CONVENZIONE

TRA

IL MINISTERO DELL'AMBIENTE E DELLA SICUREZZA ENERGETICA (MASE)

E

LA SOCIETA' GENERALE D'INFORMATICA S.P.A. (SOGEI)

PER LA REALIZZAZIONE DELLA PIATTAFORMA RELATIVA ALL'INIZIATIVA BONUS AMBIENTE E LA GESTIONE DELLE ATTIVITA' AD ESSA CONNESSE

CONVENZIONE

PER LA REALIZZAZIONE DELLA PIATTAFORMA RELATIVA ALL'INIZIATIVA BONUS AMBIENTE E LA GESTIONE DELLE ATTIVITÀ AD ESSA CONNESSE

TRA

il Ministero dell'Ambiente e della Sicurezza Energetica (nel prosieguo MASE), con sede in Roma, via Cristoforo Colombo, n. 44, 00147 Roma, codice fiscale 97047140583, rappresentato da Giuseppe Lo Presti, in qualità di Direttore generale della Direzione uso sostenibile del suolo e delle risorse idriche (DG USSRI).

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, in persona del suo legale rappresentante pro-tempore e Amministratore Delegato, dott. Andrea Quacivi che agisce per la stipula della presente Convenzione in virtù dei poteri conferitigli dal Consiglio di Amministrazione come da delibera del 13 luglio 2021 (nel prosieguo SOGEI);

PREMESSE

VISTE le disposizioni vigenti sull'amministrazione del patrimonio e sulla contabilità generale dello Stato, nonché quelle correttive, integrative e di attuazione;

VISTA la legge 8 luglio 1986, n. 349, che ha istituito il Ministero dell'ambiente e ne ha definito le funzioni;

VISTO il decreto legislativo 30 luglio 1999, n. 300 e, in particolare, gli articoli da 35 a 40, come da ultimo modificato dal decreto legge 1 marzo 2021, n. 22, convertito dalla legge 22 aprile 2021, n. 55, relativi alle attribuzioni e all'ordinamento del Ministero della Transizione Ecologica;

VISTO il Decreto del Presidente del Consiglio dei Ministri del 29 luglio 2021, n. 128, recante "Regolamento di organizzazione del Ministero della Transizione Ecologica";

VISTO il decreto del Ministro della transizione ecologica n. 458 del 10 novembre 2021, recante "Individuazione e definizione dei compiti degli uffici di livello dirigenziale non generale del Ministero della Transizione Ecologica";

CONSIDERATO che, ai sensi dell'articolo 2, comma 1, del citato decreto del Presidente del Consiglio dei ministri n. 128 del 2021, il Ministero è articolato in tre Dipartimenti e dieci Direzioni Generali, oltre agli Uffici di diretta collaborazione del Ministro, e che ai sensi dell'articolo 2, comma 2, del medesimo

decreto i Dipartimenti assumono la denominazione di Dipartimento amministrazione generale, pianificazione e patrimonio naturale (DiAG), Dipartimento sviluppo sostenibile (DiSS) e Dipartimento energia (DiE);

CONSIDERATO che, ai sensi dell'articolo 2, comma 4, del citato decreto del Presidente del Consiglio dei ministri n. 128 del 2021, nel Dipartimento DiSS è inserita, tra le altre, la Direzione Generale Uso Sostenibile del Suolo e delle Risorse Idriche (USSRI);

VISTO il Documento di economia e finanza 2021, approvato dal Consiglio dei Ministri il 15 aprile 2021, e la relativa nota di aggiornamento deliberata il 29 settembre 2021;

VISTO il decreto del Ministro della transizione ecologica n. 464 del 12 novembre 2021, recante "Atto di indirizzo sulle priorità politiche per l'anno 2022 e il triennio 2022-2024";

VISTA la legge 30 dicembre 2021, n. 234, concernente il "Bilancio di previsione dello Stato per l'anno finanziario 2022 e bilancio pluriennale per il triennio 2022- 2024";

VISTO il decreto del Ministro dell'Economia e delle Finanze del 31 dicembre 2021, recante "Ripartizione in capitoli delle Unità di voto parlamentare relative al bilancio di previsione dello Stato per l'anno finanziario 2022 e per il triennio 2022-2024";

VISTO il decreto del Presidente del Consiglio dei Ministri del 20 gennaio 2022, registrato dalla Corte dei Conti in data 4 febbraio 2022, n. 151, con cui il dott. Giuseppe Lo Presti ha ricevuto l'incarico di Direttore della Direzione Generale uso sostenibile del suolo e delle risorse idriche (USSRI);

VISTA la direttiva generale recante gli indirizzi generali sull'attività amministrativa e sulla gestione del Ministero della transizione ecologica per l'anno 2022, approvata con decreto ministeriale n. 101 del 3 marzo 2022 e ammessa alla registrazione della Corte dei Conti in data 24 marzo 2022 al n. 554;

VISTO il decreto del Capo Dipartimento sviluppo sostenibile prot. n. 80 del 5 aprile 2022, vistato dall'Ufficio Centrale di Bilancio il 7 aprile 2022 n. 87, con cui è stata delegata la gestione delle risorse finanziarie, nell'ambito di alcuni programmi di spesa, delle azioni, dei capitoli e dei piani gestionali ai Direttori Generali del Dipartimento DiSS, tra cui il Dr Giuseppe Lo Presti, in quanto titolare del relativo centro di costo;

VISTO l'art. 4, comma 1, del D.L. 173 del 11/11/2022, in base al quale il Ministero della transizione ecologica assume la denominazione di Ministero dell'ambiente e della sicurezza energetica;

VISTO il Decreto del Presidente del Consiglio dei Ministri del 10 dicembre 2021 e relativo al Credito d'imposta per le erogazioni liberali per interventi di bonifica e prevenzione del dissesto idrogeologico su edifici e terreni pubblici, per la realizzazione di parchi e aree verdi e recupero di aree dismesse di proprietà pubblica (GU 8 febbraio 2022 n. 32) in attuazione della legge 30 dicembre 2018, n. 145, recante «Bilancio

di previsione dello Stato per l'anno finanziario 2019 e bilancio pluriennale per il triennio 2019-2021» e, in particolare, i commi da 156 a 161 dell'articolo 1 che riconoscono un credito d'imposta per erogazioni liberali per interventi su edifici e terreni pubblici di bonifica ambientale, di prevenzione e risanamento del dissesto idrogeologico e sistemazione di parchi e aree verdi;

CONSIDERATO che, fatte salve le disposizioni di cui al decreto legislativo 30 giugno 2003, n. 196, recante il «Codice in materia di protezione dei dati personali», al Ministero della transizione ecologica spetta provvedere agli adempimenti previsti dal comma 160 dell'articolo 1 della legge n. 145 del 2018, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri per il bilancio dello Stato;

VISTO l'art. 1, comma 97, della legge 27 dicembre 2019, n. 160, il quale dispone che "*al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa e di favorire la sinergia tra processi istituzionali afferenti ambiti affini, favorendo la digitalizzazione dei servizi e dei processi attraverso interventi di consolidamento delle infrastrutture, razionalizzazione dei sistemi informativi e interoperabilità tra le banche dati, in coerenza con le strategie del Piano triennale per l'informatica nella pubblica amministrazione, il Ministero dell'ambiente e della tutela del territorio e del mare può avvalersi della SOGEI S.p.A. di cui all'articolo 83, comma 15, del decreto legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, per servizi informatici strumentali al raggiungimento dei propri obiettivi istituzionali e funzionali, nonché per la realizzazione di programmi e progetti da realizzare mediante piattaforme informatiche rivolte ai destinatari degli interventi. L'oggetto e le condizioni dei servizi sono definiti mediante apposite convenzioni*.";

VISTO il 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;

VISTO il Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 contenente il Regolamento europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

CONSIDERATO che la SOGEI è stata interamente acquisita dal Ministero dell'Economia e delle Finanze ai sensi dell'articolo 59 del Decreto legislativo 30 luglio 1999 n. 300 e i relativi diritti dell'azionista in virtù dell'articolo 83, comma 15, del decreto legge 25 giugno 2008, n. 112, convertito con modificazioni dalla legge 6 agosto 2008, n. 133, sono esercitati dal Ministero dell'Economia e delle Finanze – Dipartimento del Tesoro, inoltre ai sensi del vigente Statuto della SOGEI il controllo analogo è esercitato dal Dipartimento delle finanze del Ministero dell'Economia e delle Finanze;

CONSIDERATO che la SOGEI S.p.A., ai sensi dell'articolo 4 del proprio Statuto, in quanto Organismo di diritto pubblico/amministrazione aggiudicatrice e in quanto interamente partecipata dal Ministero dell'Economia e delle Finanze ha per oggetto prevalente la prestazione "*in house*" di servizi strumentali all'esercizio delle funzioni pubbliche attribuite al Ministero dell'Economia e delle Finanze e delle Agenzie fiscali ed ha, tra l'altro, per oggetto lo svolgimento, nel rispetto della normativa vigente, di ogni attività di natura informatica per conto dell'Amministrazione pubblica centrale;

CONSIDERATO che il riuso dei programmi informatici di proprietà delle pubbliche amministrazioni garantisce il raggiungimento delle finalità di economicità, efficienza, tutela degli investimenti e neutralità tecnologica;

VISTA la nota del 04/02/2022 prot. n. 13858 con la quale la Direzione Generale Uso sostenibile del suolo e delle risorse idriche ha informato la Direzione Generale Innovazione Tecnologica e Comunicazione, nelle more della completa definizione del nuovo assetto organizzativo del Ministero, che come è noto prevedeva tale competenza in capo alla Direzione Generale Innovazione Tecnologica, di essere disposta a provvedere direttamente alla realizzazione del portale web in questione, mediante l'utilizzo delle risorse appostate sul capitolo di spesa 7525;

VISTA la nota del 04/03/2022 prot. n. 27731 con la quale la Direzione Generale Innovazione Tecnologica e Comunicazione ha dato riscontro alla nota del 04/02/2022 prot. n. 13858 della Direzione Generale Uso sostenibile del suolo e delle risorse idriche ed ha espresso il nulla osta alla realizzazione della Piattaforma tramite convenzione con la SOGEI mediante l'utilizzo delle risorse finanziarie all'uopo destinate sul capitolo 7525;

VISTA la Convenzione del 17/08/2022 prot. n. 63 tra la Direzione Generale Innovazione Tecnologica e Comunicazione e Società Generale di Informatica Sogei S.p.A. per la progettazione, lo sviluppo e la conduzione del sistema informativo del Mite, registrata alla Corte dei Conti in data 24/10/2022 n.2739;

CONSIDERATO che per la copertura finanziaria del predetto servizio di gestione delle attività di liquidazione il Ministero si avvale delle risorse iscritte sul capitolo 7525 "Somma da accreditare alla contabilità speciale 1778 " Agenzia delle Entrate – Fondi di bilancio" per essere riversata all'entrata del bilancio dello Stato a reintegro dei minori versamenti conseguenti ai crediti di imposta fruiti dalle persone fisiche e dagli enti non commerciali per le erogazioni liberali in denaro effettuate per interventi su edifici e terreni pubblici, ai fini della bonifica ambientale, compresa la rimozione dell'amianto dagli edifici, della prevenzione e risanamento del dissesto idrogeologico, della realizzazione o ristrutturazione di parchi e aree verdi attrezzate e il recupero di aree dismesse di proprietà pubblica" , Programma 19, Missione 18, Azione 3, dello stato di previsione del Ministero della Transizione Ecologica (ora Ministero dell'ambiente e della sicurezza energetica) per il corrente esercizio finanziario;

CONSIDERATO che l'importo complessivo dell'offerta tecnico economica non supera il limite massimo del 2% delle risorse iscritte sul capitolo 7525;

VISTA la nota prot. n. 91786 del 22/07/2022 con cui il MiTE ha richiesto a SOGEI S.p.A. di trasmettere un'offerta tecnico-economica per la realizzazione dell'iniziativa e la gestione delle attività di implementazione e sviluppo di un portale web in coerenza con quanto disposto dal DPCM 10 dicembre 2021;

VISTA la nota acquisita al prot. n. 27295 del 08/08/2022, attraverso la quale SOGEI, in riscontro alla richiesta del MiTE di cui al precedente visto, ha trasmesso l'offerta tecnico-economica per un importo complessivo di € 271.090,05 (duecentosettantunomilanovanta/05) IVA inclusa, di cui 151.869,55 (centocinquantunomilaottocentosessantanove/55) per l'anno 2022 e 119.220,50 (centodiciannovemiladuecentoventi/50) per l'anno 2023;

