafo 2.2 Nel suballegato 1 è riportato il dettaglio della composizione dei costi La durata minima del servizio è pari a 12 mesi (il servizio potrà comunque terminare prima del previsto purché con un preavviso di almeno 3 mesi)

Note per la fatturazione

Contratto CREG200297 Fornitore RTI Engineering D.HUB S.p.A, Accenture S.p.A., Engineering Ingegneria Informatica S.p.A., Accenture Technology Solutions S.r.l , Cybertech S.r.l, EY Advisory

S.p.A. - con riferimento ai servizi remunerati a canone, l'Impresa potrà emettere fattura al termine del trimestre di riferimento, a decorrere dalla relativa "Data di accettazione del servizio"

Gli importi delle fatture dei Fornitori saranno presentati alla struttura del Commissario in concomitanza con l'invio dei rapporti periodici previsti dalla Convenzione. La fattura sarà emessa all'approvazione del rapporto periodico.

2.4 GESTIONE DI UN SECURITY OPERATION CENTER (SOC)

La società dovrà provvedere a strutturare un SOC con la funzione di salvaguardare la sicurezza dei sistemi (architetture, applicativi e dati) in termini di disponibilità, integrità e riservatezza.

In particolare Sogei erogherà il servizio SIEM per la raccolta ed analisi dei LOG, mentre il fornitore di II livello erogherà un servizio di gestione e monitoraggio h24 7x7 delle console di sicurezza azure in stretto contatto con la struttura SOC Sogei. La medesima struttura gestirà le componenti di sicurezza (es. Firewall e relative regole e controllo) dell'infrastruttura

Descrizione	**Costo**	**Dettagli**
Security Operation Center	19.010 €/mese x monitoraggio sicurezza tenant	In particolare saranno forniti: - Servizi di monitoraggio h24 7x7 delle console di sicurezza su Azure in stretto contatto con il SOC Sogei che accoglierà nella propria SIEM i log; - Gestione della sicurezza dell'infrastruttura 5x8 + 24h reperibilità Nel suballegato 1 sono riportati i dettagli della composizione dei costi La durata minima del servizio è pari a 12 mesi (il servizio potrà comunque terminare prima del previsto purché con un preavviso di almeno 3 mesi)

Note per la fatturazione:

Saranno utilizzati i seguenti Contratti:

- Contratto CREG200297 Fornitore RTI Engineering D.HUB S.p.A, Accenture S.p.A., Engineering Ingegneria Informatica S.p.A., Accenture Technology Solutions S.r.l , Cybertech S.r.l, EY Advisory S.p.A. - con riferimento ai servizi remunerati a canone, l'Impresa potrà emettere fattura al termine del trimestre di riferimento, a decorrere dalla relativa "Data di accettazione del servizio"

Gli importi delle fatture dei Fornitori saranno presentati alla struttura del Commissario in concomitanza con l'invio dei rapporti periodici previsti dalla Convenzione. La fattura sarà emessa all'approvazione del rapporto periodico.

2.5 ASSISTENZA TECNICA DI TIPO CORRETTIVO, ADATTATIVO ED EVOLUTIVO

Le prestazioni di cui al presente paragrafo riguardano l'attuazione della manutenzione correttiva di secondo livello ed evolutiva dei sistemi infologistici; l'ampliamento delle loro funzionalità applicative e la realizzazione di manualistica procedurale a supporto della Struttura Commissariale.

Ogni singola attività potrà essere commissionata alla Società mediante una "scheda lavoro" (vedi Appendice) in cui saranno esplicitati:

- Una descrizione sintetica dell'attività;
- Il requisito tecnico preliminare;
- Un'analisi schematica dell'attività da svolgere;
- Le risorse da impiegare;
- I tempi di prevista consegna.

Al termine di ogni lavorazione saranno conteggiate, a consuntivo, le ore/giornate effettivamente impiegate che comunque non potranno mai superare le ore congruite a meno di varianti approvate dal Direttore dell'Esecuzione Contrattuale.

La Ditta, all'atto del completamento di ogni singola attività, dovrà rilasciare gli aggiornamenti della documentazione tecnica ed operativa.

Per quanto concerne le modalità di sviluppo (luogo delle lavorazioni, piattaforme, strumenti di sviluppo, etc.) test e consegna, le attività saranno concertate fra il DEC e il referente della ditta.

La verifica di buona esecuzione di ciascuna attività deve avvenire attraverso un piano di test appositamente predisposto dalla Ditta ed approvato dal DEC, che deve accertare la:

- rispondenza al Requisito Utente del prodotto fornito;
- completezza ed efficacia della documentazione prodotta.

La verifica si ritiene andata a buon fine dopo che il SW installato nell'ambiente di esercizio

Per quanto concerne i costi giornalieri di ciascuna figura professionale, utilizzabile nell'ambito della convenzione, ci si riferirà alla tabella riportata nel Suballegato 1.

Mensilmente il DEC redigerà un rapporto consuntivo relativo alle schede lavoro concluse con esito positivo e calcolerà i relativi costi totali "a consumo" che potranno essere imputati alla Struttura Commissariale.

Mensilmente il DEC redigerà un rapporto consuntivo relativo alle schede lavoro concluse con esito positivo e calcolerà i relativi costi totali "a consumo" che potranno essere imputati alla Struttura Commissariale.

Note per la fatturazione:

Saranno utilizzati i seguenti Contratti:

– Contratto CREG200297 Fornitore RTI Engineering D.HUB S.p.A, Accenture S.p.A., Engineering Ingegneria Informatica S.p.A., Accenture Technology Solutions S.r.l , Cybertech S.r.l, EY Advisory S.p.A. - con riferimento ai servizi remunerati in gg/persona a consumo, l'Impresa potrà emettere fattura al termine del trimestre di riferimento sulla base del numero di giorni/persona, a decorrere dalla relativa "Data di accettazione del servizio"

Gli importi delle fatture dei Fornitori saranno presentati alla struttura del Commissario in concomitanza con l'invio dei rapporti periodici previsti dalla Convenzione. La fattura sarà emessa all'approvazione del rapporto periodico.

2.6 CONSULENZA SPECIALISTICA PER GLI ASPETTI DI PRIVACY

Si prevedono attività di supporto sulla privacy da effettuare congiuntamente alle strutture preposte della gestione Commissariale al fine di:

- supportare il titolare nello svolgimento degli adempimenti di propria competenza;

- verificare l'adeguatezza delle misure di sicurezza implementate sulla piattaforma in ottica "privacy by design" (Art.32 GDPR).

Le consulenze potranno essere richieste dal Data Protection Officer (DPO), per il tramite del DEC, attraverso apposita scheda lavoro ed impegneranno figure professionali specializzate messe a disposizione dalla Società.

Per quanto concerne i costi di ciascuna figura professionale, utilizzabile nell'ambito della convenzione ci si riferirà alla tabella sottostante.

Servizio Professional	Corrispettivo Unitario (giornaliero)
Servizio di Coordinamento	€ 800/g
Servizio Specialistico	€ 502/g
Servizio operativo	€ 362/g

Mensilmente il DEC redigerà un rapporto consuntivo relativo alle schede lavoro concluse con esito positivo, e calcolerà i relativi costi totali "a consumo" che potranno essere imputati alla Struttura Commissariale.

Note per la fatturazione:

Le attività saranno erogate da personale della Società.

All'atto del Rapporto periodico sarà fornito il consuntivo delle attività; la fattura sarà emessa all'approvazione del rapporto periodico.

2.7 PROGRAM MANAGEMENT

Alla Società è riconosciuto un onere relativo all'attività di program management che, su richiesta del DEC, fornirà supporto al Committente per:

- Gestione rapporto con i fornitori;
- Riunioni quotidiane di SAL e periodiche di rendicontazione;
- Assistenza a personale Difesa sull'utilizzo delle applicazioni menzionate;
- Valutazione di bugs e migliorie da apportare alle applicazioni;
- Revisione manualistica associata alle applicazioni;

- Coordinamento e supporto al passaggio di consegne ai nuovi fornitori;
- Organizzazione sessioni formative verso Difesa con i fornitori;
- Gestione di interventi di manutenzione evolutiva di estrema urgenza con tempi rapidissimi di esecuzione e messa in produzione;
- configurazione dell'infrastruttura
- abilitazioni degli utenti della stessa Struttura Commissariale all'utilizzo delle diverse funzionalità;
- governo della gestione del servizio e delle tecnologie. Opereranno in stretto contatto con il DEC e con i fornitori dei servizi di I e II livello esercitando il controllo sull'esecuzione dei task assegnati;
- analisi SOC degli eventi raccolti nella SIEM Sogei, in stretta correlazione con i fornitori che erogano il servizio di monitoraggio h24 7x7 sulle console di sicurezza e gestione delle componenti di sicurezza del tenant azure

Per quanto concerne i costi orari di ciascuna figura professionale, utilizzabile nell'ambito della convenzione ci si riferirà alla tabella sottostante.

