<<RC_PG_ GF_00_Procedura di Gestione dei Fornitori

Identificativo: in qualità di Responsabili del trattamento di dati personali>>

<<Ver. 2.0>>

Data: 10/07/2024

PROGETTO:

GOVERNO DELLA CYBERSECURITY E DELLA DATA PROTECTION

Procedura di Gestione dei Fornitori in qualità di Responsabili del trattamento di dati personali

Regione Calabria

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Deloitte Risk Advisory S.r.l.

EY Advisory S.p.A.

Teleco S.r.l.

Lista di Distribuzione

Rev.	Data	Destinatario	Ente/Azienda
2.0	10/07/2024	Ing. Alfredo Pellicanò	Regione Calabria
2.0	10/07/2024	Dott.ssa Paola Zuccaro	Regione Calabria
2.0	10/07/2024	Ing. Giovanna Pisano	Regione Calabria
2.0	10/07/2024	Avv. Angela Stellato	Regione Calabria
2.0	10/07/2024	Avv. Daniela Labate	Regione Calabria
2.0	10/07/2024	Avv. Giovanni Sacchi	Regione Calabria
2.0	10/07/2024	Dott.ssa Ilenia Pia Viceconti	Deloitte
2.0	10/07/2024	Dott.ssa Alessia Ruta	Deloitte
2.0	10/07/2024	Dott.ssa Valentina Laurenzano	Deloitte
2.0	10/07/2024	Dott.ssa Ilaria Mattesi	Deloitte
2.0	10/07/2024	Dott.ssa Alessandra Di Giovanni	Deloitte
2.0	10/07/2024	Dott. Luca Cristantielli	Deloitte

Registro delle Revisioni

Rev.	Data	Descrizione delle modifiche	Autore di rif.
1.0	11/04/2024	Prima emissione	Ilenia Pia Viceconti
2.0	10/07/2024	Integrazione paragrafo 5.2	Ilenia Pia Viceconti

Calendario degli Incontri Principali

Data	Incontro	Stato
11/04/2024	Riunione con il DPO Avv. Angela Stellato	Effettuato
24/04/2024	Riunione con il DPO Avv. Angela Stellato	Effettuato
28/06/2024	Riunione con il DPO Avv. Angela Stellato e Avv. Giovanni Sacchi	Effettuato

1. INTRODUZIONE

Il Regolamento Generale sulla Protezione dei Dati (GDPR) disciplina all'art. 28 il rapporto tra il Titolare del trattamento dei dati personali e il Responsabile. Quest'ultimo è una figura che tratta i dati personali per conto del Titolare del trattamento, secondo le modalità e finalità da esso stabilite.

Secondo la norma, Titolare e Responsabile del trattamento devono stipulare un accordo sul trattamento dei dati personali (c.d. "Data Processing Agreement" o nel prosieguo DPA) che deve contenere una serie di clausole specifiche, tra cui l'obbligo per il Responsabile del trattamento di:

- Trattare i dati personali solo in base alle istruzioni del Titolare;

- Garantire la sicurezza dei dati personali trattati;

- Garantire la riservatezza dei dati personali trattati;

- Garantire la nomina di un Responsabile della protezione dei dati (DPO) nei casi previsti dalla legge;

- Fornire assistenza al Titolare del trattamento in caso di richieste di esercizio dei diritti degli interessati e/o in caso di Data Breach.

1.1 SCOPO

Regione Calabria, contando un grande numero di Fornitori qualificabili come Responsabili del trattamento, si dota della presente procedura al fine di disciplinare la gestione degli aspetti di sicurezza (privacy) sulle attività esternalizzate che richiedono un trattamento di dati personali.

1.2 CAMPO DI APPLICAZIONE

Tale procedura è valida per l'intera Regione Calabria e per ogni struttura di cui essa si compone.