VISTA la nota acquisita al prot. n. 140160 dell'10/11/2022, attraverso la quale SOGEI, ha trasmesso una nuova offerta in sostituzione della precedente formulata con nota prot. 27295 del 08/08/2022, per un importo complessivo pari ad € 267.896,56 (duecentosessantasettemilaottocentonovantasei/56), di cui 128.448,46 (centoventottomilaquattrocentoquarantotto/46) per l'anno 2022 e 139.448,10 (centotrentanovemilaquattrocentoquarantotto/10) per l'anno 2023;

VISTA la nota prot. n. 141917 del 14/11/2022, rettificata con nota prot. 142457 del 15/11/2022, con cui la Direzione generale uso sostenibile del suolo e delle risorse idriche ha accettato l'offerta tecnico – economica presentata da SOGEI S.p.A. con nota prot. n. 140160 del 10/11/2022;

VISTA la nota del 21/11/2022 prot. n. 39935 con la quale SOGEI ha provveduto, ai sensi dell'articolo 26, comma 5 dello Statuto, a dare specifica informativa al Dipartimento delle Finanze, che esercita il controllo analogo sulla SOGEI S.p.A., ed alla struttura del Dipartimento del Tesoro, che esercita i diritti dell'Azionista sulla SOGEI S.p.A., al fine della verifica del mantenimento dell'equilibrio economico finanziario in relazione all'iniziativa di cui alla presente convenzione;

CONSIDERATO che con nota del 29/11/2022, prot. n. 67644, il Dipartimento delle Finanze e con nota del 20/12/2022, prot. MEF-DT n. 0102009/2022, il Dipartimento del Tesoro hanno espresso il proprio parere in ordine alla sottoscrizione della presente Convenzione;

VISTA la nota prot. MiTE n. 140492 del 10/11/2022 con la quale la Direzione generale USSRI ha informato il Dipartimento Amministrazione Generale, Pianificazione e Patrimonio Naturale (DiAG) che è in procinto di sottoscrivere una nuova Convenzione con Sogei S.p.A.;

VISTA la nota prot. MiTE n. 142347 del 15/11/2022 con la quale il dirigente della divisione V, Ing. Luciana Distaso, della Direzione generale uso sostenibile del suolo e delle risorse idriche, ha trasmesso l'Attestato di congruità sulla convenienza economica dell'Offerta tecnico - economica presentata dalla Sogei S.p.A., ai sensi dell'articolo 192, comma 2, del Codice dei contratti pubblici;

VISTO il decreto direttoriale USSRI n. 306 del 16/11/2022, pubblicato sul sito web del Ministero, con il quale è stata adottata la Determina a contrarre, ai sensi dell'art. 32 del succitato Decreto Legislativo 18 aprile 2016, n. 50, per l'affidamento diretto alla Società Generale d'Informatica – Sogei S.p.A., dello sviluppo di una piattaforma web per la realizzazione dell'iniziativa di cui Bonus Ambiente e la gestione delle attività ad essa connesse;

TUTTO CIO' PREMESSO
SI CONVIENE E SI STIPULA QUANTO SEGUE

ARTICOLO 1
OGGETTO E DURATA E MASSIMALE

1. Le premesse e gli allegati alla presente Convenzione formano parte integrante e sostanziale della stessa.

2. La presente Convenzione ha per oggetto lo svolgimento da parte di SOGEI dei servizi di cui al successivo articolo 2, meglio descritti nell'Allegato "A" "Descrizione Servizi, Livelli di Servizio e corrispettivi" che la SOGEI esegue secondo le modalità e nei tempi riportati nell'Allegato "B" "Piano Operativo 2022/2023".

3. La presente Convenzione regola il rapporto tra il MASE e la SOGEI, a decorrere dalla data di registrazione dello stesso da parte degli organi di controllo e fino al 31 dicembre 2023.

4. La presente Convenzione è vincolante per la SOGEI dalla data di sottoscrizione, mentre esplicherà la sua efficacia per il MASE solo a seguito della formale registrazione da parte del competente Organo di Controllo anche in ordine all'impegno delle necessarie somme sui capitoli di spesa per competenza.

5. Resta inteso che il MASE comunicherà tempestivamente per iscritto alla SOGEI la data in cui si saranno verificate le condizioni di legge di cui al precedente comma 4.

6. L'importo della presente Convenzione è determinato nella cifra complessiva massima prevista pari ad € 219.587,34 (duecentodicianovemilacinquecentoottantasette /34), oltre l'IVA, per un importo complessivo di € 267.896,56 (duecentosessantasettemilaottocentonovantasei/56).

7. La tabella riportante la ripartizione dell'importo complessivo, di cui al precedente comma 6, è riportata nell'Allegato "B" alla presente Convenzione e potrà essere modificata, di comune accordo, mediante il solo scambio di corrispondenza fermo restando l'importo massimale dell'intera durata contrattuale.

8. Qualora le variazioni di cui al precedente comma 7, rendano necessaria la modifica dell'importo massimale di cui al precedente comma 6, le Parti provvederanno alla stipula di appositi atti aggiuntivi.

ARTICOLO 2
SERVIZI

1. Nell'esecuzione della presente Convenzione la SOGEI erogherà i Servizi indicati nell'Allegato B alla presente Convenzione. La descrizione dettagliata dei Servizi, i relativi corrispettivi e Livelli di servizio sono definiti nell'Allegato A alla presente Convenzione.
2. I Servizi di cui al precedente comma 1, saranno remunerati sulla base dei corrispettivi stabiliti con il parere AGID numero 12/2020, citato in premessa.
3. La SOGEI si impegna, a richiesta del MASE, a fornire ad altre Pubbliche Amministrazioni, centrali o locali, nel rispetto della normativa vigente e delle norme statutarie applicabili, servizi che consentano il riuso delle applicazioni software di cui al presente articolo ovvero delle soluzioni progettuali adottate nell'ambito del Sistema Informativo, a condizioni economiche e contrattuali da definire di comune accordo tra le Parti.

ARTICOLO 3
GARANZIE

1. La SOGEI assume in proprio ogni responsabilità, per tutta la durata della Convenzione, per qualsiasi danno direttamente causato a persone o beni, tanto della SOGEI quanto del MASE, in dipendenza di omissioni, negligenze e/o altre inadempienze relative all'esecuzione delle prestazioni contrattuali a esso riferibili, anche se eseguite in tutto o in parte da terzi nei limiti del valore della presente Convenzione.
2. La SOGEI si impegna a porre in essere tutte le attività necessarie per garantire che i programmi utilizzati per l'esecuzione dell'attività siano esenti da virus nonché a realizzare ogni e qualsiasi opportuna attività atta a porre efficacemente rimedio nel caso in cui i programmi non siano esenti da virus.
3. Le suddette garanzie sono prestate in proprio dalla SOGEI anche per il fatto del terzo, rimanendo il MASE del tutto estraneo ai rapporti tra la SOGEI e le ditte fornitrici.
4. Con riferimento ai precedenti commi 2 e 3, la SOGEI si obbliga a provvedere anche alla rimozione di ogni e qualsiasi errore alla stessa direttamente imputabili.

ARTICOLO 4
RAPPORTI PERIODICI

1. La SOGEI darà conto del servizio erogato mediante appositi Rapporti Periodici, ovvero con relazioni quadrimestrali sullo stato di avanzamento delle attività e della spesa nel periodo di riferimento, secondo lo schema di cui all'allegato "C", denominato "Schema Rapporto Periodico", che riportano i dati di preventivo e i consuntivi.
2. I Rapporti Periodici con cadenza quadrimestrale verranno trasmessi dalla SOGEI al MASE, entro 25

(venticinque) giorni dalla fine del periodo di riferimento, fermo restando che il Rapporto Periodico relativo all'ultimo quadrimestre dell'anno di riferimento sarà inviato entro 45 (quarantacinque) giorni dal termine del quadrimestre stesso.

3. Il MASE verificherà, in sede di esame del Rapporto periodico, che le prestazioni oggetto della presente Convenzione siano state erogate, sotto il profilo degli obiettivi, delle caratteristiche tecniche, economiche e qualitative, in conformità alle previsioni della Convenzione e dei suoi allegati.

4. Il MASE concluderà la verifica di ciascun Rapporto Periodico entro 30 (trenta) giorni lavorativi dalla trasmissione dello stesso da parte della SOGEI, a seguito del quale la stessa provvederà ad emettere fattura elettronica indirizzata al codice IPA – Codice Univoco Ufficio Y9YZWM

ARTICOLO 5
LIVELLI DI SERVIZIO E PENALI

1. I livelli dei Servizi di cui al precedente articolo 2 che la SOGEI dovrà conseguire quadrimestralmente e l'importo delle penali da applicare, in caso di loro mancato conseguimento, sono dettagliatamente descritti nell'allegato "A" alla presente Convenzione.

2. Le penali potranno essere applicate dal MASE previa contestazione scritta dell'addebito e previa valutazione delle deduzioni al riguardo addotte dalla SOGEI che dovranno essere presentate non oltre il termine di 30 (trenta) giorni dal ricevimento della comunicazione contenente la contestazione stessa.

3. Il MASE, valutate le predette deduzioni, potrà decidere di dare corso all'applicazione delle penali dandone comunicazione scritta alla SOGEI non oltre il termine di 30 (trenta) giorni dal ricevimento delle deduzioni.

4. La SOGEI provvederà a pagare al MASE l'importo della penale indicata nella comunicazione di cui al precedente comma 2. Le Parti si danno peraltro atto che, qualora la SOGEI ritenga di non condividere le conclusioni del MASE, il pagamento di cui sopra non potrà costituire in nessun caso riconoscimento di responsabilità e/o di debito ove la SOGEI dia inizio alla procedura di cui al successivo articolo 14 entro 60 (sessanta) giorni dal pagamento stesso.

ARTICOLO 6
ESONERO DELLA SOGEI DA RESPONSABILITÀ

1. Fermo restando quanto stabilito al precedente articolo 3, la SOGEI non è responsabile per ritardi o impossibilità nello svolgimento delle attività, dovuti a cause ad essa non imputabili; in particolare, la SOGEI non può essere ritenuta responsabile per fatti o circostanze dipendenti, derivanti da o comunque connessi con:

   a. l'inadempimento di prestazioni o l'inattività o il ritardo nell'espletamento di attività non affidate alla SOGEI nell'ambito della presente Convenzione;

b. eventi fortuiti o causa di forza maggiore.

ARTICOLO 7
REFERENTI PER LA GESTIONE DELLA CONVENZIONE E COMUNICAZIONI

1. Entro 15 (quindici) giorni successivi alla sottoscrizione della presente Convenzione, il MASE e la SOGEI nominano ciascuna un proprio referente per la gestione dello stesso. Il referente della SOGEI indicato sarà Responsabile unico delle attività convenzionali (RUAC) per l'intero periodo di esecuzione della Convenzione. A questo il MASE farà riferimento per gli aspetti generali, o interpellerà per ogni problema riguardante la fornitura stessa. Tra i compiti del Responsabile della SOGEI rientrano tra l'altro, a titolo esemplificativo e non limitativo, i seguenti: organizzare, programmare e dirigere l'esecuzione delle attività oggetto della presente Convenzione conformemente ai contenuti dello stesso e dei relativi allegati e delle eventuali richieste dal Referente del MASE avanzate in conformità a quanto previsto nei citati documenti. Il Responsabile della SOGEI, ai sensi della normativa vigente in materia di sicurezza, sarà preposto alla direzione del servizio, assumendone le responsabilità dell'andamento. Il Responsabile della SOGEI deve inoltre garantire, nei casi eccezionali di criticità e di urgenza, le necessarie sinergie e la soluzione tempestiva delle problematiche; gestire le criticità e i rischi complessivi di progetto risolvendo tutti i potenziali conflitti e/o eventuali disservizi; riferire proattivamente sull'ottimale e costante dimensionamento, in quantità e qualità, del team impiegato.
2. L'effettuazione delle comunicazioni richieste o da effettuarsi in relazione alla presente Convenzione, ivi comprese eventuali contestazioni, avverrà tramite l'utilizzo della posta elettronica certificata.
3. Gli indirizzi PEC presso i quali le *Parti* eleggono domicilio sono: per la SOGEI: protocollosogei@pec.sogei.it, per il MASE: USSRI@PEC.mite.gov.it.