Servizio Professional	Corrispettivo Unitario (giornaliero)
Servizio di Coordinamento	€ 800/g
Servizio Specialistico	€ 502/g
Servizio operativo	€ 362/g

Note per la fatturazione:

Le attività saranno erogate da personale della Società.

All'atto del Rapporto periodico sarà fornito il consuntivo delle attività; la fattura sarà emessa all'approvazione del rapporto periodico.

3 Riepilogo generale

Si riportano nella tabella sottostante gli importi previsti per i beni e servizi raggruppati per tipologia di costo:

	Corrispettivo una tantum	Corrispettivo Mensile	Corrispettivo 1 Anno	Corrispettivo 2 Anno	Corrispettivo Totale
Una Tantum					
Assistenza specialistica per la migrazione dei sistemi infologistici.	195.438,00		200.680,00		200.680,00
Supporto Microsoft alla migrazione dal tenant - Architect Microsoft Azure	214.656,00		214.656,00		214.656,00
A Canone					
Fornitura di sottoscrizione di servizi Cloud per ospitare i sistemi infologistici a supporto della struttura commissariale.		31.296,13	375.553,56	375.553,56	751.107,12
Prodotti di Collaboration		4.926,00	59.112,00	68.964,00	128.076,00
Prodotti di backup			2.840,00	2.840,00	5.680,00
Servizio di First Line Support		134.416,00	1.612.992,00	1.612.992,00	3.225.984,00
Security Operation Center		19.010	228.120,00	228.120	456.240,00
A Consumo		Stima mensile			Stima annuale
Fornitura di sottoscrizione di servizi Cloud per ospitare i sistemi infologistici a supporto della struttura commissariale.		25.299,00	303.588,00	303.588,00	607.176,00
Assistenza tecnica di tipo correttivo, adattativo ed evolutivo (basket)			407.324,60	407.324,60	814.649,20
Consulenza specialistica per gli aspetti di privacy (basket)		3.514	42.168,00	42.168,00	84.336,00
Program Management (basket)		20.080	240.960,00	240.960,00	481.920,00
Totale	**410.094,00**	**238.541,13**	**3.682.752,16**	**3.282.510,16**	**6.965.262,32**

Totale in 2 anni: **6.965.262,32** (al netto dell'IVA)

APPENDICE 1

Scheda di Lavoro

PRESIDENZA DEL CONSIGLIO DEI MINISTRI ***STRUTTURA DI SUPPORTO AL COMMISSARIO STRAORDINARIO ALL'EMERGENZA EPIDEMIOLOGICA COVID-19***	Scheda lavoro n°…..in data …… Sottosistema……...…..
ATTIVITA' DA SVOLGERE E INDICAZIONE DEI TERMINI DI CONSEGNA **(descrizione generica a cura del Direttore dell'Esecuzione Contrattuale)**	
REQUISITO TECNICO PRELIMINARE **(a cura del Direttore dell'Esecuzione Contrattuale)**	
DOCUMENTO PRELIMINARE DI ANALISI (**Esame congiunto Ditta - Direttore dell'Esecuzione Contrattuale**)	
FIGURE PROFESSIONALI DA IMPIEGARE (***Stima Oraria da parte Ditta)*** **- Servizio di Coordinamento** **nr ……** **- Servizio Specialistico** **nr ……** **- Servizio Operativo** **nr ……** **Totale Giornate** **Totale Ore**	
VALUTAZIONE TECNICO-ECONOMICA (**congruitàa cura del Direttore dell'Esecuzione Contrattuale**) **- Servizio di Coordinamento** **nr ……** **- Servizio Specialistico** **nr ……** **- Servizio Operativo** **nr ……** **Totale Giornate** **Totale Ore**	
DATA ASSEGNAZIONE LAVORI:	
DATA DI FINE LAVORI :	
per accettazione **DIRETTORE ESECUZIONE CONTRATTUALE:** **REFERENTE SOCIETA':**	

SUBALLEGATO 1 AD ALLEGATO A - Riepilogo generale acquisizioni beni e servizi a rimborso e dettaglio per definizione importi

1. RIEPILOGO GENERALE ACQUISIZIONI BENI E SERVIZI A RIMBORSO

Si riportano nella tabella sottostante gli importi previsti per i beni e servizi a rimborso, raggruppati per tipologia:

Tipologia Bene/ Servizio	**Corrispettivo Annuale/1° anno**	**Corrispettivo Annuale/2° anno**	**Importo totale (a rimborso)**	**Contratto Sogei (Repertorio e Oggetto)**	**Stazione appaltante contratto e tipologia di procedura di affidamento eseguita**	**Fornitore aggiudicatario (singolo o in RTI)**	**Società esecutrice attività/servizio/fornitura**
Sottoscrizioni Cloud per ospitare i sistemi infologistici	**€ 679.141,56**	**€ 679.141,56**	**€ 1.358.283,12**	CSQT210090 *Porting degli applicativi per la gestione della pandemia da Invitalia a Sogei*	Consip previa Procedura negoziata d'urgenza	Telecom Italia S.p.A.	Telecom Italia S.p.A.
Prodotti di Collaboration	**€ 59.112**	**€ 68.964**	**€ 128.076**	CSQG200192 *Acquisto di licenze d'uso e rinnovo della manutenzione dei prodotti software Microsoft per Sogei Spa*	Consip previa Gara a procedura aperta	Telecom Italia S.p.A.	Telecom Italia S.p.A.
Prodotti di backup	**€ 2.840**	**€ 2.840**	**€ 5.680**	Da definire In valutazione se Aderire al Contratto Quadro Consip SPC Cloud lotto 2 oppure 6/5 sul contratto CREM200217 per supporto software Veeam	Nel caso di utilizzo del contratto CREM200217 Consip -Procedura negoziata su MEPA	Novanext s.r.l.	Novanext s.r.l.
Servizi di Gestione	*Importo come da allegato A – piano operativo*	*Importo come da allegato A – piano operativo*	*Importo come da allegato A – piano operativo*	CREG200297 *Servizi di conduzione e supporto specialistico per l'infrastruttura ICT* (GSM lotto 1)	Consip previa Gara a procedura aperta SOGEI provvederà all'autorizzazione al subappalto	RTI Engineering D.HUB S.p.A, Accenture S.p.A., Engineering Ingegneria Informatica S.p.A., Accenture Technology	Subapplato di Engineering in favore di Engage

Tipologia Bene/ Servizio	Corrispettivo Annuale/1° anno	Corrispettivo Annuale/2° anno	Importo totale (a rimborso)	Contratto Sogei (Repertorio e Oggetto)	Stazione appaltante contratto e tipologia di procedura di affidamento eseguita	Fornitore aggiudicatario (singolo o in RTI)	Società esecutrice attività/servizio/fornitura
						Solutions S.r.l , Cybertech S.r.l, EY Advisory S.p.A.	
Ambito Dynamics	*Importo come da allegato A – piano operativo*	*Importo come da allegato A – piano operativo*	*Importo come da allegato A – piano operativo*	NRXD200405 - Contratto Quadro Consip SPC Cloud Lotto 2 Sicurezza + altra adesione da operare	Consip previa Gara a procedura aperta Sogei provvederà all'adesione al Contratto Quadro	RTI Leonardo/Sistemi Informativi Srl/IBM/Fastweb	Subappalto di Leonardo o Sistemi informativi in favore di AGIC Technology
Piattaforme Azure - servizi First line support	*€ 1.612.992*	*€ 1.612.992*	*€ 3.225.984*	CREG200297 *Servizi di conduzione e supporto specialistico per l'infrastruttura ICT* (GSM lotto 1)	Consip previa Gara a procedura aperta SOGEI provvederà all'autorizzazione al subappalto	RTI Engineering D.HUB S.p.A, Accenture S.p.A., Engineering Ingegneria Informatica S.p.A., Accenture Technology Solutions S.r.l , Cybertech S.r.l, EY Advisory S.p.A.	Subappalto di Engineering in favore di Engage
Gestione console di sicurezza Cloud Azure (SOC)	*€ 228.120*	*€ 228.120*	*€ 456.240*	CREG200297 *Servizi di conduzione e supporto specialistico per l'infrastruttura ICT* (GSM lotto 1)	Consip previa Gara a procedura aperta SOGEI provvederà all'autorizzazione al subappalto	RTI Engineering D.HUB S.p.A, Accenture S.p.A., Engineering Ingegneria Informatica S.p.A., Accenture Technology Solutions S.r.l , Cybertech S.r.l, EY Advisory S.p.A.	Subappalto di Engineering in favore di Engage