2. DEFINIZIONE E ACRONIMI

2.1 DEFINIZIONI

Termine	Descrizione
Dato personale	Ex art. 4, comma 1 del GDPR, "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"
Trattamento	Ex art. 4, comma 2 del GDPR: "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, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"
Titolare del trattamento	Ex art. 4, comma 7 del GDPR: "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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri"
Responsabile del trattamento	Ex art. 4, comma 8 del GDPR: "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento"
Titolare autonomo del trattamento	I soggetti esterni che erogano i propri servizi in forza di codici deontologici di settore e/o mandati di rappresentanza e con l'ausilio della propria organizzazione (e.g. liberi professionisti quali studi legali, Commercialisti e Notai).
Co-titolare del trattamento	Ex art. 26 del GDPR: "Allorché due o più Titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento…"
Accountability	Ex art. 5, paragrafo 2 del GDPR: "Il Titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)". Il paragrafo 1 dell'art. 5 del GDPR riguarda i principi fondamentali che devono essere accuratamente applicati ai trattamenti di dati personali.

Violazione dei dati personali ("Data Breach")	Ex art. 4, comma 12 del GDPR: "la violazione dei dati personali è 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".

2.2 ACRONIMI

Termine	Descrizione
GDPR	General Data Protection Regulation
DT	Delegato del Titolare
RPD / DPO	Responsabile della Protezione dei Dati Personali / Data Protection Officer
RTD	Responsabile del trattamento
AdS	Amministratore di Sistema
RUP	Responsabile Unico del Progetto
DEC	Direttore dell'esecuzione del contratto
DPA	Data Processing Agreement

3. RIFERIMENTI

3.1 DOCUMENTI APPLICABILI

Rif.	Codice	Titolo
DA-1.	RC05_Piano Fabbisogni_Governo Cybersecurity e Data Protection v16	Piano dei fabbisogni
DA-2.	CIG 8884642E81	Contratto Esecutivo del 05 marzo 2024

3.2 DOCUMENTI DI RIFERIMENTO

Rif.	Codice	Titolo
DR-1.	Doc. web n. 32016R0679	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)
DR-2.	DGR N. 29 del 1° febbraio 2021	Regolamento Regionale n. 20 del 18 dicembre 2018 modificato dalla deliberazione di Giunta Regionale n. 29 del 1° febbraio 2021
DR-3.	DGR N. 12 del 14 dicembre 2022	Regolamento Regionale n. 12/2022 e ss.mm.ii "Regolamento di organizzazione delle strutture della Giunta Regionale" (ultima modifica 28/12/2023)
DR-4.	Linee Guida Modelli di Designazione Responsabili Esterni, Autorizzati, Amministratori di Sistema	Linee Guida sulle modalità di nomina dei Responsabili del trattamento esterni.

4. RIFERIMENTI NORMATIVI

Il presente documento è redatto in coerenza con le seguenti normative e documenti di riferimento:

[1] Regolamento UE 2016/679 - General Data Protection Regulation (di seguito GDPR);

[2] D.lgs. 2003/196 Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

[3] D.lgs. 231/2001 Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300;

[4] D.lgs. 101/2018 - 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);

[5] Circolare 18 aprile 2017, n. 2/2017 Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni;

[6] Regolamento Regionale n. 20 del 18 dicembre 2018;

[7] Deliberazione della Giunta Regionale n. 29 della seduta del 01.02.2021 e Allegato A “Competenze in materia di trattamento dei dati personali - approvazione modifiche al regolamento regionale n. 20 del 18 dicembre 2018”;

[8] Decreto del Presidente della Regione n. 177 del 04/11/2021.

5. RUOLI E RESPONSABILITÀ

Tutti i Dipartimenti e Strutture Equiparate della Regione Calabria sono destinatari del presente documento.

Di seguito i ruoli e le relative responsabilità definite:

- ***Responsabile Unico del Progetto (RUP):***

Il Responsabile Unico del Progetto per le fasi di programmazione, progettazione, affidamento e per l'esecuzione di ciascuna procedura soggetta al Codice degli appalti 36/2023. Il RUP assicura il completamento dell'intervento pubblico nei termini previsti e nel rispetto degli obiettivi connessi al suo incarico, svolgendo tutte le attività necessarie.