ARTICOLO 8
CORRISPETTIVI E FATTURAZIONE

1. I corrispettivi contrattuali per i Servizi di cui al precedente articolo 2 sono riportati nell'allegato "A".
2. La SOGEI, nell'ambito dell'importo complessivo di cui al precedente articolo 1, comma 6, procederà quadrimestralmente, alla fatturazione sulla base dei servizi erogati riportati nei singoli Rapporti Periodici di cui al precedente articolo 4, acquisita la preventiva autorizzazione del MASE all'emissione della fattura secondo quanto definito all'articolo 4, comma 4.
3. Per i crediti derivanti dall'applicazione delle penali di cui alla presente Convenzione, il MASE potrà compensare il credito con quanto dovuto alla SOGEI. La richiesta e/o il pagamento delle penali di cui alla presente Convenzione non esonera in nessun caso la SOGEI dall'adempimento dell'obbligazione per la quale il MASE ritiene si sia resa inadempiente e che ha fatto sorgere, a parere del MASE, l'obbligo di pagamento della medesima penale.

ARTICOLO 9
PAGAMENTO

1. Entro 30 (trenta) giorni lavorativi dal ricevimento di ciascuna fattura, il MASE provvede a effettuare il relativo mandato di pagamento.

2. I pagamenti sono effettuati mediante bonifico bancario sul conto corrente contraddistinto dal codice IBAN IT59M0200805364000030008189, intestato alla SOGEI e che la stessa società dichiara, nella persona del suo legale rappresentante o di altro soggetto dotato di idonei poteri di rappresentanza, essere dedicato alle transazioni di commesse pubbliche ai sensi dell'articolo 3, comma 1, della Legge 13 agosto 2010 n. 136.

3. La SOGEI, sotto la propria esclusiva responsabilità, si impegna a rendere tempestivamente note al MASE eventuali variazioni relative alle coordinate bancarie di cui al precedente comma. In assenza di tali notificazioni, la SOGEI esonera il MASE da ogni responsabilità per i pagamenti eseguiti.

ARTICOLO 10
SICUREZZA DEL SISTEMA

1. Tenuto conto dei livelli di servizio richiesti, la SOGEI in collaborazione con il MASE dovrà operare attraverso l'adozione di idonee misure organizzative, tecniche e operative nel rispetto dei concordati livelli di sicurezza del sistema, come previsti nell'allegato "A".

ARTICOLO 11
TRATTAMENTO DEI DATI

1. Le Parti si impegnano a rispettare le disposizioni normative vigenti in materia di protezione dei dati personali, con particolare riguardo all'adozione di idonee misure di sicurezza, e a farle osservare ai propri dipendenti e collaboratori che, opportunamente istruiti, saranno autorizzati al trattamento dei dati personali.

2. Le finalità e le modalità del trattamento dei dati personali devono conformarsi ai principi di necessità e di legalità, nonché agli altri principi e regole contenute nel Regolamento UE 2016/679. Inoltre, il trattamento dei dati personali verrà effettuato dalle Parti in modo tale da garantire la sicurezza e la riservatezza necessarie e potrà essere attuato mediante strumenti manuali, cartacei, informatici e telematici idonei a trattare i dati nel rispetto della normativa vigente in materia di protezione dei dati personali.

3. Il MASE tratta i dati forniti dalla SOGEI, ai fini della stipula della Convenzione, per l'adempimento degli obblighi legali ad esso connessi, oltre che per la gestione ed esecuzione economica ed amministrativa della Convenzione stessa. Tutti i dati acquisiti dal MASE potranno essere trattati anche per fini di studio e statistici.

4. Con la sottoscrizione della presente Convenzione, i legali rappresentanti pro-tempore delle Parti acconsentono espressamente al trattamento dei propri dati personali.

5. La SOGEI 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 MASE (www.mite.gov.it) nella sezione relativa alla trasparenza.

6. Il MASE, con la sottoscrizione dell'allegato "D" denominato "Atto di designazione del responsabile del trattamento" alla presente Convenzione, nomina la SOGEI Responsabile esterno del trattamento dati ex art. 28 del Regolamento Europeo n. 2016/679 in conformità a quanto previsto dall'art. 3, comma 4, del citato Regolamento.

ARTICOLO 12
RISERVATEZZA

1. La SOGEI si obbliga a non divulgare in alcun modo e forma le notizie – classificate dal MASE come riservate – relative alle attività dei sistemi informativi del MASE di cui il personale della stessa SOGEI venga a conoscenza in relazione all'esecuzione della presente Convenzione, ivi comprese le informazioni che transitano per le apparecchiature di elaborazione dei dati. Tale obbligo non sussiste per le notizie già note o di pubblico dominio.

2. La SOGEI si impegna, altresì, a prevedere, nella disciplina contrattuale che regola i rapporti con i fornitori a fare osservare anche a questi ultimi gli obblighi stabiliti dal Codice Etico.

3. Le predette notizie e informazioni, comprese quelle relative al software, non possono essere utilizzate dalla SOGEI e/o da chiunque collabori alle sue attività per fini diversi da quelli contemplati nella presente Convenzione. A tal fine, la SOGEI si obbliga ad adottare opportune misure volte a garantire la massima riservatezza sulle informazioni raccolte negli archivi dei sistemi informativi del MASE, nonché quelle necessarie a garantire la sicurezza fisica, logica e delle infrastrutture di rete dei Sistemi Informativi stessi.

4. Le statuizioni di cui al comma 3 del presente articolo riguardano tutto il materiale, originario o predisposto in esecuzione della presente Convenzione, che resta, comunque, di esclusiva proprietà del MASE, quale unico destinatario del servizio svolto.

ARTICOLO 13
PROPRIETÀ DEI RISULTATI

1. Le applicazioni software realizzate dalla SOGEI in attuazione della presente Convenzione e gli eventuali prodotti realizzati sono di proprietà del MASE.

2. Resta esclusa qualsiasi responsabilità del MASE nel caso in cui la SOGEI utilizzi, per l'esecuzione

delle attività previste nella presente Convenzione, dispositivi e soluzioni su cui altri siano titolari di diritti di privativa.

3. I diritti di proprietà e/o di utilizzazione e sfruttamento economico di tutti gli elaborati realizzati dalla SOGEI o da suoi dipendenti e collaboratori nell'ambito o in occasione dell'esecuzione del Servizio, rimarranno di titolarità ed esclusiva proprietà del MASE che potrà, quindi, disporne, senza alcuna restrizione, la pubblicazione, la diffusione, l'utilizzo, la duplicazione e la cessione anche parziale. Detti diritti, ai sensi della normativa sulla protezione del diritto d'autore, devono intendersi ceduti, acquisiti e/o licenziati in modo perpetuo, illimitato e irrevocabile.
4. La SOGEI assume ogni responsabilità conseguente all'uso di dispositivi o all'adozione di soluzioni tecniche o di altra natura che violino diritti di brevetto, di autore ed in genere di privativa altrui. La SOGEI, pertanto, si obbliga a manlevare il MASE, per quanto di propria competenza, dalle pretese che terzi dovessero avanzare in relazione a diritti di privativa vantati da terzi.
5. Qualora venga promossa nei confronti del MASE un'azione giudiziaria da parte di terzi che vantino diritti sulle applicazioni software realizzate dalla SOGEI, la SOGEI assume a proprio carico tutti gli oneri conseguenti, incluse le spese eventualmente sostenute per la difesa in giudizio.

ARTICOLO 14
RISOLUZIONE DELLE CONTROVERSIE

1 Nel caso di controversie di qualsiasi natura che dovessero insorgere tra le Parti in ordine alla interpretazione o all'applicazione della presente Convenzione, o comunque direttamente o indirettamente ad esso connesse, ove non sia stato possibile comporre bonariamente fra i referenti delle Parti di cui al precedente articolo 7, ciascuna Parte comunicherà per iscritto all'altra l'oggetto ed i motivi della contestazione.

2 Al fine di comporre bonariamente la controversia, le Parti si impegnano a esaminare congiuntamente la questione, entro il termine massimo di cinque giorni dalla data di ricezione della contestazione, e a pervenire ad una composizione entro il successivo termine di dieci giorni.

3 Resta, peraltro, inteso che le controversie in atto non pregiudicheranno in alcun modo la regolare esecuzione delle attività della presente Convenzione, né consentiranno se non per concordate ragioni gravi e rilevanti alcuna sospensione delle prestazioni dovute dall'una e dall'altra Parte, fermo restando che riguardo le questioni oggetto di controversia le Parti si impegnano a concordare di volta in volta, in via provvisoria, le modalità di parziale esecuzione che meglio possano garantire il pubblico interesse e il buon andamento dell'attività amministrativa.

4 In caso di mancata composizione bonaria, la controversia è devoluta alla competenza del Foro di Roma.

ARTICOLO 15
DISPOSIZIONI IN MATERIA DI ANTICORRUZIONE

1 Le *Parti* si impegnano all'osservanza delle vigenti disposizioni e degli obblighi di legge in materia di prevenzione della corruzione e della integrità e trasparenza degli atti. La SOGEI si impegna, in particolare, a dare piena attuazione al sistema di prevenzione della corruzione e della trasparenza ed integrità degli atti, secondo un modello integrato con quello previsto dal d.lgs. n. 231/2001 e ss.mm.ii., nonché all'osservanza delle particolari disposizioni impartite dal Ministero dell'Economia e delle Finanze e dall'Autorità Nazionale Anticorruzione relativamente alle società partecipate dal predetto Ministero dell'Economia e delle Finanze.

ARTICOLO 16
ESONERO DALLA CAUZIONE

1. La SOGEI è esonerata dall'obbligo di prestare cauzione poiché il Ministero dell'Economia e delle Finanze ne è azionista unico e in quanto trattasi di un organismo di diritto pubblico che opera nell'interesse e per conto delle Amministrazioni Pubbliche nel settore dei servizi informatici e dell'innovazione nella Pubblica Amministrazione.

ARTICOLO 17
ONERI E SPESE CONTRATTUALI

1. Sono a carico della SOGEI le spese relative alla presente Convenzione, ad eccezione di quelle che, per legge, cedono a carico del MASE.
2. A tal fine la SOGEI dichiara che le prestazioni di cui alla presente Convenzione sono effettuate nell'esercizio di impresa e che trattasi di operazioni imponibili non esenti dall'IVA e soggette al trattamento previsto dall'art. 17-ter del D.P.R. 26 ottobre 1972, n. 633, e successive modificazioni. Di conseguenza, alla presente Convenzione dovrà essere applicata l'imposta di registro in misura fissa, ai sensi dell'articolo 40 del D.P.R. 26 aprile 1986, n. 131, e successive modificazioni.

ARTICOLO 18
COMPOSIZIONE DELLA CONVENZIONE E VALORE DEGLI ALLEGATI

1. La presente Convenzione si compone di n. 18 articoli e di n. 4 allegati, di cui al seguente comma 2, che, sottoscritti digitalmente dalle Parti, ne costituiscono parte integrante e sostanziale.
2. Vengono allegati alla presente Convenzione i seguenti documenti:
   - "A": "Descrizione Servizi, Livelli di servizio e corrispettivi".
   - "B": "Piano Operativo 2022/2023"
   - "C": "Schema Rapporto Periodico"

"D": "Atto di designazione del responsabile del trattamento".

Ministero
dell'Ambiente e della Sicurezza Energetica
Direzione Generale uso sostenibile
del suolo e delle risorse idriche
(Dott. Giuseppe Lo Presti)
Firmato digitalmente

SOGEI
Società Generale d'Informatica S.p.A.
L'Amministratore Delegato
(Dott. Andrea Quacivi)
Firmato digitalmente

FLUSSO DI NOTIFICA DI *DATA BREACH*

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 della notifica di avvenuto *Data Breach* all'Amministrazione Titolare affinché quest'ultima possa adempiere agli obblighi previsti dagli articoli 33 e 34 del RGPD.

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'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". Il CERT Sogei comunica 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 USSRI@pec.mite.gov.it, ITC@pec.mite.gov.it e rpd@pec.minambiente.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" 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 all'incidente.

- 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, comunicando 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 è stata accertata la "violazione di dati personali" ed è stata valutata la gravità dell'evento da intendersi come la stima del potenziale impatto sugli interessati derivante dalla violazione), 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. La suddetta comunicazione viene inviata dalla casella PEC del CERT Sogei (cert@pec.sogei.it) verso le caselle PEC dell'Amministrazione Titolare e del RPD della stessa o, laddove non disponibili, verso le caselle di posta elettronica ordinaria di questi ultimi.
- l'Amministrazione Titolare, ricevuta la notifica di *Data Breach* e sentito il proprio RPD, valuta il livello di gravità della "violazione di dati personali" proposto da Sogei. Nel caso in cui la "violazione di 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'incidente, 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 al CERT Sogei.

2. CONTENUTI DELLA NOTIFICA DI DATA BREACH ALL'AMMINISTRAZIONE TITOLARE

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

Il CERT Sogei utilizzerà il modulo disponibile sul sito dell'Autorità di Controllo per fornire le informazioni necessarie all'Amministrazione Titolare, comprendenti almeno le seguenti:

- 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.