Tipologia Bene/ Servizio	**Corrispettivo Annuale/1° anno**	**Corrispettivo Annuale/2° anno**	**Importo totale (a rimborso)**	**Contratto Sogei (Repertorio e Oggetto)**	**Stazione appaltante contratto e tipologia di procedura di affidamento eseguita**	**Fornitore aggiudicatario (singolo o in RTI)**	**Società esecutrice attività/servizio/fornitura**
Servizi di Consulenza	*Importo come da allegato A – piano operativo*	*Importo come da allegato A – piano operativo*	*Importo come da allegato A – piano operativo*	CSQT200138 Rinnovo Servizi Premier e DAS CREG200297 per *Servizi di conduzione e supporto specialistico per l'infrastruttura ICT* (GSM lotto 1)	CSQT200138 Consip previa procedura negoziata diretta con Microsoft CREG200297 Consip previa Gara a procedura aperta SOGEI provvederà all'autorizzazione al subappalto	RTI Engineering D.HUB S.p.A, Accenture S.p.A., Engineering Ingegneria Informatica S.p.A., Accenture Technology Solutions S.r.l , Cybertech S.r.l, EY Advisory S.p.A.	Subappalto di Engineering in favore di Microsoft e altri operatori da definire
Supporto Microsoft alla migrazione dal tenant - Architect Microsoft Azure	**214.656**		**214.656**	CREG200297 per *Servizi di conduzione e supporto specialistico per l'infrastruttura ICT del MEF* (GSM lotto 1)	Consip previa Gara a procedura aperta SOGEI provvederà all'autorizzazione al subappalto	RTI Engineering D.HUB S.p.A, Accenture S.p.A., Engineering Ingegneria Informatica S.p.A., Accenture Technology Solutions S.r.l , Cybertech S.r.l, EY Advisory S.p.A.	Subappalto di Engineering in favore di Microsoft

2. SERVIZI

2.1 SOTTOSCRIZIONI CLOUD - MICROSOFT AZURE E SOFTWARE DI COLLABORATION (CSQT210090)

DETTAGLIO COSTI CLOUD SOFTWARE MICROSOFT

Voce	costo scontato/mese	costo scontato/anno	qtà	totale/anno	% sconto vs listino	SKU	COSTO MESE
Servizi SaaS (canone)							
Dyn365ECstmrSrvc ShrdSvr ALNG SubsVL MVL PerUsr/DDW-00003 - Canone mensile offerto (€)	69,90 €	838,80 €	20	16.776,00 €	0,851%	DDW-00003	**31.296,13 €**
Dyn365EUnfOpsAddDBCpcty ShrdSvr ALNG SubsVL MVL AddOn/PTU-00002 - Canone mensile offerto (€)	29,43 €	353,16 €	100	35.316,00 €	0,842%	PTU-00002	
Dyn365EOpsSandboxTier2 ShrdSvr ALNG SubsVL MVL Srvcs StdAccptTest/DMR-00001 - Canone mensile offerto (€)	995,83 €	11.949,96 €	3	35.849,88 €	0,600%	DMR-00001	
PowerAppsPrtlPgvwCpcty ALNG SubsVL MVL 100Kexternalpageviews AddOn/SE5-00001 - Canone mensile offerto (€)	73,76 €	885,12 €	2	1.770,24 €	0,606%	SE5-00001	
PowerAutomateplan ShrdSvr ALNG SubsVL MVL PerUsr/SPU-00002 - Canone mensile offerto (€)	11,04 €	132,48 €	200	26.496,00 €	0,809%	SPU-00002	
PwrBIPremP2 ShrdSvr ALNG SubsVL MVL/GSN-00002 - Canone mensile offerto (€)	7.618,12 €	91.417,44 €	1	91.417,44 €	0,600%	GSN-00002	
Dyn365ESpplyChnMgmnt ShrdSvr ALNG SubsVL MVL PerUsr/S2R-00001 - Canone mensile offerto (€)	132,44 €	1.589,28 €	50	79.464,00 €	0,853%	S2R-00001	

Dyn365EFinanceAttach ShrdSvr ALNG SubsVL MVL toQlfygDyn365BaseSKUPerUsr/SAJ-00001 - Canone mensile offerto (€)	22,07 €	264,84 €	50	13.242,00 €	0,854%	SAJ-00001	
PwrBIPro ShrdSvr ALNG SubsVL MVL PerUsr/NK4-00002 - Canone mensile offerto (€)	7,65 €	91,80 €	50	4.590,00 €	0,649%	NK4-00002	
PowerAppsPlan ShrdSvr ALNG SubsVL MVL PerUsr/SEJ-00002 -	29,43 €	353,16 €	200	70.632,00 €	0,842%	SEJ-00002	
Servizi Azure (consumo)							
Azure/6QK-00001 - Canone mensile offerto (€)	84,33 €	1.011,96 €	300	303.588,00 €	0,000%	NA	**25.299,00 €**
Totale 12 mesi				679.141,56 €			
Totale 24 mesi				1.358.283,12 €			

2.2 ASSISTENZA PER LA MIGRAZIONE DEI SISTEMI INFOLOGISTICI

Contratto: CREG200297

Contesto	Profilo	Attività in orario di servizio (8 ore comprese fra le 08.00 e le 18.00)	Interventi fuori orario di servizio standard (tariffa oraria)
Consulente .Net	Consulente di integrazione applicativa	€ 360,00/g	€ 58,50/h
Team Leader	Consulente processi	€ 470,00/g	€ 76,38/h
Consulente CRM	Consulente specialista di prodotto	€ 344,00/g	€ 55,90/h
Consulente Power BI	Consulente specialista di prodotto	€ 344,00	€ 55,90/h
Consulente Azure	Consulente di evoluzione tecnologica	€ 360,00	€ 58,50
Consulente O365	Consulente di evoluzione tecnologica	€ 360,00	€ 58,50
Consulente Security	Consulente di evoluzione tecnologica	€ 360,00	€ 58,50

Figura professionale	Tariffa giornaliera
Capo progetto	€ 300,00
Security Architect	€ 372,90
Specialista di tecnologia/prodotto Senior	€ 295,00
Specialista di tecnologia/prodotto	€ 235,00
Specialista di tecnologia/prodotto Senior (H24)	€ 1.180,00
Specialista di tecnologia/prodotto (H24)	€ 930,00

2.3 FIRST LINE SUPPORT (FLS)

DETTAGLIO COSTITUZIONE CANONI FLS (CREG200297)

Competenza	Profilo	Tariffa std	Tariffa extra	gg std	gg in reperibilità	Canone mensile Std	Canone mensile reperibilità	Totali
20+ anni exp. Erogazione servizi, automazione, DBA	Consulente processi	470,00	564,00	21		9870	0	82.882,00
20+ anni exp. Gestione ambienti di esercizio	Consulente di evoluzione tecnologica	360,00	432,00	21		7560	0	
Sys Admin, 20+ anni di exp in Help Desk 1° e 2° livello	Consulente di evoluzione tecnologica	360,00	432,80	21	5	7560	2164	
10+ anni exp in Help Desk 1° Livello (Telecom, TSF, ACEA, Gemelli, ecc)	Consulente specialista di prodotto	344,00	412,80	21	5	7224	2064	

Control Room Leader, Help Desk 1° e 2° Livello	Consulente specialista di prodotto	344,00	412,80	21	5	7224	2064	
Sys Admin, Microsoft & Linux administrator, Help Desk & SOC Operator	Consulente specialista di prodotto	344,00	412,80	21	5	7224	2064	
Microsoft Cerified, HD & SOC Operator in RAI	Consulente specialista di prodotto	344,00	412,80	21	5	7224	2064	
Technical expert, O365, Azure & Sharepoint experience, Jr. Developer	Consulente specialista di prodotto	344,00	412,80	21	5	7224	2064	
Help Desk, Tester, Sys Admin, Developer	Consulente specialista di prodotto	344,00	412,80	21	5	7224	2064	
20+ Anni exp. Erogazione servizi, Data Management, DBA, Azure, Microsoft 365 Expert	Consulente processi	470,00	564,00	21	3	9870	1692	51.534,00
Power BI expert	Consulente di evoluzione tecnologica	360,00	432,00	21	2	7560	864	
20+ anni exp. Sviluppo .NET, .NET Coreazure, React	Consulente di evoluzione tecnologica	360,00	432,00	21	2	7560	864	
15+ anni exp. Sviluppo .NET, .NET Core	Consulente processi	470,00	564,00	21	3	9870	1692	
20+ anni exp. sviluppo .NET, .NET Core, 5 anni .NET solution architect, React	Consulente processi	470,00	564,00	21	3	9870	1692	

2.4 GESTIONE DI UN SECURITY OPERATION CENTER (SOC)

DETTAGLIO SERVIZIO SOC (CREG200297)

Profilo	Tariffa Std	Tariffa extra	gg std	gg in reperibilità	Canone mensile std	Canone mensile reperibilità	Totale
Consulente processi	470,00	564,00	19		8.930,00		19.010,00
Consulente di evoluzione tecnologica	360,00	432,00	28		10.080,00		