- ***Direttore dell'esecuzione del contratto (DEC)***

Tale figura deve svolgere un'attività di controllo volta ad indagare la regolare esecuzione nei tempi prestabiliti ed il rispetto delle prescrizioni contenute nei documenti contrattuali. Anche al DEC spettano: la verifica del rispetto degli obblighi dell'esecutore e del subappaltatore, la gestione di contestazioni, la proposta al RUP di modifiche e varianti nel corso dell'esecuzione.

- ***Delegato dipartimentale al trattamento dei dati personali***

Il Titolare del Trattamento delega i compiti e le funzioni di cui all'art. 1, comma 1 del Regolamento Regionale n. 20 del 18 dicembre 2018, come modificato dalla Deliberazione di Giunta Regionale n. 29 del 1 febbraio 2021, a ciascun Dirigente della Giunta Regionale, al Responsabile della prevenzione della corruzione e della trasparenza, nonché ai Responsabili di struttura o ufficio di diretta collaborazione, quali "Delegati al trattamento dei dati personali" (di seguito Delegato del Titolare), ognuno per le attività di trattamento dei Dati Personali effettuate nell'ambito dell'articolazione amministrativa di cui è responsabile. I Delegati sopracitati hanno pertanto il compito di individuare e nominare i «Responsabili del trattamento».

- ***Settore referente privacy dipartimentale***

Il Settore referente privacy dipartimentale è individuato da ciascun Dirigente Generale di Dipartimento o di Struttura Equiparata compie, per le attività di trattamento dei Dati Personali effettuate dall'Ente, una serie di compiti e funzioni riportati all'art. 1, comma 2 del regolamento regionale n. 20 del 18 dicembre 2018, come modificato dalla Deliberazione di Giunta regionale n. 29 del 1 febbraio 2021, tra cui: coordina le attività dei Delegati del Titolare nell'ambito del dipartimento o struttura equiparata e costituisce il punto di contatto dipartimentale per il DPO, il settore regionale competente in materia di privacy ed il settore regionale competente in materia di Agenda Digitale.

- ***Settore referente sicurezza informatica regionale***

Il Settore referente sicurezza informatica regionale, competente in materia di Agenda Digitale, supporta i Delegati del Titolare con la collaborazione del "Settore referente privacy regionale" nelle attività di valutazione della gravità delle eventuali violazioni di sicurezza e di determinazione delle misure di contenimento e contrasto per porre rimedio alle violazioni riscontrate. Inoltre, collabora con il "Settore referente privacy regionale" nelle attività di definizione e verifica delle misure di sicurezza informatica,

valutazione di impatto delle attività di trattamento (DPIA), notificazione formale di violazione dati al Garante Privacy ed eventuale comunicazione agli interessati ed infine, nella verifica delle condizioni tecniche per l'eventuale trasferimento dati verso paesi terzi o organizzazioni internazionali.

- ***Settore referente privacy regionale***

Il Settore referente privacy regionale competente in materia di privacy, oltre ai compiti e funzioni previsti dai vigenti atti di organizzazione, predispone la modulistica relativa agli adempimenti richiesti dal GDPR.

- ***Data Protection Officer (DPO) – Ufficio Privacy Regionale***

Il DPO e l'Ufficio Privacy hanno il compito di controllare e monitorare la corretta adozione degli adempimenti privacy all'interno della Regione Calabria, eventualmente anche con il supporto di consulenti esperti di sistemi di controllo per gli aspetti tecnici. Inoltre, il DPO supporta i Dipartimenti e le Strutture Equiparate della Regione Calabria nella valutazione dell'adozione di strumenti per assicurare la corretta gestione dei Fornitori.

- ***Lead Auditor e Auditor***

Il Lead Auditor (o anche Auditor) ha la responsabilità di assicurare un'efficace ed efficiente esecuzione dell'Audit. Calato nel contesto di Regione Calabria, il Lead Auditor può essere un soggetto terzo, o in alternativa, un soggetto comunque designato dal Delegato del Titolare.