CONVENZIONE

PER LA REALIZZAZIONE DELLA PIATTAFORMA RELATIVA ALL'INIZIATIVA BONUS AMBIENTE E LA GESTIONE DELLE ATTIVITÀ AD ESSA CONNESSE

ALLEGATO A

DESCRIZIONE DEI SERVIZI, LIVELLI DI SERVIZIO E CORRISPETTIVI

INDICE

1. PREMESSA

Nel presente allegato, parte integrante e sostanziale alla presente Convenzione stipulata tra Sogei e l'Amministrazione, vengono definiti i Servizi erogati, i relativi corrispettivi ed i Livelli di servizio da garantire.

Il rapporto contrattuale prevede da parte di Sogei l'erogazione di servizi corredati di facility che ne consentano la piena fruibilità in termini di sicurezza, monitoraggio e integrazione.

In tale contesto Sogei si pone come responsabile di tutti gli aspetti applicativi, tecnologici, architetturali, di qualità e di sicurezza dell'intero Sistema Informativo, operando le scelte più opportune in base alle esigenze dell'Amministrazione.

L'Amministrazione si configura come fruitore dei servizi di cui ha fatto richiesta monitorando la loro erogazione.

Per Servizio ICT si intende "*l'insieme di applicazioni informatiche omogenee e della relativa infrastruttura tecnologica, in grado di supportare lo svolgimento di un processo/sottoprocesso amministrativo e per le quali sia comunque opportuno esercitare il controllo/monitoraggio a livello di unica entità. Nei casi previsti dalla normativa (GDPR) può essere collegato ad uno o più "trattamento" dei dati*"

Per gli indicatori relativi ai Servizi vengono realizzati sistemi di rilevazione specifici normalmente disponibili dal secondo quadrimestre di erogazione del servizio stesso; a riguardo si specifica che:

- la rilevazione è per tutti su base quadrimestrale a meno che diversamente specificato;

- la rilevazione di alcuni LDS potrebbe richiedere un periodo di osservazione e/o di sviluppo della modalità di rilevazione stessa;
- nei casi in cui si verifichi un fermo di Servizio concordato con l'Amministrazione, la fascia temporale corrispondente verrà esclusa ai fini del calcolo dei Livelli di servizio stessi.

Termini/Definizioni dei Livelli di servizio

Si riportano nel seguito i termini e le definizioni di riferimento utilizzati nelle descrizioni dei Livelli di servizio relativi ai prodotti/servizi forniti.

- Arrotondamenti
  - ai fini del calcolo dello scostamento tra le percentuali effettive e quelle contrattuali le prime devono essere arrotondate:
  - nel caso di aumenti o riduzione dello 0,1%, si arrotonda allo 0% per scostamenti compresi tra lo 0,000% e lo 0,049% ed allo 0,1% per scostamenti superiori;
  - nel caso di aumenti o riduzioni dell'1%, si arrotonda allo 0% per scostamenti compresi tra lo 0,00% e lo 0,49% ed all'1% per scostamenti superiori.
  - ai fini del calcolo delle ore di ritardo, le frazioni sono così arrotondate:
  - da 1 a 29 minuti: zero ore;
  - da 30 a 59 minuti: 1 ora.
- Errore software - si considera un errore software ogni

intervento correttivo sul software innescato da uno o più problemi. Verranno considerati tutti i problemi segnalati, sullo strumento utilizzato per tracciatura del servizio di assistenza alla data di completa distribuzione della versione corretta del software. Resta inteso che più segnalazioni relative allo stesso problema software vengono considerate una sola volta ai fini del conteggio nel livello di servizio.

La modalità di rilevazione degli errori sarà definita dalla "Procedura di rilevazione dell'errore" che sarà fornita all'Amministrazione.

- Finestra Temporale di erogazione del servizio - arco di tempo in cui il servizio deve essere erogato; i livelli di servizio sono calcolati sugli orari di erogazione dei servizi oggetto del presente documento, salvo diversa esplicita indicazione.
- Giorni - giorni lavorativi, salvo ove espressamente indicato.
- Ore - ore lavorative ovvero ore ricadenti nella finestra temporale di erogazione, salvo diversa esplicita indicazione (festivi esclusi a meno del riferimento ad H24).
- Periodo di osservazione contrattuale - arco di tempo a cui è relativa la misurazione dei livelli di servizio. Viene fissata su base quadrimestrale.

In caso di violazione di Livelli di servizio che riguardino obiettivi per i quali siano previsti valori di soglia incrementali, verrà applicata esclusivamente la penale che si

riferisce al valore più alto riscontrato.

2. SERVIZI PROFESSIONAL

Il Servizio comprende l'insieme di attività professionali di Supporto ai clienti su tematiche di natura organizzativa, istituzionale, di innovazione e operativa nonché nell'ambito dell'iter di acquisizione.

I Servizi di Supporto e Governance, indipendentemente dal contesto in cui sono erogati, prevedono il ricorso a risorse con diverse professionalità che possono essere identificate nelle seguenti figure professionali:

- **Operativa:** personale con competenze e professionalità "tecniche" e padronanza sulla materia di competenza su cui viene coinvolto.
- **Specialistica**: personale con competenze di alto livello su specifiche filiere "tecniche" e che esprime piena padronanza sulle conoscenze tecnico-professionali di ruolo, agendo anche come punto di riferimento operativo per gli specialisti impegnati nei processi di interesse.
- **Di coordinamento**: personale il cui profilo è finalizzato ad assicurare il raggiungimento di importanti risultati tecnici, economici e qualitativi attraverso il coordinamento di risorse e progetti complessi. Governano programmi e progetti, relazioni organizzative interne ed esterne articolate, e rapporti fiduciari e negoziali con i clienti.

Nell'ambito dei Servizi Professional viene offerto il mix di competenze e professionalità più opportuno sulla base del tipo di supporto richiesto dall'Amministrazione, condiviso con la stessa; l'impegno economico che ne deriva sarà

calcolato sulla base della tipologia di professionalità richiesta.

2.1 *SUPPORTO*

Il Servizio di supporto offerto può essere erogato nei contesti di seguito descritti:

- Contesto organizzativo
  - nelle attività di certificazione di qualità dei processi operativi dei clienti e per le indagini di customer satisfaction;
  - nelle metodologie di progettazione e conduzione di un sistema di ascolto dell'utente;
  - nella partecipazione a commissioni, gruppi di lavoro e seminari;
  - nell'assistenza anche telefonica non informatica.
- Contesto istituzionale
  - nello svolgimento dei compiti istituzionali di competenza dei clienti attraverso il trattamento ottimale delle informazioni presenti nel Sistema informativo;
  - nella individuazione di soluzioni finalizzate all'attuazione della normativa di riferimento dell'Amministrazione;
  - nelle attività per lo scambio di informazioni fra i Clienti e tra queste ed i cittadini;
  - nella gestione degli aspetti amministrativi e gestionali di specifici programmi e/o progetti finanziati con fondi europei;

- Contesto di innovazione
    - nella produzione di documentazione tecnica e prototipi di soluzioni innovative;
    - nella progettazione, implementazione e attuazione delle misure di sicurezza dei sistemi informativi di responsabilità nonché di quelle relative alla qualità del sistema informativo;
    - nella progettazione e implementazione di architetture e applicazioni particolarmente innovative.
- Contesto Operativo
    - nella formazione e tutoraggio, nonché addestramento all'uso dei servizi informatici;
    - nell'attivazione tecnica delle apparecchiature acquisite nonché nell'attivazione funzionale delle soluzioni realizzate, presso le sedi dei clienti;
    - nelle attività operative specifiche di settore dei singoli clienti;
    - nell'assistenza tecnica periferica;
    - nei servizi accessori di assistenza.

2.2 *GOVERNANCE*

Il Servizio di Governance può essere erogato nei contesti di seguito descritti:

- Governance degli approvvigionamenti – comprende le attività necessarie per l'acquisizione, attraverso il ricorso al mercato, di beni e servizi a rimborso tesi al soddisfacimento dei bisogni dell'Amministrazione

relativi allo sviluppo, alla evoluzione ed alla conduzione del Sistema Informativo;

- Governance dei Contratti - comprende le attività necessarie a supportare l'Amministrazione nell'attuazione delle varie fasi dei processi di pianificazione pluriennale, di programmazione annuale, di controllo e di monitoraggio per garantire il governo dei processi di gestione del Contratto, per gli aspetti specifici derivanti dai processi dell'Amministrazione.

3. PROGETTAZIONE E SVILUPPO SERVIZI ICT

Include i servizi finalizzati allo sviluppo, modifica, evoluzione e personalizzazione di soluzioni innovative rispondenti alle esigenze dei clienti.

Per l'erogazione del Servizio la Sogei adotta un Processo di produzione proprietario standardizzato, certificato secondo le norme ISO 9001:2015 e conforme con la normativa ISO 27001:2013, e ISO 25012:2014 in materia di controlli sulla sicurezza e qualità dei dati nonché alle regole introdotte dal GDPR.

Tale processo è basato sui modelli metodologici di sviluppo Evolutivo/Incrementale, RUP – Rational Unified Process e Agile applicati in funzione dei contesti di sviluppo per ottimizzare i fattori produttivi e gestionali.

La Sogei opera nell'ambito dell'Application Lifecycle Management (ALM) che identifica un approccio strategico alla gestione delle informazioni, dei processi e delle risorse a supporto del ciclo di vita delle applicazioni software.

La Manutenzione migliorativa sarà considerata parte integrante dell'effort di sviluppo e manutenzione evolutiva in quanto attività essenziale per il raggiungimento della qualità attesa nel software prodotto.

3.1 *PERSONALIZZAZIONE DEL SOFTWARE DI MERCATO*

Il Servizio è finalizzato alla realizzazione di soluzioni basate su parametrizzazione e personalizzazione di pacchetti software acquistati sul mercato.

La Sogei applica tale servizio in caso di:

- personalizzazione/parametrizzazione di prodotti software di mercato (con particolare riferimento ai sistemi ERP - Enterprise Resource Planning);
- realizzazione di interventi di Data Warehouse (DW) e business intelligence (B.I.).

In particolare, il servizio di personalizzazione del software di mercato consiste in:

- sviluppo residuale di funzioni fortemente integrate con il prodotto nell'ambito del quale la personalizzazione viene effettuata che comporta la conoscenza del prodotto e dell'eventuale linguaggio proprietario;
- interventi effettuati su prodotti con tecnologie/linguaggi non dimensionabile correttamente attraverso l'uso del FP (ad esempio BI).

Gli sviluppi esterni al prodotto che ne consentono l'estensione in termini di funzionalità, sono invece considerati sviluppi ad hoc e come tali dimensionati e remunerati.

Tale servizio viene erogato attraverso un processo di produzione che:

- parte da un'analisi comparativa, tra il prodotto base ed i requisiti dell'utente (gap-analisys), volta ad evidenziare quali requisiti non sia possibile soddisfare mediante l'attività di parametrizzazione e per i quali di conseguenza occorrerebbero degli interventi di personalizzazione;
- si sviluppa in attività progressive di affinamento di un modello iniziale standard;

- condivide con l'Amministrazione ogni attività di affinamento;
- utilizza estensivamente un approccio prototipale.

Per quanto riguarda gli interventi di Datawarehouse e BI il servizio prevede l'utilizzo di specifiche tecnologie quali i tool di modellazione dei dati, gli strumenti di gestione dei metadati (Repository), i tool di ETL, gli strumenti di visualizzazione oltre che la realizzazione di software dedicato.

Indipendentemente dalle tecnologie adottate, il processo presenta caratteristiche omogenee relativamente all'articolazione in fasi (analisi dei requisiti, attuazione, avviamento, verifica di confromità) e alla documentazione prodotta a supporto.

Sogei garantisce che le personalizzazioni si integrino correttamente con il prodotto di base e segnalerà anticipatamente all'Amministrazione se, l'intervento richiesto, in fase di realizzazione facesse emergere problematiche in tal senso.

Per un periodo di 365 (trecentosessantacinque) giorni solari, decorrenti dalla data di inizio estensione delle applicazioni software, la Sogei è impegnata a prestare, a propria cura e spese, la manutenzione correttiva delle personalizzazioni effettuate.