2.5 ASSISTENZA TECNICA DI TIPO CORRETTIVO, ADATTATIVO ED EVOLUTIVO

EFFORT STIMATO PER INTERVENTI DI ASSISTENZA (CREG200297)

Profilo	**Figura professionale**	**Tariffa giornaliera**	**gg stimate**	**totale**
		(8 ore comprese fra le 08.00 e le 18.00)		
Consulente .Net	Consulente di integrazione applicativa	360	100	36.000,00
Team Leader	Consulente processi	470	150	70.500,00
Consulente CRM	Consulente specialista di prodotto	344	210	72.240,00
Consulente Power BI	Consulente specialista di prodotto	344	250	86.000,00
Consulente Azure	Consulente di evoluzione tecnologica	360	100	36.000,00
Consulente O365	Consulente di evoluzione tecnologica	360	50	18.000,00
Consulente Security	Consulente di evoluzione tecnologica	360	50	18.000,00
Specialista MS Dynamics	Supporto di II livello su piattaforma Dynamics	525,47	80	42.037,60
Consulente MS Dynamics	Supporto e formazione on the job piattaforma Dynamics	570,94	50	28.547,00
				407.324,60

Profilo	**Tariffa giornaliera** **(8 ore comprese fra le 08.00 e le 18.00)**
Capo Progetto	300,00
Security Architect	372,90
Specialista di tecnologia/ prodotto Senior	295,00
Specialista di tecnologia/ prodotto	235,00
	(Orario Continuativo H24)
Specialista di tecnologia/ prodotto Senior	1180,00
Specialista di tecnologia/ prodotto	930,00

ALLEGATO B

ATTRIBUZIONE DEL RUOLO E DEGLI OBBLIGHI DI CUI ALL'ART. 28 DEL REGOLAMENTO UE 2016/679

INDICE

1. DEFINIZIONI

Nel presente documento si intende per

- "*Amministrazione Cliente*", il Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto per l'emergenza epidemiologica COVID -19 e per l'esecuzione della campagna vaccinale nazionale, Gen. C.A. Francesco Paolo Figliuolo, nominato con DPCM 1°- 2021, (di seguito anche "Commissario") destinatario dei servizi erogati dalla Sogei, che riveste la qualifica di *Titolare del Trattamento* e per cui Sogei riveste la qualifica di *Responsabile del trattamento*;
- "*Dati Personali*" qualsiasi informazione relativa a una persona fisica identificata o identificabile (interessato) - ivi inclusi i dati di cui agli artt. 9 e 10 del Regolamento - trattata dal Responsabile del trattamento per conto del Titolare;
- "*Contratto*" si intende la *Convenzione* comprensiva di tutta la documentazione allo stessa afferente, stipulata tra il Commissario e Sogei S.p.A.;
- "*Norme in materia di protezione dei dati personali*" il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento nell'ordinamento nazionale al Regolamento (UE) n. 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 di cui al D.lgs. 30 giugno 2003 n. 196, come modificato e integrato dal D.lgs. n. 101/2018;
- "*Misure di Sicurezza*" le misure di sicurezza tecniche e organizzative adeguate garantire un livello di sicurezza adeguato al rischio di cui all'art. 32 del Regolamento;
- "*Persone autorizzate al trattamento*" persone che in qualità di dipendenti, collaboratori, amministratori di sistema o consulenti del Responsabile del trattamento e/o del Sub-Responsabile del trattamento sono stati da questi autorizzati al trattamento dei dati personali sotto la loro diretta autorità;
- "*Registro delle attività di trattamento*" o "*Registro*", il registro tenuto dal Responsabile del trattamento di tutte le categorie di attività relative al trattamento svolte per conto del Titolare del trattamento, di cui all'art. 30 del GDPR;
- "*Regolamento*" o "*GDPR*" il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27.04.2016, relativo 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);
- "*Responsabile iniziale del trattamento*" o "*Responsabile del trattamento*" o "*Responsabile*" ai sensi dell'art. 4, n. 8 del Regolamento, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento individuato per i trattamenti dati di seguito

specificati per conto del Titolare o dell'eventuale Contitolare del trattamento, individuato in relazione al Contratto nella società Sogei S.p.A.;

- "*Sub-Responsabile del trattamento*" o "*Sub-Responsabile*" il fornitore o i suoi subappaltatori e subfornitori, individuati con procedura a evidenza pubblica, di cui Sogei S.p.A. si avvale per effettuare eventuali trattamenti di dati personali per conto del Titolare;
- *Titolare del trattamento*" o "*Titolare*" ai sensi dell'art. 4, n. 7 del Regolamento, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali nell'*Amministrazione Cliente*;
- "*Trattamento*" qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma messa a disposizione, il raffronto o l'interconnessione, la limitazione, allineamento o combinazione, la cancellazione o la distruzione;
- "*Violazione dei dati personali (data breach)*" la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

2. ATTRIBUZIONE DEL RUOLO DI RESPONSABILE

Premesso che

- il Commissario svolge i compiti ad esso demandati dalla legge ed in particolare dall'articolo 122 del decreto-legge 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27;
- Sogei riveste il ruolo di società in house al Ministero dell'economia e delle finanze, in ragione delle disposizioni di legge e di Statuto che ne regolano l'attività;
- a tale riguardo è stato stipulato in data 30 marzo 2021 il Contratto in relazione al quale è necessario procedere alla sottoscrizione di apposito atto di attribuzione a Sogei S.p.A. del ruolo di Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento (cd. designazione);
- Sogei S.p.A. presenta garanzie sufficienti in termini di conoscenza specialistica, affidabilità, esperienza e risorse per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del Regolamento, compreso il profilo relativo alla sicurezza del trattamento.

e che le premesse formano parte integrante e sostanziale del presente atto,

Il Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto per l'emergenza epidemiologica COVID -19 e per l'esecuzione della campagna vaccinale nazionale, Gen. C.A. Francesco Paolo Figliuolo, nominato con DPCM 1°- 2021, in qualità di Titolare del trattamento, ai sensi dell'art. 28 del Regolamento

ATTRIBUISCE A

Sogei S.p.A., con sede legale in Roma, via M. Carucci n. 99, codice fiscale 02327910580, partita IVA 01043931003, in persona del legale rappresentante dott. Andrea Quacivi, domiciliato per la carica presso la sede sociale, il ruolo di Responsabile del trattamento dei dati personali effettuato nell'esecuzione del Contratto ai sensi dell'art. 28 del regolamento.

A tale riguardo il Responsabile del trattamento, sottoscrivendo il presente atto:

- conferma la sua diretta e approfondita conoscenza degli obblighi che si assume in relazione a quanto disposto dal Regolamento e, più in generale, dalle Norme in materia di protezione dei dati personali;
- si obbliga a procedere al trattamento dei dati – laddove questo sia necessario all'esecuzione delle prestazioni affidate – attenendosi in materia di sicurezza dei dati, oltre che al rispetto della normativa vigente in materia di protezione dei

dati personali anche, alle istruzioni di carattere generale nonché a ogni altra istruzione documentata concordate con il Titolare.

Di seguito sono definite le istruzioni di carattere generale, che possono essere integrate e modificate nel tempo per iscritto dal Titolare.

3. ISTRUZIONI

3.1 ELEMENTI ESSENZIALI DEI TRATTAMENTI CHE IL RESPONSABILE È AUTORIZZATO A SVOLGERE

Il Responsabile è autorizzato a trattare per conto del Titolare tutti i dati personali necessari per la corretta esecuzione del Contratto.

La durata del trattamento è limitata e coincide con la durata dell'incarico conferito dal Titolare con il Contratto ovvero di sue eventuali proroghe, fatti salvi l'adempimento di specifici obblighi di legge o di documentate istruzioni impartite dal Titolare.

Alla luce delle attribuzioni del Commissario Straordinario ex art 122 del D.L. 17 marzo 2020, n.18, recante "Misure di potenziamento del Sevizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19" (convertito, con modificazioni, dalla L. 24 aprile 2020, n. 27), il tipo di dati personali trattati è correlato a finalità di carattere contrattuale (art. 6, co.1 lett. b) GDPR), all'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 6, co. 1, lett. e) GDPR) e per adempiere a un obbligo legale (art. 6, co. 1, lett. c) GDPR).

Il tipo di dati personali trattati sono:

- dati personali comuni ex art. 4 GDPR;
- dati personali particolari di cui all'art. 9 GDPR strettamente correlati alla finalizzazione delle procedure gestite mediante le Piattaforme Digitali.

Le categorie di interessati a cui si riferiscono i dati personali sono i soggetti che presentano la domanda di accreditamento alle Piattaforme Digitali.

Per l'esecuzione delle attività di cui al Contratto, il Responsabile del trattamento è autorizzato in via generale, ai sensi dell'art. 28, paragrafo 2 del Regolamento, a ricorrere ove necessario ad altri responsabili del trattamento (Sub-Responsabili) individuati con procedure a evidenza pubblica, assumendo, ricorrendone le condizioni, gli obblighi di cui all'art. 28, paragrafo 4 del Regolamento, come precisato nel successivo punto 3.2.7 del presente atto.