Di seguito si illustrano i due principali processi privacy da considerare per la corretta gestione degli aspetti di sicurezza dei Fornitori che trattano in toto o in parte dati personali:

A - Gestione degli atti di nomina dei Fornitori a Responsabili del trattamento

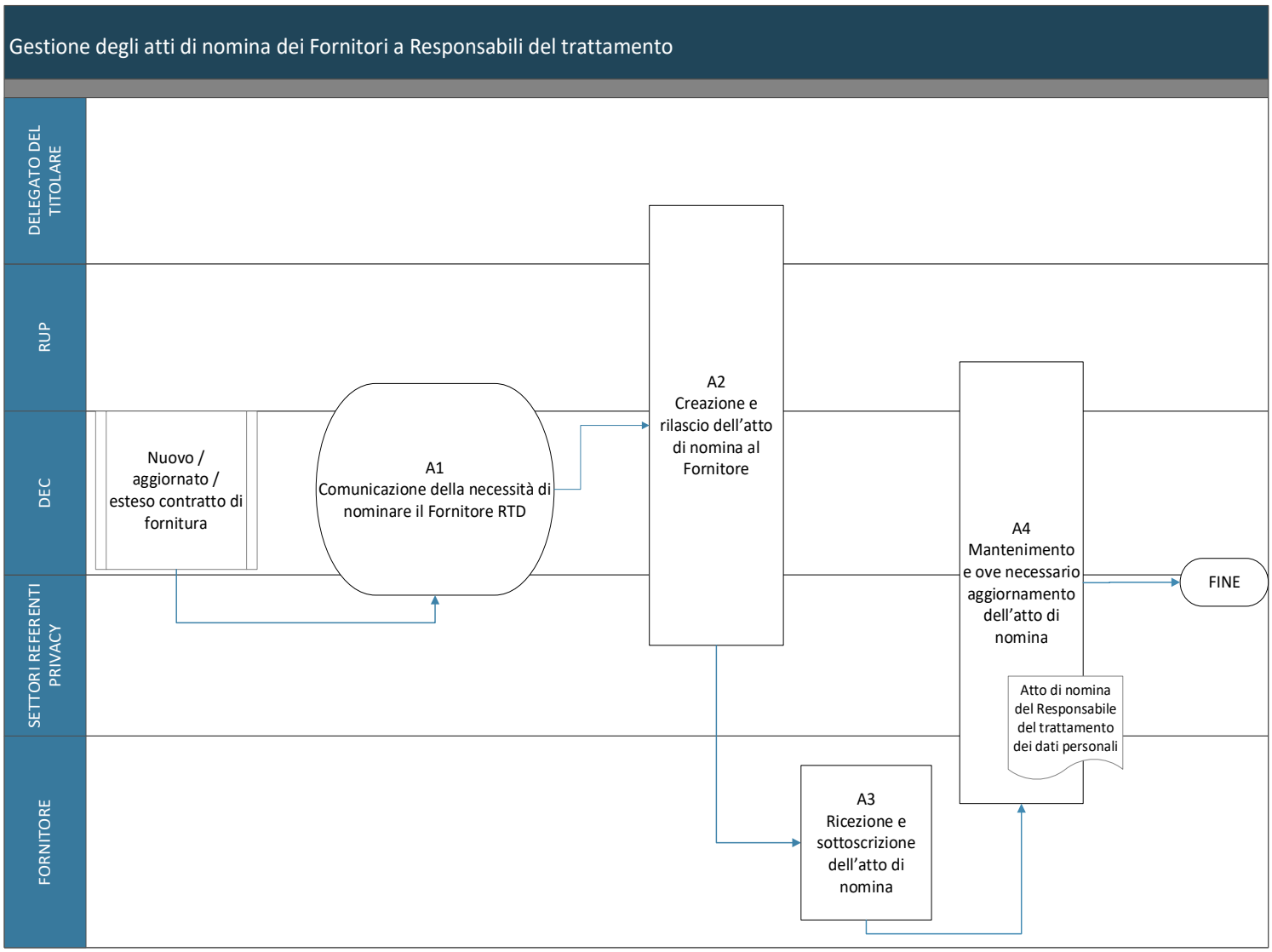
B - Gestione dell'attività di Privacy Audit