3.1.1 *Livelli di Servizio*

Servizio	Personalizzazione del software di mercato		
Livelli di Servizio	Soglia	Penale	
Difettosità alla prima	0 errori rispetto ai casi di	€ 300,00 per ogni	

Servizio	Personalizzazione del software di mercato		
Livelli di Servizio	Soglia	Penale	
verifica di conformità	test previsti nel piano di test	errore riscontrato	
Mantenimento data di "Disponibilità alla Verifica di conformità" condivisa con l'Amministrazione	10 giorni dalla data di consegna del software condivisa con l'Amministrazione	€ 250,00 per ogni giorno di ritardo successivo al decimo e sino al trentesimo giorno	
		€ 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	

Le date di "Disponibilità alla Verifica di Conformità" di riferimento per il LdS vengono definite inizialmente nel Piano operativo condiviso e approvato tra le Parti e successivamente possono essere modificate mediante scambio di comunicazione.

4. SERVIZI DI GESTIONE E CONDUZIONE

La gestione dei sistemi include le attività necessarie per condurre, mantenere funzionante ed aggiornata l'infrastruttura hardware e software utilizzata per l'erogazione di più servizi informatici. Questo insieme di Servizi si identifica come la gestione dell'esercizio dei sistemi la cui criticità necessita di essere garantita h24x365 e con reperibilità, interventi festivi e notturni, per mantenere la piena efficienza anche a fronte di problematiche.

Riguarda questa classe di servizi l'insieme degli investimenti, costi, risorse, infrastrutture che concorrono a garantire la conduzione, lo sviluppo tecnologico e l'erogazione dei servizi ICT ospitati nel Data Center Sogei o che usufruiscono anche di piattaforme esterne (cloud) comunque gestite e selezionate da Sogei.

Si precisa che il buon funzionamento di Server, Storage è misurato attraverso livelli di servizio i cui i indicatori (tempi di disponibilità) si intendono riferiti ai Servizi ICT erogati su tali piattaforme:

Livelli di Servizio	Soglia	Penale	Orario di osservazione
Disponibilità del Servizio ICT erogato attraverso l'infrastruttura sottostante	99,0%	€ 1.250,00 per ogni decimo di punto percentuale di diminuzione rispetto al valore prefissato	H24

4.1 *SERVER*

La Conduzione centrale – Server comprende la conduzione tecnico operativa e sistemistica del componente Server dei sistemi open centrali, incluse le attività relative alla sicurezza e alla rete in ambiente Open centrale.

La struttura dei servizi, inclusi nel driver SERVER, si può suddividere in:

- Infrastrutture IT,
- Piattaforme & DATI,
- Applicazioni.

Infrastrutture IT

Comprende la gestione dei sistemi sino al sistema operativo e le relative componenti di base in termini di configurazione e tuning, redazione di procedure di controllo, allestimento e gestione di ambiti virtuali, produzione di report analitici sull'operatività degli ambienti, ecc.).

Rientrano nel servizio le piattaforme hardware a supporto, nonché le attività di predisposizione delle infrastrutture server fino all'hypervisor, ove presente, per tutte le tipologie di sistemi e le relative componenti software di base al di fuori di quelle che rientrano nell'ambito del servizio IAM e Appliance.

Sono incluse inoltre tutte le licenze software di base, del sistema operativo, dell'hypervisor, dei gestori di volumi, delle componenti di alta affidabilità, dei software di automazione e di tutte le componenti necessarie al provisioning e configurazione dei sistemi, nonché le attività ad essi correlate di configurazione, mantenimento ed evoluzione.

Si aggiungono a queste tutte le componenti legate alla parte di connettività e di sicurezza. Sono incluse in questo ambito anche tutte le componenti ed i servizi relativi a strumenti di automazione, software defined, orchestrazione etc, che concorrono all'erogazione dei servizi di infrastruttura (di tipo IaaS) secondo modelli di tipo 'cloud'.

Sono inoltre incluse tutte le componenti tecnologiche hw e sw ed i relativi servizi associati, per il controllo ed il monitoraggio delle componenti infrastrutturali.

Tale monitoraggio è organizzato e strutturato, secondo il paradigma ITIL, in una Service Control Room che contempla tutti i tre livelli in cui l'ambito server è qui 'descritto'.

Piattaforme & Dati

Comprende la gestione del middleware applicativo ovvero tutta la parte costituita da Application Server o analoghi in cui fisicamente venga collocato il codice applicativo, nonché i vari prodotti a supporto. Sono incluse in questo ambito anche tutte le componenti ed i servizi relativi a strumenti di automazione, software defined, orchestrazione etc, che concorrono all'erogazione dei servizi di piattaforma secondo modelli di tipo 'cloud'.

Alla gestione di questi ambiti va aggiunto quanto necessario per quelli che concorrono all'erogazione complessiva dei servizi al di fuori dei classici tier della pila WEB: in particolare trattasi di sistemi di elaborazione destinati al trattamento dei dati ricevuti, soprattutto attraverso canali telematici.

Anche questo livello comprende l'area destinata al monitoraggio.

Applicazioni

Si tratta del livello più elevato della pila infrastrutturale a supporto delle applicazioni. Comprende i servizi di deploy strutturato delle applicazioni e tutte le attività ad esse correlate.

Anche questo livello comprende l'area destinata al monitoraggio: in particolare, rientrano qui le attività di analisi delle problematiche e delle ottimizzazioni.

L'orario del servizio è H24.

4.1.1 *Livelli di Servizio*

In caso in cui venga richiesto un orario H24 senza possibilità di prevedere fermi concordati, ne verrà valutata la fattibilità e attivato un apposito servizio PLATINUM remunerato sulla base delle risorse aggiuntive necessarie.

<table>
<tr><td>Servizio</td><td colspan="3">Server</td></tr>
<tr><td>Livelli di Servizio</td><td>Soglia</td><td>Penale</td><td>Orario di osservazione</td></tr>
<tr><td>Disponibilità del Servizio ICT erogato attraverso l'infrastruttura sottostante (cpu, ram immagine)</td><td colspan="2">vedi tabella par. 4 “SERVIZI DI BASE DI GESTIONE, CONDUZIONE INFRASTRUTTURA”</td><td rowspan="2">H24</td></tr>
<tr><td>Tempi di risposta</td><td>I Servizi ICT oggetto di analisi e la relativa soglia, verranno definiti fra le Parti nel corso di definizione</td><td>€ 100,00 per ogni decimo di punto percentuale di diminuzione rispetto al valore prefissato</td></tr>
</table>

Servizio	Server		
Livelli di Servizio	Soglia	Penale	Orario di osservazione
	del Piano Operativo annuale e corrispondono ai requisiti espressi in fase di sviluppo/MEV.		

4.2 *STORAGE*

La Conduzione centrale – Storage riguarda la conduzione tecnico operativa e sistemistica del componente DISK STORAGE (inclusi Backup-Restore dei dati ed archiviazioni a medio lungo termine) per gli ambienti OPEN, garantendo la massima disponibilità, anche mediante tecnologia RAID.

Nella gestione delle banche dati vengono utilizzate tecnologie, architetture e modalità operative per assicurare la costante disponibilità dei dati e del servizio, anche in caso di possibili eventi disastrosi.

Accanto alla copia on-line su disco viene resa disponibile anche una copia su nastro o su disco specializzato - Backup. Il servizio mette a disposizione sia l'infrastruttura che l'esercizio e la conduzione della stessa.

L'orario del servizio è H24.

4.2.1 ***Livelli di Servizio***

Servizio	Storage		
Livelli di Servizio	Soglia	Penale	Orario di osservazione
Disponibilità del servizio erogato dall'infrastruttura sottostante (GB)	vedi tabella par. 4 “SERVIZI DI BASE DI GESTIONE, CONDUZIONE INFRASTRUTTURA”		H24

5. CORRISPETTIVI

SERVIZI PROFESSIONAL		
Servizio	CORRISPETTIVI	Euro/giorno
Professional (Supporto e Governance)	Servizio di Coordinamento	800
	Servizio Specialistico	502
	Servizio Operativo	362

Il Servizio può essere remunerato secondo due modalità:

- se le attività di supporto richieste rivestano natura progettuale e sono identificabili output concreti oggetto di consegna, l'obiettivo sarà dimensionato secondo le tariffe della tabella precedente e l'importo complessivo derivante sarà remunerato a fronte della consegna degli output definiti.
- se le attività di supporto rivestano natura occasionale verranno remunerate a Tempo e Spesa secondo le tariffe della tabella precedente.

SERVIZI DI SVILUPPO		
Servizio	CORRISPETTIVI	Euro/giorno
Personalizzazione prodotti di mercato	Personalizzazione prodotti di mercato	341,00

Il Servizio è dimensionato attraverso i corrispettivi di cui sopra applicati alle quantità stimate e alla modalità di remunerazione definite in fase di pianificazione delle attività.

GESTIONE E CONDUZIONE INFRASTRUTTURA		
Servizio	CORRISPETTIVI	Euro/mese
Server	Immagini	558,32
	vCPU	98,68
	vRAM	15,86
Storage	GB allocati	0,395

CONVENZIONE PER LA REALIZZAZIONE DELLA PIATTAFORMA RELATIVA ALL'INIZIATIVA BONUS AMBIENTE E LA GESTIONE DELLE ATTIVITÀ AD ESSA CONNESSE

ALLEGATO B - PIANO OPERATIVO 2022 E 2023

INDICE

1. OBIETTIVI

Il presente documento costituisce parte integrante e sostanziale della Convenzione tra il Ministero dell'Ambiente e della Sicurezza Energetica (MASE) e la Società Generale d'Informatica (Sogei S.p.A.) ed in particolare contiene la descrizione delle attività ed i servizi previsti nel Piano ed i relativi impegni economici per il periodo di vigenza della Convenzione.

La legge del 30 dicembre 2018 riconosce un credito d'imposta, nella misura del 65 per cento delle erogazioni effettuate, riconosciute nei periodi d'imposta successivi a quello in corso al 31 dicembre 2018, per erogazioni liberali per interventi su edifici e terreni pubblici di bonifica ambientale, di prevenzione e risanamento del dissesto idrogeologico e sistemazione di parchi e aree verdi di proprietà pubblica.

Il credito d'imposta è riconosciuto in tre quote ripartite annualmente di pari importo alle persone fisiche e agli enti non commerciali nei limiti del 20 per cento del reddito imponibile, nonché ai soggetti titolari di reddito d'impresa nei limiti del 10 per mille dei ricavi annui, anche qualora le erogazioni liberali in denaro siano destinate ai soggetti concessionari o affidatari dei beni oggetto degli interventi;

Le risorse a disposizione affinché venga riconosciuto il credito d'imposta, sono pari a:

- 5 milioni di euro per l'anno 2020;
- 10 milioni di euro per l'anno 2021;
- 10 milioni di euro per l'anno 2022.

Il piano ha come finalità l'implementazione e la gestione della piattaforma web che consente l'accoglimento e la pubblicizzazione delle iniziative finanziabili, nonché la gestione delle richieste di adesione al bonus e la comunicazione dei relativi esiti.

Il presente Piano Operativo ha validità da novembre 2022 fino al 31 dicembre 2023.

I Servizi descritti nei successivi paragrafi vengono erogati secondo le modalità, la remunerazione ed i corrispettivi definiti nell'allegato A alla presente Convezione denominato "Descrizione dei servizi, Livelli di servizio e Corrispettivi".

2. SVILUPPO DELLE APPLICAZIONI PER LA GESTIONE DEL BONUS AMBIENTE

I servizi di sviluppo ed evoluzione del software riguardano l'implementazione e la gestione della piattaforma web che consente l'erogazione del bonus ambiente; comprendono la realizzazione delle seguenti funzionalità utilizzabili attraverso la piattaforma web responsive:

Accronimi / glossario

PA : Pubblica amministrazione

MASE: Ministero dell'ambiente e sicurezza energetica

SEL: Soggetto che intende effettuare erogazione liberazione

- **Accesso alla Piattaforma web "Bonus Ambiente"**

    1. **Accesso e accreditamento PA**: le PA accedono e si accreditano alla Piattaforma web "Bonus Ambiente".

    2. **Accesso e accreditamento funzionari del MASE**: i funzionari del MASE, preventivamente accreditati sulla Piattaforma web "Bonus Ambiente" tramite l'invio dei relativi codici fiscali alla società Sogei S.p.A., accedono tramite credenziali SPID/CIE.

    3. **Accesso e registrazione del SEL:** il SEL accede tramite credenziali SPID/CIE al la Piattaforma web "Bonus Ambiente" e completa la procedura di registrazione inserendo i dati richiesti.

- **Gestione Interventi sulla Piattaforma web "Bonus Ambiente"**

    1. **Inserimento intervento (PA)**: le PA segnalano attraverso la Piattaforma web "Bonus Ambiente" l'intervento o gli interventi ai sensi dell' articolo 5, comma 1, del DPCM 10 dicembre 2021, che dovranno essere pubblicati dal MASE, sulla medesima Piattaforma. L'elenco degli interventi è continuamente aggiornato attraverso le segnalazioni delle PA.