3.2 OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO NEI CONFRONTI DEL TITOLARE

3.2.1 LIMITI E TERMINI DEL TRATTAMENTO DEI DATI PERSONALI

Il Responsabile è tenuto a trattare i dati personali solo e nei limiti in cui ciò sia necessario per l'esecuzione delle prestazioni contrattuali e le relative finalità e nel Contratto.

3.2.2 ISTRUZIONI DEL TITOLARE

Il Responsabile è tenuto a trattare i dati personali soltanto su istruzione documentata del Titolare, anche in caso di trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile; in tal caso esso è tenuto ad informare il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

Il Responsabile non può trasferire i dati personali verso un Paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto un'autorizzazione scritta del Titolare. Tale autorizzazione, con la sottoscrizione del presente atto, viene concessa al Responsabile, e quindi ai suoi Sub-Responsabili, per tutti quei casi in cui questi ultimi ne abbiano necessità per il corretto funzionamento dei servizi e per l'erogazione degli stessi.

Ove il Responsabile rilevi la sua impossibilità a rispettare le istruzioni impartite dal Titolare deve attuare comunque le possibili e ragionevoli misure di salvaguardia e deve avvertire immediatamente il Titolare e concordare eventuali ulteriori misure di protezione.

Qualora il Responsabile ritenga che una delle istruzioni violi il Regolamento o altre disposizioni nazionali o comunitarie deve informare immediatamente il Titolare.

3.2.3 FORNITURA DEI DATI AL TITOLARE

Qualora il Titolare o soggetto/funzione da esso incaricato/a abbia necessità, per lo svolgimento dei propri compiti istituzionali, di accedere a dati non disponibili attraverso i servizi applicativi, li richiede per iscritto, esplicitando la tipologia dei dati, la tempistica e la modalità di fornitura, al Responsabile il quale è tenuto a renderli disponibili, secondo linee guida da concordare.

3.2.4 REGISTRO DEI TRATTAMENTI

Il Responsabile tiene un Registro di tutte le categorie di attività relative al trattamento (o ai trattamenti) svolti per conto del Titolare. Il Responsabile ed il Titolare devono assicurare la coerenza reciproca dei propri Registri.

Il Responsabile mette a disposizione dell'Autorità di controllo il Registro, ove richiesto, dandone al contempo informazione al Titolare.

3.2.5 AUTORITÀ DI CONTROLLO

Il Responsabile è tenuto in ogni caso a cooperare, su richiesta, con l'Autorità di controllo nell'esecuzione dei suoi compiti.

Il Responsabile si obbliga a cooperare con il Titolare al fine di fornire tutte le informazioni, i dati e la documentazione necessaria affinché il Titolare possa adempiere alle richieste dell'Autorità di controllo ovvero qualora si rendessero necessarie informazioni in caso di precontenzioso o contenzioso.

3.2.6 COMUNICAZIONE E DIFFUSIONE DI DATI

Il Responsabile non può comunicare e/o diffondere dati senza l'esplicita autorizzazione del Titolare, fatte salve le particolari esigenze di riservatezza espressamente esplicitate dall'Autorità Giudiziaria.

3.2.7 RICORSO A SUB-RESPONSABILI DEL TRATTAMENTO

Il Sub-Responsabile del trattamento dovrà rispettare gli obblighi in materia di protezione dei dati personali imposti al Responsabile dalla normativa in materia di protezione dei dati personali e dal Titolare con il presente atto e le eventuali ulteriori istruzioni documentate che lo stesso dovesse impartire.

A tal fine il Responsabile è autorizzato dal Titolare a designare ai sensi dell'art. 28 del Regolamento i fornitori quali Sub-Responsabili.

Ai Sub-Responsabili verranno imposti, con l'atto di attribuzione del ruolo stesso di Sub-Responsabile ai sensi dell'art. 28 del Regolamento - che può essere anche contenuto, ove possibile, nella documentazione della procedura ad evidenza pubblica - i medesimi obblighi e le medesime istruzioni ricevute dal Titolare, salvo

che la particolare natura del servizio acquisito richieda necessariamente, per la fruizione dello stesso da parte del Titolare, l'adesione a condizioni generali inerenti la protezione dei dati personali stabilite dal fornitore.

In tale caso il fornitore sarà nominato quale Sub-Responsabile ed il Titolare terrà conto, a riguardo, che l'adempimento alle prescrizioni del Regolamento, ivi incluse quelle relative alle misure di sicurezza ed alla privacy by default e by design da parte del Sub-Responsabile, saranno attuate sulla base delle condizioni e dei termini per la protezione dei dati personali stabilite da quest'ultimo.

Qualora il Sub-Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale del trattamento conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub- Responsabile ove abbia trasferito allo stesso gli stessi obblighi e le stesse istruzioni ricevute dal Titolare.

Il Responsabile si impegna a informare il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al Titolare l'opportunità di opporsi a tali modifiche.

Il Responsabile si impegna comunque a rispettare le condizioni di cui ai paragrafi 2 e 4 dell'art. 28 del Regolamento, per quanto applicabili.

3.2.8 RISERVATEZZA E FORMAZIONE DELLE PERSONE AUTORIZZATE AL TRATTAMENTO

Il Responsabile garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza e che siano adeguatamente formate in relazione alle Norme in materia di protezione dei dati personali e pienamente edotte rispetto alle istruzioni impartite dal Titolare.

3.2.9 OBBLIGHI DEL RESPONSABILE NELL'AMBITO DEI DIRITTI ESERCITATI DAGLI INTERESSATI

Il Responsabile, ove richiesto, deve collaborare e supportare nel dare riscontro scritto, anche di mero diniego, alle istanze trasmesse dagli Interessati nell'esercizio dei diritti previsti dagli artt. 15-23 del GDPR, vale a dire alle istanze per l'esercizio del diritto di accesso, di rettifica, di integrazione, di cancellazione e di opposizione, diritto alla limitazione del trattamento, diritto alla portabilità dei dati, diritto a non essere oggetto di un processo decisionale automatizzato, compresa la profilazione.

Qualora gli interessati trasmettano la richiesta per l'esercizio dei loro diritti al Responsabile, quest'ultimo deve inoltrarla tempestivamente al Titolare.

3.2.10 MISURE DI SICUREZZA

Fermo restando quanto precisato riguardo ai servizi cloud nell'articolo 12.3 del Contratto, il Responsabile, sulla base delle indicazioni del Titolare, adotta le misure richieste dall'art. 32 del Regolamento.

Nell'esecuzione del Contratto, il Responsabile supporta il Titolare nel tener conto dei principi della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita.

Fatto salvo quanto previsto al par. 3.2.7, quarto paragrafo, il Responsabile dovrà operare attenendosi alle previsioni contenute nel documento condiviso di "Metodologia per la protezione dei dati e per la valutazione d'impatto", se applicabile alla tipologia di servizio erogato, rendendo disponibile al Titolare ogni utile informazione per il corretto adempimento degli obblighi di cui agli articoli 25, 32 e 35 del Regolamento. Tale documento, allegato alle presenti istruzioni, sarà oggetto di revisione condivisa, secondo le modalità contenute nello stesso.

3.2.11 CANCELLAZIONE E DISTRUZIONE DEI DATI

E' facoltà del Titolare, terminata la prestazione dei servizi relativi al trattamento, ottenere in qualunque momento la cancellazione o la restituzione di tutti i dati personali e la cancellazione totale di tutte le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati.

3.2.12 ISPEZIONI E REVISIONE

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi a suo carico, consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto da questi incaricato, anche attraverso periodiche attività di audit, con modalità che saranno, di volta in volta, concordate.

3.2.13 CODICI DI CONDOTTA

Ne caso in cui il Responsabile del trattamento aderisca a un codice di condotta approvato ai sensi dell'articolo 40 del Regolamento o a un meccanismo di certificazione approvato ai sensi dell'articolo 42 del Regolamento, tale adesione può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 dell'art. 28 del Regolamento.

3.2.14 VIOLAZIONI DEI DATI

Il Responsabile del trattamento si dichiara consapevole degli obblighi che incombono sul Titolare del trattamento, ai sensi dell'art. 33 del Regolamento, in caso di violazione dei dati che sia tale da presentare un rischio per i diritti e le libertà fondamentali delle persone.

Il Responsabile si impegna a comunicare al Titolare la violazione dei dati personali "senza ingiustificato ritardo", ai sensi e nei termini previsti dall'art. 33 del Regolamento. Tale obbligo di cooperazione si impone anche nel caso in cui il Titolare debba comunicare la violazione all'interessato.

Il Responsabile si atterrà al "Flusso di notifica di Data Breach all'Autorità di controllo" allegato alle presenti istruzioni.