    2. **Approvazione interventi (MASE):** Il MASE pubblica sulla Piattaforma web "Bonus Ambiente" tutte le informazioni inerenti gli interventi precedentemente segnalati dalle PA, ai sensi dell' articolo 5, comma 1, del DPCM 10 dicembre 2021.

- **Gestione Erogazione sulla Piattaforma web "Bonus Ambiente"**

1. **Manifestazione interesse all'erogazione (SEL):** l'utente individua dalla Piattaforma web "Bonus Ambiente" l'intervento da sostenere, ai sensi dell' articolo 5, comma 2, lettera a), del DPCM 10 dicembre 2021.

2. **Proposta erogazione liberale (SEL):** il SEL concorda importo e termini dell'erogazione liberale con la PA segnalatrice dell'intervento in oggetto, ai sensi articolo 5, comma 2, lettera a), del DPCM 10 dicembre 2021.

3. **Lavorazione proposta di erogazione liberale (PA):** la PA valuta ed eventualmente approva l'importo e i termini dell'erogazione liberale proposta.

4. **Ammissione al contributo (MASE):** una volta concordato importo e termini dell'erogazione liberale tra PA e SEL, nei 10 giorni successivi il MASE, comunica al SEL l'ammissione al contributo, ai sensi articolo 5, comma 2, lettera c), del DPCM 10 dicembre 2021.

5. **Versamento erogazione liberale prenotata (SEL):** entro 10 giorni successivi alla comunicazione dell'ammissione al contributo, il SEL effettua il versamento secondo i termini precedentemente concordati, ai sensi articolo 5, comma 2, lettera d), del DPCM 10 dicembre 2021.

6. **Verifica avvenuto versamento (PA):** entro 30 giorni dall'avvenuto versamento, la PA proprietaria del bene oggetto di finanziamento verifica il buon fine del pagamento, ai sensi articolo 5, comma 2, lettera e) del DPCM 10 dicembre 2021.

7. **Ottenimento dichiarazione (SEL):** il SEL accede alla Piattaforma web "Bonus ambiente" per scaricare apposita dichiarazione prodotta dalla Piattaforma attestante la donazione, sulla base delle informazioni fornite dai soggetti pubblici, e acconsente o meno alla pubblicazione di propri dati identificativi sul sito web istituzionale del Ministero, ai sensi articolo 5, comma 2, lettera f), del DCPM 10 dicembre 2021.

8. **Aggiornamento elenco donazioni (MASE):** il MASE pubblica sulla Piattaforma web "Bonus Ambiente" l'elenco delle donazioni ricevute, facendo esplicito riferimento al titolo dell'intervento, all'ente beneficiario, all'ammontare dell'erogazione e agli eventuali finanziamenti pubblici ricevuti dal medesimo intervento.

- **Attività di reportistica**

  - **Comunicazione mensile informazioni relative agli interventi (PA / Concessionari / Affidatari)**: tutti i sogetti beneficiari delle erogazioni liberali comunicano mensilmente al MASE, per il tramite della Piattaforma web "Bonus Ambiente", tutte le informazioni

relative all'intervento, i fondi pubblici assegnati per l'anno in corso, l'ente responsabile del bene, nonché le informazioni relative alla fruizione. Gli eventuali concessionari o affidattari beneficiari delle erogazioni liberali hanno l'onere di effettuare la medesima attività di comunicazione per il tramite dei soggetti pubblici proprietari del bene, ai sensi dell'articolo 5, comma 4, del DPCM 10 dicembre 2021.

- **Pubblicazione donazioni ricevute (MASE):** il MASE pubblica sulla Piattaforma web "Bonus Ambiente" l'elenco delle donazioni ricevute, facendo esplicito riferimento al titolo dell'intervento, all'ente beneficiario, all'ammontare dell'erogazione, e agli eventuali finanziamenti pubblici ricevuti dal medesimo intervento, ai sensi dell'articolo 5, comma 3, del DPCM 10 dicembre 2021. Il Ministero medesimo ha facolta di pubblicare i nominativi dei soggetti che hanno effettuato l'erogazione liberale solo previa autorizzazione ai sensi dell'articolo 5, comma 2, lettera f), del DPCM 10 dicembre 2021.

- **Invio dati all'Agenzia delle Entrate:** il MASE trasmette all'Agenzia delle entrate, con modalità telematiche definite d'intesa, entro il giorno 5 di ciascun mese, l'elenco dei soggetti beneficiari del credito d'imposta che nel mese precedente hanno reso la dichiarazione di cui all'articolo 5, comma 2, lettera f), del DPCM 10 dicembre 2021, con i relativi codici fiscali e gli importi spettanti (calcolati nella misura del 65% dell'erogazione liberale effettuata). Con le stesse modalità sono trasmesse successivamente le eventuali variazioni e revoche, ai sensi dell'articolo 6, comma 4, del DPCM 10 dicembre 2021.

Nell'ambito del servizio di sviluppo è previsto che l'attività di manutenzione, come descritta nell'allegato "A" alla Convenzione, venga erogata in garanzia per un periodo di 365 (trecentosessantacinque) giorni solari decorrenti dalla data di inizio estensione delle applicazioni software realizzate. Nel periodo Sogei è impegnata a prestare, a propria cura e spese, la manutenzione delle applicazioni software.

Sviluppo applicazione per la gestione del bonus ambiente							
Servizio	**Descrizione Rilascio/Obiettivo**	**Corrispettivo**	**Unità di misura**	**Volumi**	**Prezzo unitario**	**Importo senza IVA**	**Importo con IVA**
Sviluppo piattaforma bonus ambiente	Piattaforma bonus ambiente	Personalizzazione prodotti di mercato	€/GP	200	341,00 €	68.200,00 €	83.204,00 €
					TOTALE	**68.200,00 €**	**83.204,00 €**

Eventuali sviluppi non previsti in questo Piano, che si dovessero rendere necessari nel corso della durata contrattuale, potranno originare una revisione del piano operativo - che dovrà essere approvato dal Ministero - nel rispetto del massimale contrattuale. Qualora i suddetti sviluppi rendano necessaria la modifica del massimale di contratto sarà necessario provvedere alla stipula di appositi atti aggiuntivi.

2.1 CONDUZIONE PER LA GESTIONE BONUS AMBIENTE

Rientrano in questo ambito le attività di conduzione infrastrutturale della Piattaforma web "Bonus Ambiente" descritta nel paragrafo precedente, previste da novembre 2022 e fino al 31 dicembre 2023.

L'importo economico della tabella seguente, la cui modalità di remunerazione prevista è a canone mensile, copre le suddette attività.

Conduzione bonus ambiente 2022 (2 mesi)							
Servizio	**Rilascio/Obiettivo**	**Corrispettivo**	**Unità di misura**	**Volumi riferiti a 2 mesi**	**Prezzo unitario**	**Importo senza IVA**	**Importo con IVA**
Conduzione infrastrutturale	SERVER	vCPU	€/mese	16	98,68€	1.578,88 €	1.926,23 €
		vRAM	€/mese	64	15,86€	1.015,04 €	1.238,35 €
	STORAGE	GB allocati	€/mese	60	0,395 €	23,70 €	28,91 €
					TOTALE	**2.617,62 €**	**3.193,50 €**

Conduzione bonus ambiente 2023 (12 mesi)							
Servizio	**Rilascio/Obiettivo**	**Corrispettivo**	**Unità di misura**	**Volumi riferiti a 12 mesi**	**Prezzo unitario**	**Importo senza IVA**	**Importo con IVA**
Conduzione infrastrutturale	SERVER	vCPU	€/mese	96	98,68€	9.473,28€	11.557,40 €
		vRAM	€/mese	384	15,86€	6.090,24€	7.430,09 €
	STORAGE	GB allocati	€/mese	360	0,395 €	142,20€	173,48 €
					TOTALE	**15.705,72 €**	**19.160,98 €**

2.2 SERVIZI DI SUPPORTO

Al fine di coadiuvare il Ministero nel governo e monitoraggio di tutte le attività connesse alla gestione del sistema di erogazione del beneficio e per recepire gli adeguamenti normativi, si prevede l'erogazione di giornate di supporto.

Le attività, svolte in modo continuativo nell'arco della durata contrattuale, sono remunerate a canone mensile.

I servizi professionali di supporto sono erogati al fine di:

- coordinare il progetto;
- segnalazione al MASE in caso di eventuali usi difformi, o di violazioni delle norme del decreto del Bonus Ambiente, derivanti o concernenti la piattaforma di gestione dell'iniziativa;
- supporto per controlli a campione;
- monitoraggio degli oneri derivanti dal programma di erogazione del bonus ambiente;
- segnalazione al MASE di esaurimento delle risorse disponibili e relativa comunicazione, su indicazione del MASE, attraverso la Piattaforma;
- partecipazione ad incontri, riunioni ed eventuali gruppi di lavoro;
- predisposizione di documenti, prospetti e riepiloghi di sintesi per evidenziare "lo stato dell'arte" di tutte le attività tecnico/operative previste dalla convenzione;
- forniture dati;
- richieste spot per interventi di modifica dati;
- supporto e forniture per specifiche indagini della Guardia di Finanza;

Nelle tabelle seguenti viene indicato l'impegno previsto per il 2022 e 2023

Servizio di Supporto 2022 (2 mesi)							
Servizio	**Rilascio/Obiettivo**	**Corrispettivo**	**Unità di misura**	**Volumi riferiti a 2 mesi**	**Prezzo unitario**	**Importo senza IVA**	**Importo con IVA**
Governance e Supporto	SUPPORTO ISTITUZIONALE	Servizio Operativo	€/GP	25	362,00 €	9.050,00 €	11.041,00 €
		Servizio specialistico	€/GP	25	502,00 €	12.550,00 €	15.311,00 €
	GOVERNANCE	Servizio specialistico	€/GP	4	502,00 €	2.008,00 €	2.449,76 €
					TOTALE	**23.608,00 €**	**28.801,76 €**

Servizio di Supporto 2023 (12 mesi)							
Servizio	**Rilascio/Obiettivo**	**Corrispettivo**	**Unità di misura**	**Volumi riferiti a 12 mesi**	**Prezzo unitario**	**Importo senza IVA**	**Importo con IVA**
Governance e Supporto	SUPPORTO ISTITUZIONALE	Servizio Operativo	€/GP	55	362,00 €	19.910,00 €	24.290,20 €
		Servizio specialistico	€/GP	55	502,00 €	27.610,00 €	33.684,20 €
	GOVERNANCE	Servizio specialistico	€/GP	8	502,00 €	4.016,00 €	4.899,52 €
					TOTALE	**51.536,00 €**	**62.873,92 €**

2.3 ASSISTENZA UTENTI

Per l'assistenza al MASE ed alle PA con riferimento alle funzionalità di accesso, accreditamento e pubblicazione degli interventi finanziabili, nonché per l'assistenza richiesta dai SEL, prima, durante e dopo la loro manifestazione di interesse, verranno erogate giornate di supporto.

Nelle tabelle seguenti viene indicato l'impegno economico previsto per il 2022 e 2023.

Assistenza utenti 2022 (2 mesi)							
Servizio	**Rilascio/Obiettivo**	**Corrispettivo**	**Unità di misura**	**Volumi riferiti a 2 mesi**	**Prezzo unitario**	**Importo senza IVA**	**Importo con IVA**
Governance e Supporto	ASSISTENZA AGLI UTENTI	Servizio Operativo	€/GP	30	362,00 €	10.860,00 €	13.249,20 €
					TOTALE	**10.860,00 €**	**13.249,20 €**

Assistenza utenti 2023 (12 mesi)							
Servizio	**Rilascio/Obiettivo**	**Corrispettivo**	**Unità di misura**	**Volumi riferiti a 12 mesi**	**Prezzo unitario**	**Importo senza IVA**	**Importo con IVA**
Governance e Supporto	ASSISTENZA AGLI UTENTI	Servizio Operativo	€/GP	130	362,00 €	47.060,00	57.413,20 €
					TOTALE	**47.060,00 €**	**57.413,20 €**

Il costo indicato è da considerarsi come massimale.

2.4 IMPEGNO ECONOMICO

Di seguito una tabella riassuntiva dell'impegno economico previsto per l'erogazione dei servizi.

Piattaforma bonus Ambiente 2022			
Descrizione Rilascio/Obiettivo	**Importo annuale senza IVA**	**Importo annuale con IVA**	**Remunerazione**
Sviluppo della Piattaforma			
Rilascio	68.200,00 €	83.204,00 €	UT
Conduzione della Piattaforma			
Conduzione	2.617,62 €	3.193,50 €	Canone mensile
Servizio di Supporto			
Servizi di supporto	23.608,00 €	28.801,76 €	Canone mensile
Analisi rimborsi inseriti			
Assistenza utenti	10.860,00 €	13.249,20 €	A consumo
TOTALE	**105.285,62 €**	**128.448,46 €**	

Piattaforma bonus Ambiente 2023			
Descrizione Rilascio/Obiettivo	**Importo annuale senza IVA**	**Importo annuale con IVA**	**Remunerazione**
Conduzione della Piattaforma			
Conduzione	15.705,72 €	19.160,98 €	Canone mensile
Servizio di Supporto			
Servizi di supporto	51.536,00 €	62.873,92 €	Canone mensile
Analisi rimborsi inseriti			
Assistenza utenti	47.060,00 €	57.413,20 €	A consumo
TOTALE	**114.301,72 €**	**139.448,10 €**	

CONVENZIONE PER LA REALIZZAZIONE DELLA PIATTAFORMA RELATIVA ALL'INIZIATIVA BONUS AMBIENTE E LA GESTIONE DELLE ATTIVITÀ AD ESSA CONNESSE

ALLEGATO C – SCHEMA RAPPORTO PERIODICO

	Codice PPT	Descrizione PPT	Progressivo rilascio / Codice obiettivo	Descrizione rilascio / obiettivo	Data inizio rilascio effettiva	Data disponibiltà al collaudo	Data disponibiltà al collaudo effettiva	Data rilascio prevista	Data rilascio effettiva
	YYYYYY	Descrizione intervento	NN	Servizo Specialistico				gg/mm/aaaa	
	YYYYYY	Descrizione intervento	NN	descrizione obiettivo				gg/mm/aaaa	
	XXXXXX	Manutenzione servizi ICT	NN	Unità di manutenzione				gg/mm/aaaa	
	ZZZZZZ	GESTIONE E CONDUZIONE INFRASTRUTTURA - SERVER	05	Immagini					
	ZZZZZZ	GESTIONE E CONDUZIONE INFRASTRUTTURA - SERVER	6	vCPU					
	ZZZZZZ	GESTIONE E CONDUZIONE INFRASTRUTTURA - SERVER	7	vRAM					

Tipo rilascio / obiettivo	Quantità / Volumi pianificati	Baseline importo rilascio	Importo rilascio	SAL rilascio	Note	Stato
PROGETTUALE			eeeeeee	x%	stato avanzamento	In corso
PROGETTUALE	nnn	eeeeeee	eeeeeee	x%	stato avanzamento	In corso
PRODOTTI/SERVIZI SPECIFICI COMUNI DI CONDUZIONE	nnn		eeeeeee			In corso
PRODOTTI/SERVIZI SPECIFICI COMUNI DI CONDUZIONE	nnn	eeeeeee	eeeeeee			In corso
PRODOTTI/SERVIZI SPECIFICI COMUNI DI CONDUZIONE	nnn	eeeeeee	eeeeeee			
PRODOTTI/SERVIZI SPECIFICI COMUNI DI CONDUZIONE	nnn	eeeeeee	eeeeeee			
		€ xxxxxxxxx	**€ xxxxxxxxxxx**			

CONVENZIONE

PER LA REALIZZAZIONE DELLA PIATTAFORMA RELATIVA ALL'INIZIATIVA BONUS

AMBIENTE E LA GESTIONE DELLE ATTIVITA' AD ESSA CONNESSE

ALLEGATO PRIVACY

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*", le Amministrazioni e/o altri enti o persone giuridiche destinatarie dei servizi erogati dalla Sogei attraverso la *Convenzione*, che rivestono la qualifica di *Titolari 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* per la realizzazione della piattaforma relativa all'iniziativa bonus ambiente e la gestione delle attività ad essa connesse, comprensiva di tutta la documentazione allo stesso afferente, stipulata tra Ministero dell'ambiente e sicurezza energetica, che rappresenta l'Amministrazione Cliente, 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 Ministero dell'ambiente e sicurezza energetica svolge i compiti ad essi demandati dalla Costituzione, dalla legge e dai propri atti regolamentari;
- 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 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 Ministero dell'ambiente e sicurezza energetica, con sede in Roma, via Cristoforo Colombo, n. 44, 00147 Roma, codice fiscale 97047140583 in persona del legale rappresentante Dott. Giuseppe Lo Presti, domiciliato per la carica presso la sede legale, 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.

I dati personali trattati sono di tipo comune e precisamente:

- dati di autenticazione del funzionario della P.A. forniti tramite accesso con Spid e CIE per consentire la registrazione al portale, l'inserimento e la rendicontazione degli interventi finanziabili (nome e cognome, codice fiscale indirizzo mail del funzionario della P.A.;
- dati di autenticazione, forniti tramite accesso con Spid e CIE, del Soggetto erogatore del finanziamento (SEF) o del suo legale rappresentante (nome e cognome, codice fiscale, indirizzo mail);
- dati di navigazione degli utenti che accedono alla piattaforma.

Gli interessati a cui si riferiscono i dati personali trattati sono i funzionari della P.A. e i Soggetti erogatori del finanziamento (SEF), nonché i loro eventuali legali rappresentanti. Con riguardo alle attività di navigazione, gli interessati sono rappresentati dagli utenti che accedono alla piattaforma.

Per quanto riguarda invece le tipologie di servizi di assistenza tipo CRM o via posta elettronica, potenzialmente sono trattate tutte le categorie di dati personali, non essendo a noi noto a priori quanto il cittadino/utente scrive come testo libero.

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.

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.

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 entro 15 giorni dalla data di ricezione della comunicazione.

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 Regolamento, 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

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.

Qualora il Titolare opti per la restituzione dei dati, sarà fornita una copia del database contenente il riepilogo della struttura delle tabelle del database medesimo ed i relativi dati, il che consentirà al Titolare di ripristinare il database stesso e tutti i dati in esso contenuti alla data in cui è terminata la prestazione dei servizi relativi al trattamento. La copia sarà resa disponibile, opportunamente criptata, attraverso una piattaforma aziendale di condivisione in tempo reale e sicura di contenuti sul cloud. La password per la decifratura sarà fornita separatamente (via email). Contestualmente i dati saranno definitivamente cancellati dal database applicativo utilizzato da Sogei.

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

- Metodologia per la protezione dei dati e per la valutazione d'impatto
- 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.

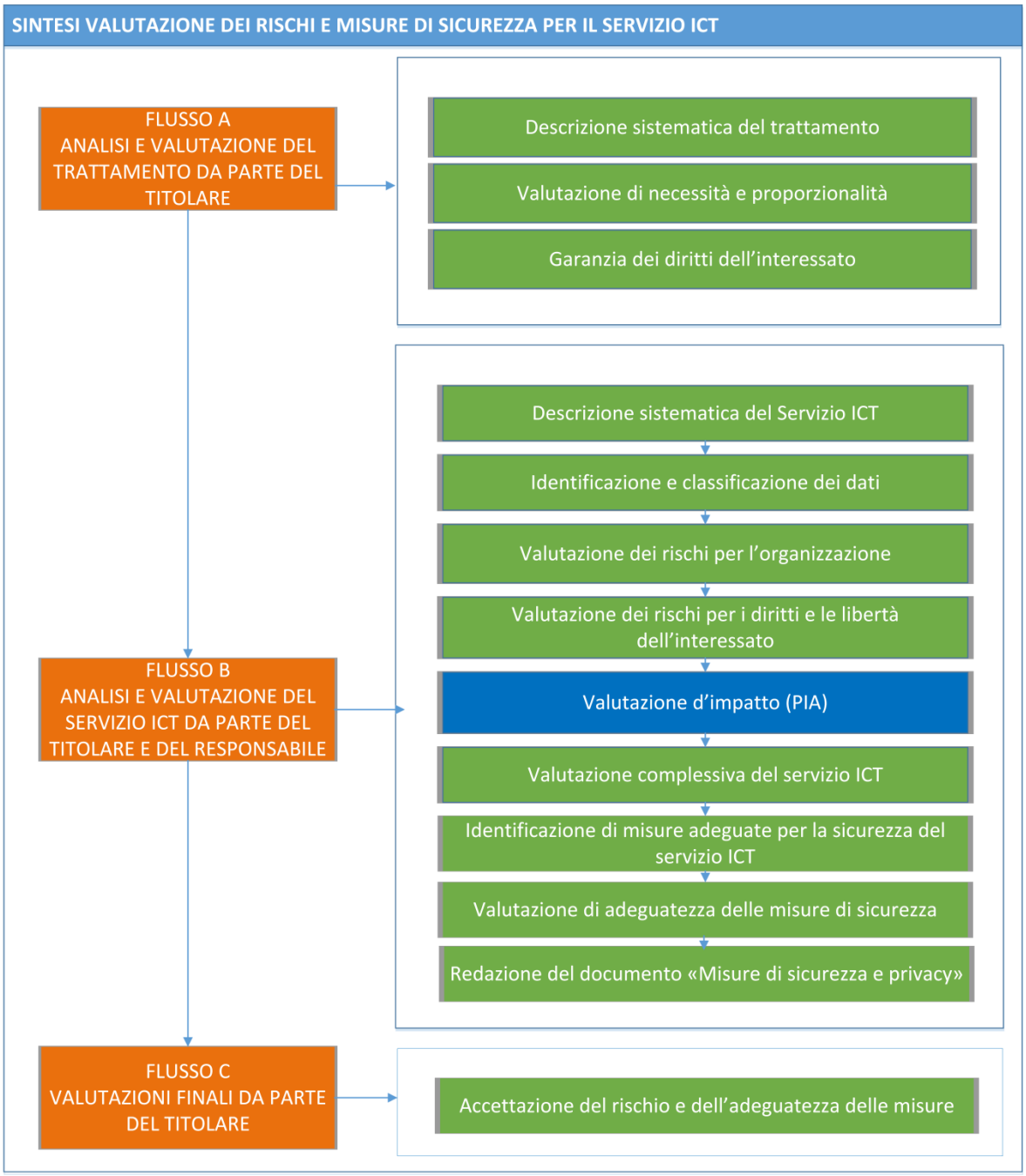
Di seguito il flusso di sintesi[1] per la valutazione dei rischi e delle misure di sicurezza per il Servizio ICT, suddiviso in tre parti:

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:

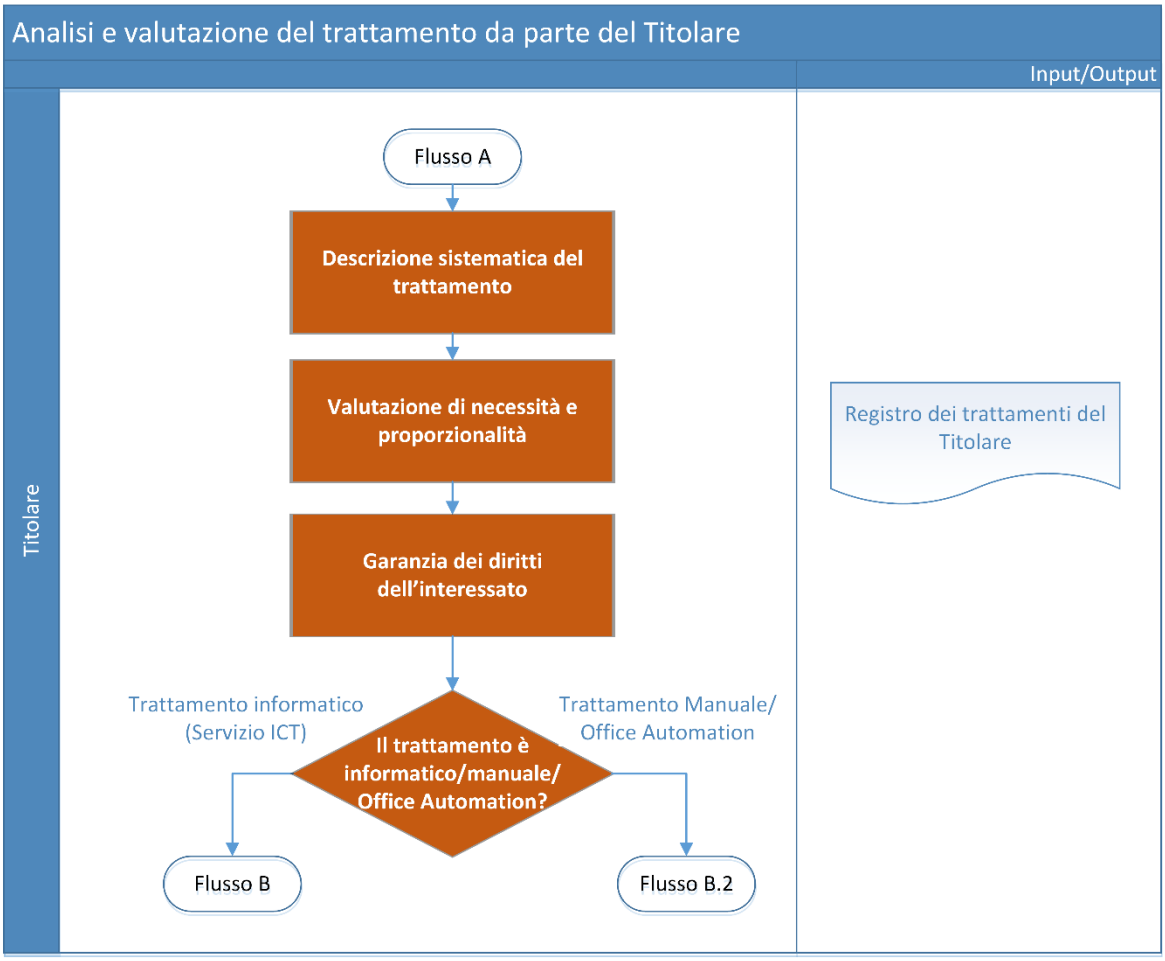
- rischi per i diritti e le libertà degli interessati - compresa la valutazione d'impatto, ove necessaria - relativi al trattamento di dati personali;
- rischi per l'organizzazione del Titolare, relativi alla sicurezza delle informazioni elaborate;
- adeguatezza delle misure di sicurezza da applicare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