3.2.15 VALUTAZIONE DI IMPATTO

Per svolgere la valutazione d'impatto sulla protezione dei dati personali il Titolare può consultarsi con il proprio Responsabile della protezione dei dati, ai sensi dell'art. 35, comma 2, del Regolamento.

Il Responsabile del trattamento si impegna ad assistere il Titolare, a livello tecnico e organizzativo, nello svolgimento della valutazione d'impatto, così come disciplinata dall'art. 35 citato, in tutte le ipotesi in cui il trattamento preveda o necessiti della preliminare valutazione di impatto sulla protezione dei dati personali o del suo aggiornamento, fatto salvo quanto previsto al par. 2.7, quarto paragrafo.

Il Responsabile dovrà operare attenendosi alle previsioni contenute nel documento condiviso di "Metodologia per la protezione dei dati e per la valutazione d'impatto", se applicabile alla tipologia di servizio erogato, rendendo disponibile al Titolare ogni utile informazione per il corretto adempimento degli obblighi di cui all'articolo 35 del Regolamento. Tale documento, allegato alle presenti istruzioni, sarà oggetto di revisione condivisa, secondo le modalità contenute nello stesso.

Il Responsabile del trattamento si impegna altresì ad assistere il Titolare nell'attività di consultazione preventiva dell'Autorità di controllo prevista dall'articolo 36 del Regolamento.

3.2.16 MODIFICHE NORMATIVE

Nell'eventualità di qualsiasi modifica delle Norme in materia di protezione dei dati personali, il Responsabile del trattamento supporta, nel rispetto dei vincoli del Contratto e nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse, il Titolare negli adeguamenti necessari.

3.3 RINVIO

Per tutto quanto non espressamente disciplinato nel presente atto, si richiamano gli obblighi previsti a carico del Responsabile del trattamento nel Contratto e dalle Norme in materia di protezione dei dati personali.

ALLEGATI

1. Metodologia per la protezione dei dati e per la valutazione d'impatto
2. Flusso di notifica di Data Breach all'Autorità di controllo

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.

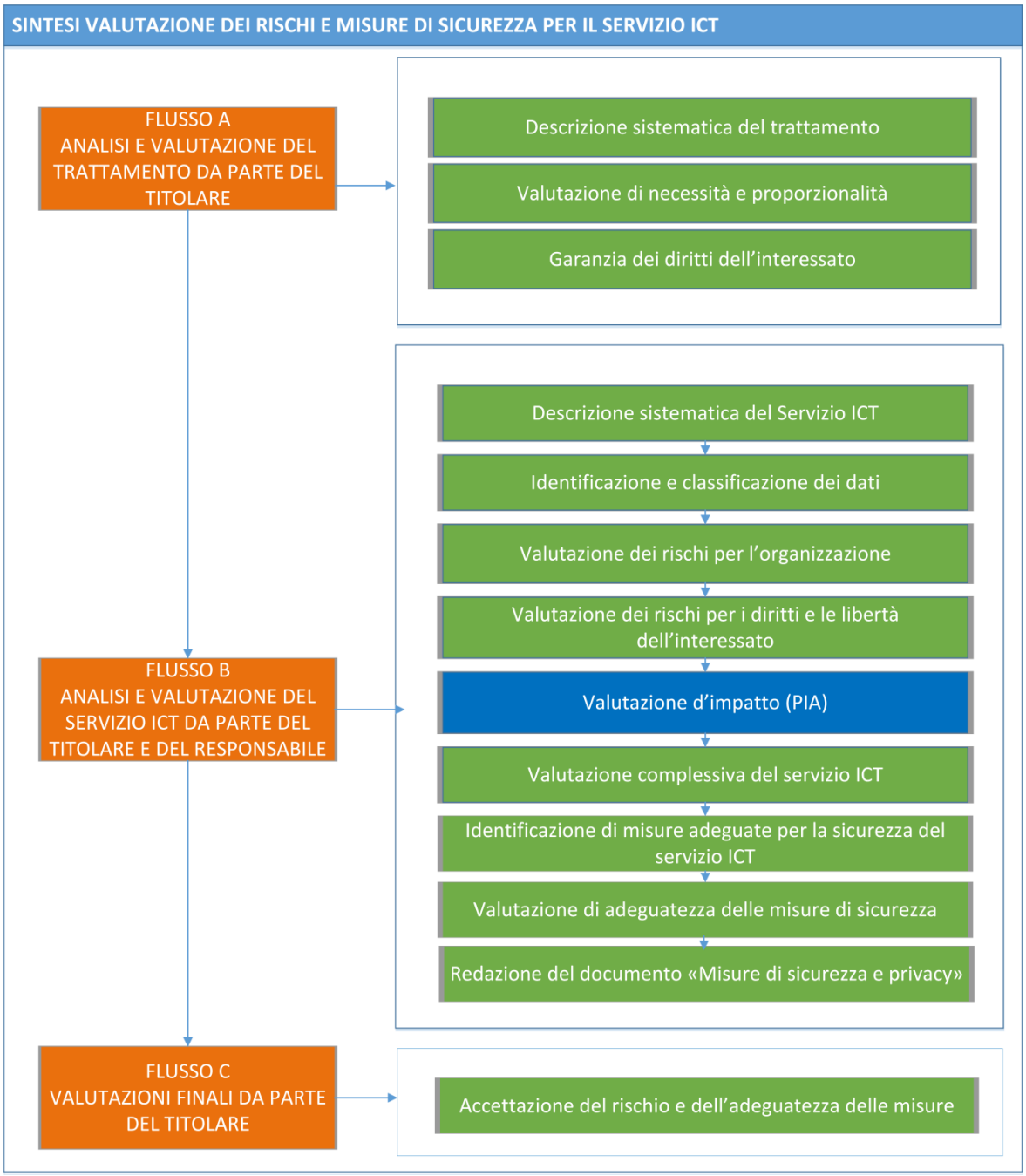
Di seguito il flusso di sintesi[1] per la valutazione dei rischi e delle misure di sicurezza per il Servizio ICT, suddiviso in tre parti:

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:

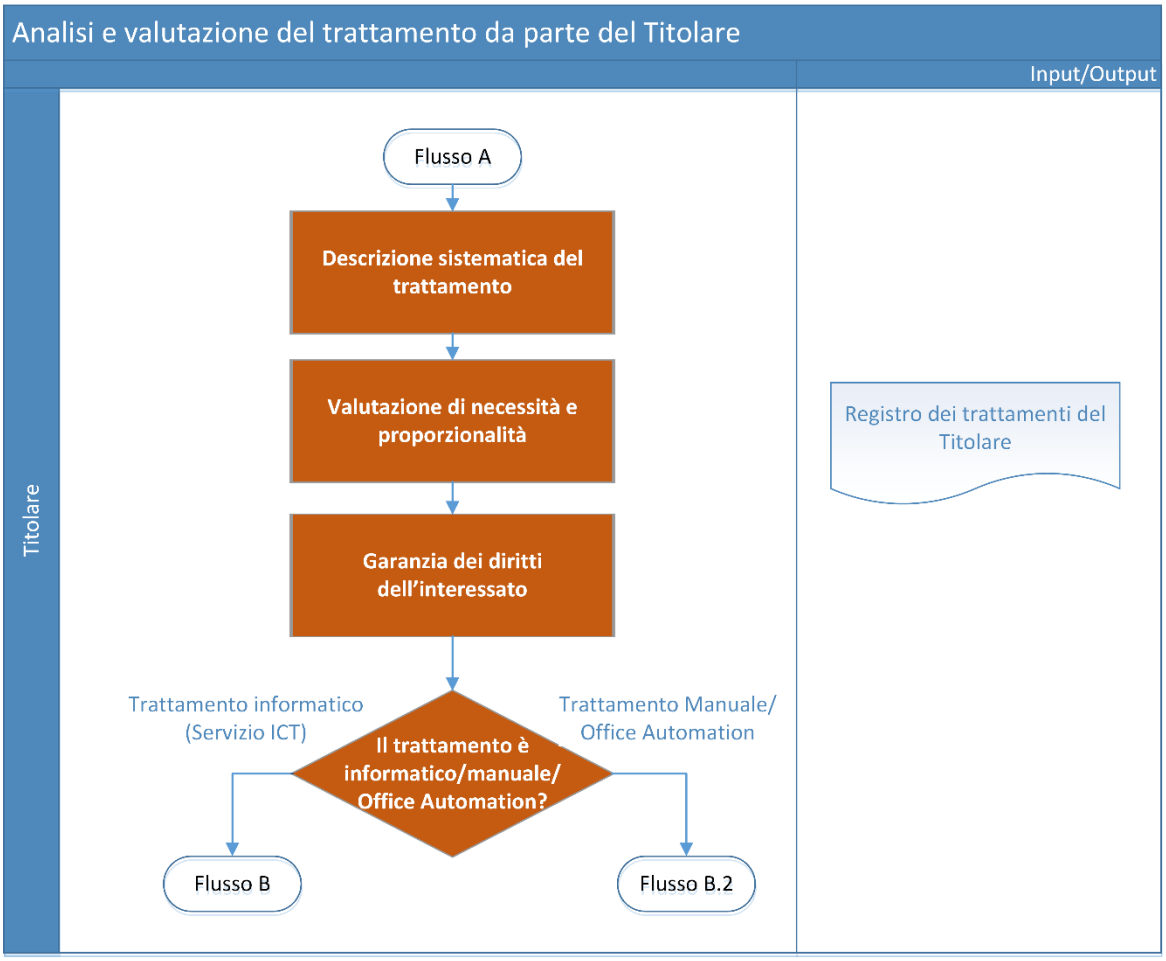
- rischi per i diritti e le libertà degli interessati - compresa la valutazione d'impatto, ove necessaria - relativi al trattamento di dati personali;
- rischi per l'organizzazione del Titolare, relativi alla sicurezza delle informazioni elaborate;
- adeguatezza delle misure di sicurezza da applicare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