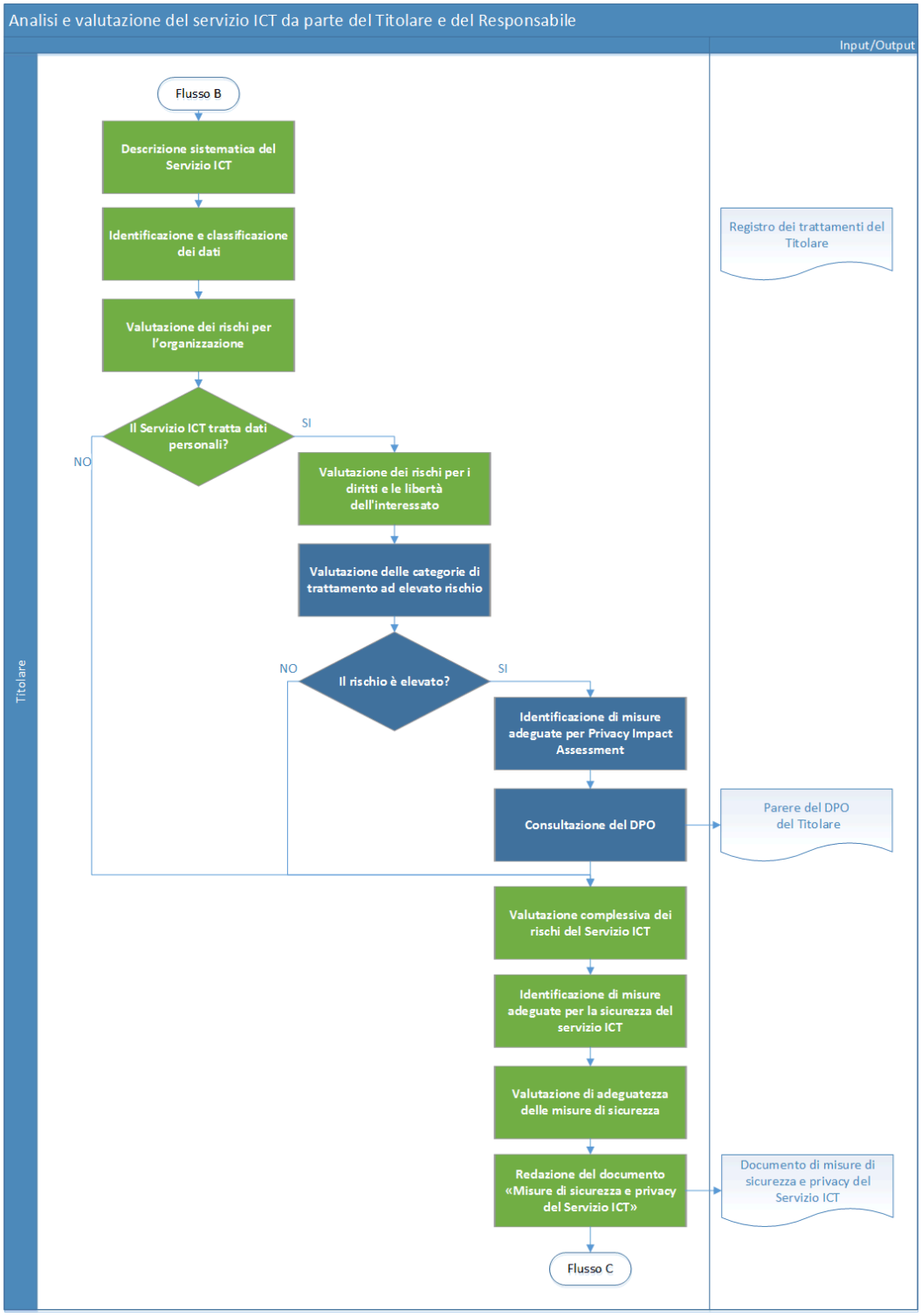
parere in merito al fine di garantire che il trattamento rispetti in ogni caso il Regolamento e può avvalersi dei propri poteri, tra cui rivolgere ammonimenti o ammonizioni, imporre limitazioni o divieti. L'Autorità di controllo, inoltre, viene notificata di eventuali violazioni di dati personali (*data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

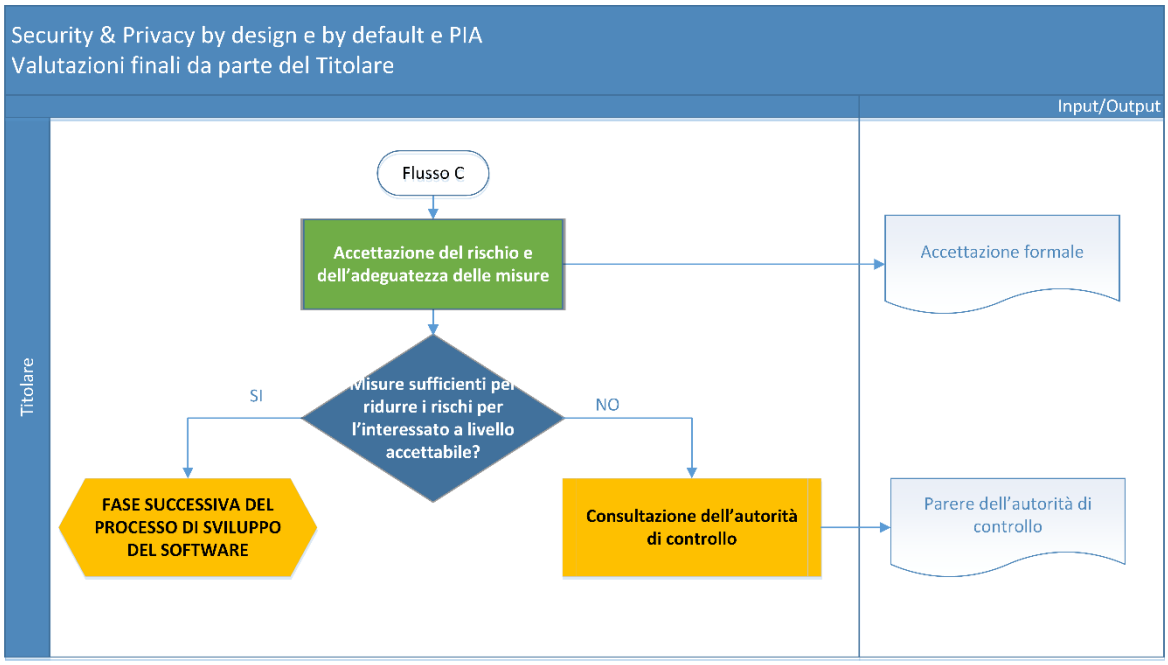
Il Responsabile del Servizio ICT invia il documento contestualmente al documento "Analisi dei Requisiti"/"Specifica di intervento" se previsto o, in caso contrario, in un momento utile a garantire comunque uno sviluppo coerente del Servizio ICT.

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.

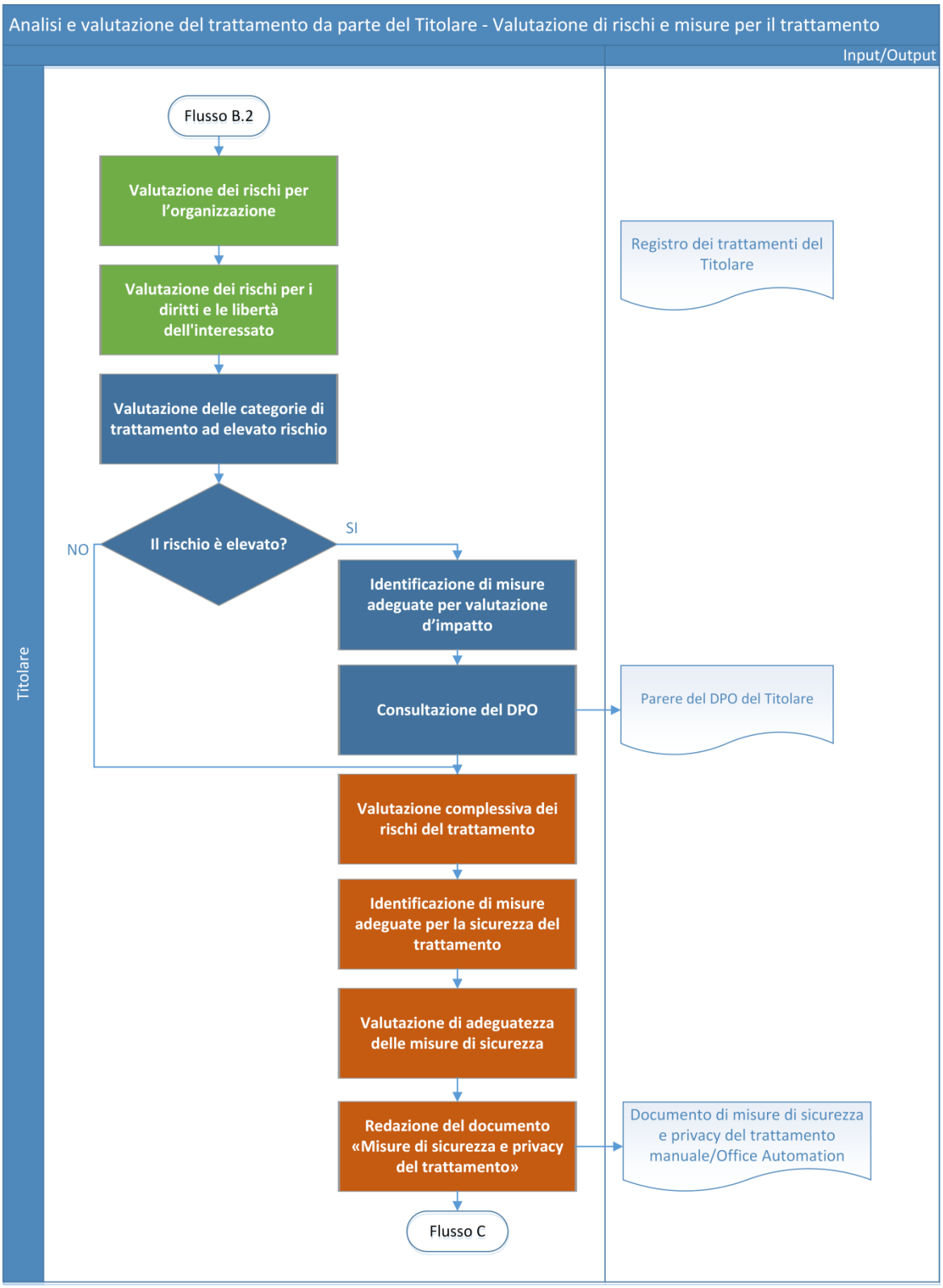
Oltre alle misure selezionate sulla base del profilo di rischio del trattamento/ Servizio ICT, Sogei protegge tutte le informazioni che tratta in qualità di Titolare o di Responsabile con un set di misure infrastrutturali elencate in specifici allegati ai registri dei trattamenti.

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