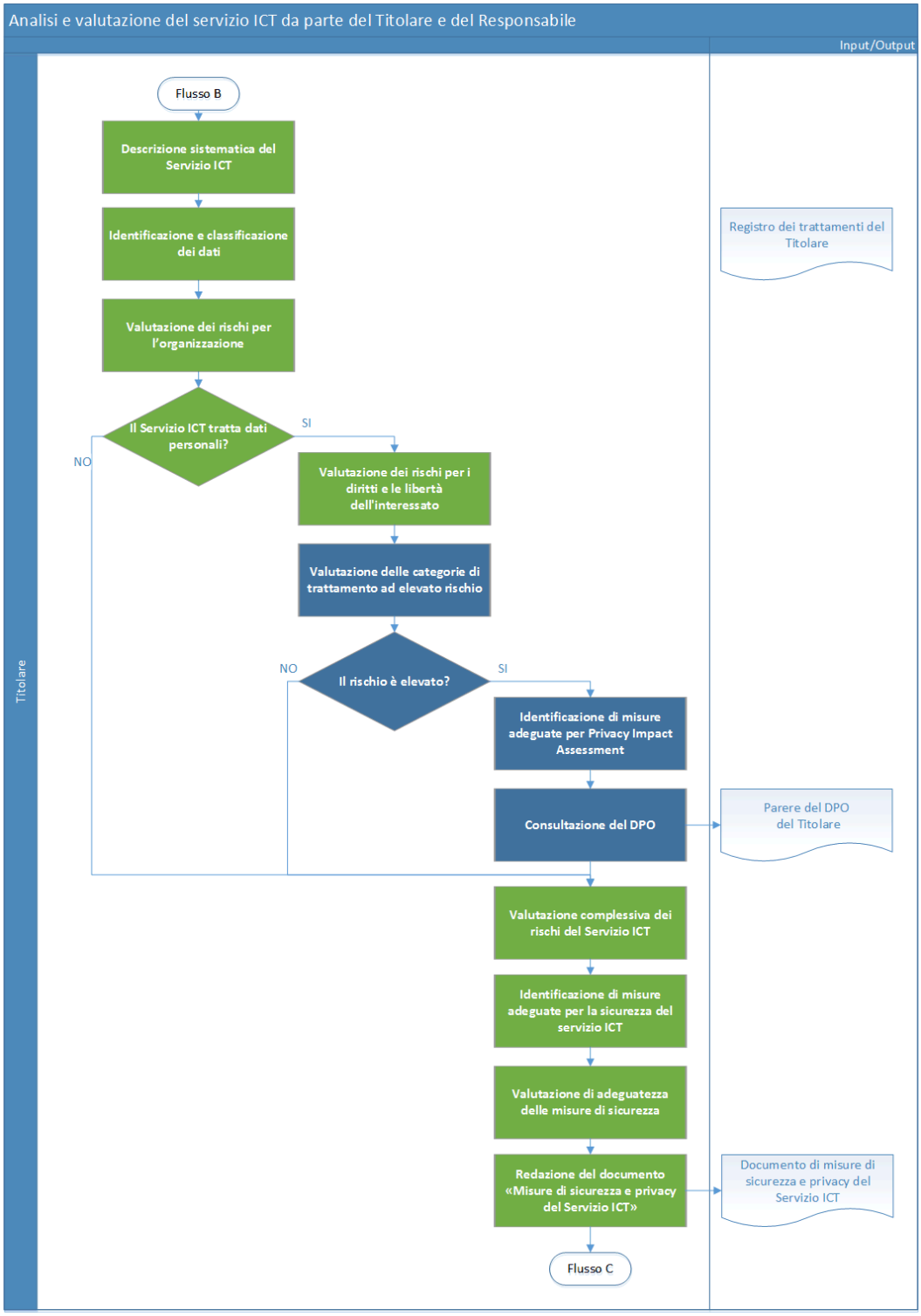
parere in merito al fine di garantire che il trattamento rispetti in ogni caso il Regolamento e può avvalersi dei propri poteri, tra cui rivolgere ammonimenti o ammonizioni, imporre limitazioni o divieti. L'Autorità di controllo, inoltre, viene notificata di eventuali violazioni di dati personali (*data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

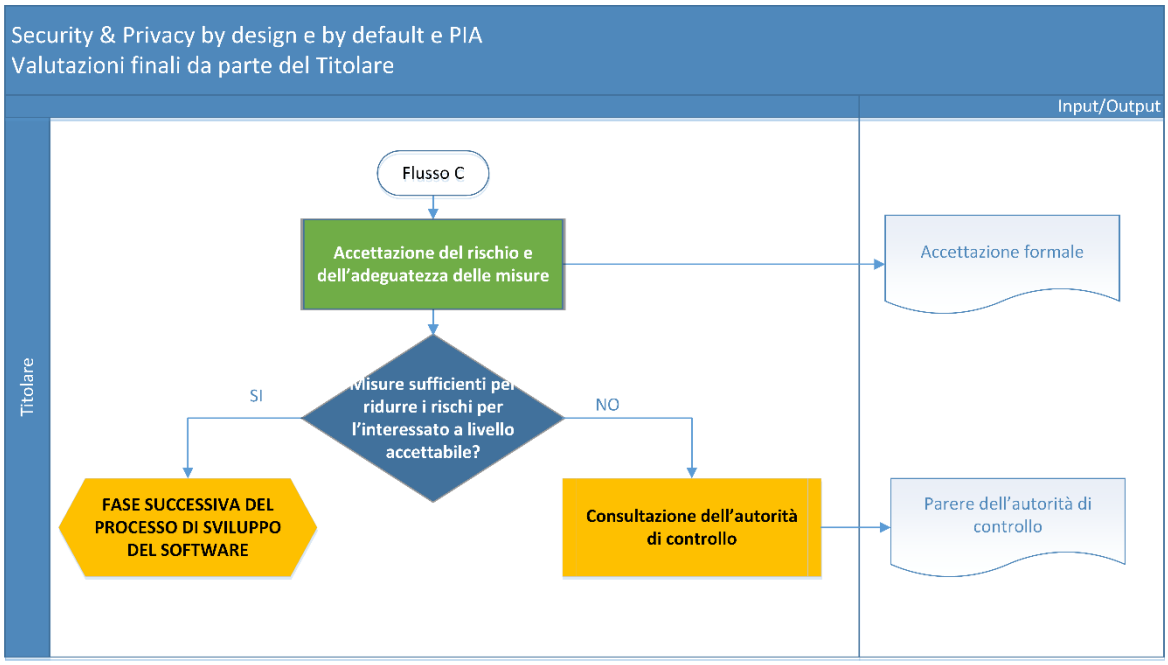
Il Responsabile del Servizio ICT invia il documento contestualmente al documento "Analisi dei Requisiti"/"Specifica di intervento" se previsto o, in caso contrario, in un momento utile a garantire comunque uno sviluppo coerente del Servizio ICT.

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.

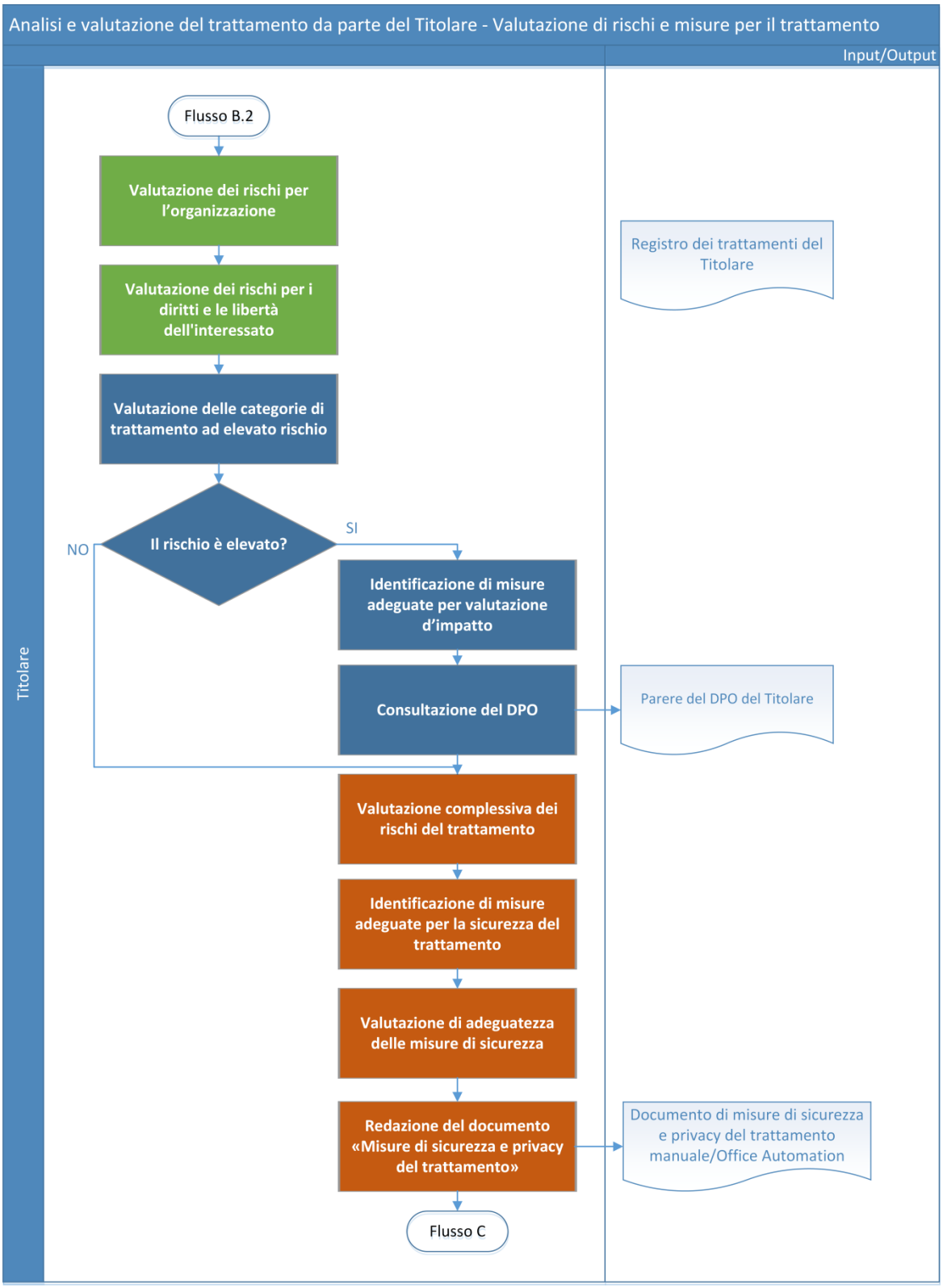
Oltre alle misure selezionate sulla base del profilo di rischio del trattamento/ Servizio ICT, Sogei protegge tutte le informazioni che tratta in qualità di Titolare o di Responsabile con un set di misure infrastrutturali elencate in specifici allegati ai registri dei trattamenti.

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

FLUSSO DI NOTIFICA DI *DATA BREACH* ALL'AUTORITÀ DI CONTROLLO

Nel presente documento è descritto il flusso di notifica delle violazioni dei dati personali che presentano un rischio per i diritti e le libertà delle persone fisiche (*Data Breach*) in conformità a quanto previsto dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 ("Regolamento Generale sulla Protezione dei Dati" - d'ora in avanti "RGPD").

Ai sensi dell'articolo 4 del RGPD per "violazione dei dati personali" si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Il flusso inizia con l'identificazione di una possibile "violazione dei dati personali" nell'ambito della gestione di un evento di sicurezza e si conclude con l'invio all'Autorità di controllo della notifica di avvenuto *Data Breach* secondo quanto previsto dal RGPD (riferimento artt. 33 e 34).

Il flusso prevede l'interazione e lo scambio di informazioni tra Sogei, il Responsabile Protezione Dati della stessa (d'ora in avanti RPD), l'Amministrazione Titolare interessata dall'evento e il RPD della stessa al fine di consentire all'Amministrazione Titolare di adempiere alle prescrizioni previste dal RGPD.

1. DESCRIZIONE DEL FLUSSO

Il flusso di notifica all'Autorità di controllo da parte dell'Amministrazione Titolare prevede i passi di seguito elencati.

- Il CERT Sogei (struttura aziendale preposta al trattamento degli incidenti di sicurezza informatica), nel corso della gestione di un incidente di sicurezza, rileva una possibile "violazione dei dati personali" (*Data Breach*). Il CERT Sogei notifica all'Amministrazione Titolare e al RPD della stessa che è in corso la valutazione di un incidente di sicurezza, fornendo, altresì, una prima sommaria descrizione dell'incidente e assegnando un identificativo univoco allo stesso: il CERT Sogei invia le informazioni scrivendo a commissarioemergenzacovid19@pec.governo.it e commissariocovid19_dpo@covid19.difesa.it. Nel caso in cui sia l'Amministrazione

Titolare a venire a conoscenza di un incidente di sicurezza caratterizzato da una possibile "violazione dei dati personali" *(Data Breach*) che necessita dell'intervento di Sogei, l'Amministrazione Titolare informa il CERT Sogei e il proprio RPD scrivendo a cert@sogei.it e ufficiodpo@sogei.it. Il CERT Sogei avvia la verifica fornendo eventualmente informazioni aggiuntive a quelle ricevute e assegnando un identificativo unico ad esso.

- Il CERT Sogei verifica la presenza o meno della "violazione di dati personali".
- In caso di esito negativo della verifica, il CERT Sogei termina il processo, notificando all'Amministrazione Titolare ed al suo RPD la chiusura dell'incidente caratterizzato dall'identificativo precedentemente comunicato e le motivazioni.
- In caso di esito positivo della verifica, ossia accertata la "violazione dei dati personali", il CERT Sogei comunica immediatamente e senza ingiustificato ritardo e in modo dettagliato il Data Breach all'Amministrazione Titolare e contestualmente al relativo RPD, riportando le informazioni di propria competenza indicate nel successivo paragrafo 2.
- l'Amministrazione Titolare, ricevuta la notifica di *Data Breach* e sentito il proprio RPD, valuta il livello di gravità della "violazione dei dati personali" proposto da Sogei avvenuta sui dati personali contenuti nelle banche dati disponibili nella propria titolarità. Nel caso in cui la "violazione dei dati personali" comporti un rischio per i diritti e le libertà delle persone fisiche, provvede a completare la notifica con le informazioni di propria competenza e ad inviare la stessa all'Autorità di Controllo entro 72 ore dalla conoscenza dell'avvenuta compromissione dei dati personali, dandone contestualmente riscontro al CERT Sogei e al RPD di quest'ultima. Qualora la notifica all'Autorità di Controllo non sia effettuata entro 72 ore, provvede, altresì, a corredarla con le motivazioni del ritardo.

Eventuali richieste di ulteriori informazioni o modifiche alla notifica all'Autorità di Controllo necessarie durante le attività di risoluzione dell'evento saranno concordate tra l'Amministrazione Titolare, il CERT Sogei e i rispettivi RPD.

Il CERT Sogei dovrà mantenere un'accurata documentazione di tutte le "violazioni di dati personali" registrate, comprese le circostanze ad esse relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione sarà integrata con le eventuali azioni intraprese dall'Amministrazione Titolare e opportunamente comunicate allo stesso.

2. NOTIFICA ALL'AUTORITA' DI CONTROLLO GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Le informazioni previste dal RGPD saranno raccolte e riportate nella notifica di avvenuto *Data Breach* secondo lo schema seguente.

Il CERT Sogei inserirà nella notifica le seguenti informazioni, che saranno comunicate all'Amministrazione Titolare:

- tipologia di incidente;
- descrizione del servizio impattato e/o della banca/banche dati oggetto di violazione di dati personali;
- intervallo temporale dell'incidente;
- luogo dell'incidente;
- misure tecniche di sicurezza applicate ai dati violati;
- misure attivate per il contenimento e la prevenzione;
- descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- descrizione della probabile conseguenza della violazione dei dati personali;
- descrizione delle misure di sicurezza adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione di dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
- proposta di comunicazione di violazione di dati personali all'/agli interessato/i in base ad un'analisi dei dati oggetto di violazione (qualora la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche) e non ricorrendo alcuna delle condizioni di cui all'articolo 34, comma 3, del RGPD, che escludono la necessità di comunicazione della violazione all'interessato.

Il Titolare notificherà la violazione all'Autorità di Controllo, avendo cura di darne comunicazione anche a Sogei.