5.1 GESTIONE DEGLI ATTI DI NOMINA DEI FORNITORI A RESPONSABILI DEL TRATTAMENTO

Di seguito è riportata una panoramica su ruoli e responsabilità per il processo di *Gestione degli atti di nomina dei Fornitori a Responsabili del trattamento*:

ID	FASE	RUP	DELEGATO DEL TITOLARE	DEC	SETTORI REFERENTI PRIVACY	FORNITORE	DPO/UFFICIO PRIVACY
A1	**Comunicazione della necessità di nominare il Fornitore RTD**	R	C/I	R	A/R	-	-
A2	**Creazione e rilascio dell'atto di nomina al Fornitore**	R	A	R	R	I	I
A3	**Ricezione e sottoscrizione dell'atto di nomina da parte del Fornitore**	I	I	I	-	A/R	I
A4	**Mantenimento e ove necessario aggiornamento dell'atto di nomina**	R	I	R	A	R	I

Di seguito, si illustra il diagramma di flusso relativo all'attività in oggetto:



Legenda:

- Primo evento
- Inizio/Fine attività
- Fase del processo
- Documento/output

Il Titolare del trattamento può esternalizzare, in toto o in parte, attività di trattamento dei dati personali, affidandole a soggetti che operano per suo conto. In questo caso, il Fornitore diventa parte del sistema

privacy del Titolare e opera sotto la sua autorità, utilizzando i dati che rientrano nel dominio del Titolare e vincolandosi a standard prestazionali e di comportamento ben definiti.

Il Responsabile ha una parziale autonomia riguardo la disciplina del servizio e alcune scelte tecnico-operative, ma non ha il potere di prendere le principali decisioni sulle finalità e le modalità di utilizzo dei dati, che spettano esclusivamente al Titolare del trattamento.

Il presupposto per l'affidamento di trattamenti a soggetti esterni è che sia valutata, nella fase istruttoria (mediante acquisizione di specifica documentazione), l'affidabilità del soggetto, in relazione all'esperienza, capacità, alle misure di sicurezza organizzative e tecnico-informatiche affinché fornisca adeguate garanzie del pieno rispetto delle disposizioni contenute nel GDPR e nella normativa in ambito vigente.

Una volta formalizzati gli accordi con il Fornitore, il Settore referente privacy, il DEC e il RUP dovranno consultare il Delegato del Titolare riguardo la necessità di rilasciare un atto di nomina del Fornitore qualificato come Responsabile del trattamento di dati per un nuovo / aggiornato / esteso contratto di fornitura.

Dopo aver ricevuto tale comunicazione, il Delegato del Titolare, di concerto con il DEC, il RUP e il Settore Referente Privacy dovrà predisporre, con l'eventuale supporto del DPO/Ufficio Privacy, la specifica modulistica, allegata al contratto di servizio/fornitura, che dovrà essere sottoscritta dal Titolare e dal Fornitore in qualità di Responsabile del trattamento.

Il Data Processing Agreement - DPA (in Regione Calabria "*Atto di nomina del Responsabile del trattamento dei dati personali*") è considerato un'importante valutazione degli aspetti privacy garantiti dal Fornitore in quanto al suo interno quest'ultimo declina e garantisce una serie di controlli specifici volti a dimostrare che il trattamento dei dati personali eseguito per conto del Titolare è conforme ai requisiti imposti dalla normativa cogente ad oggi in vigore.

In dettaglio, l'*Atto di nomina del Responsabile del trattamento dei dati personali* si compone dei seguenti ambiti:

- descrizione del trattamento dei dati personali;
- elenco dei Sub-Responsabili;
- sicurezza del trattamento e catalogo delle misure di sicurezza;
- istruzioni relative al trattamento di dati personali.

Ai sensi dell'art. 28 GDPR, si prevede in particolare che il Fornitore:

- tratti 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 del trattamento; in tal caso, il Responsabile del trattamento informa il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

- adotti tutte le misure richieste ai sensi dell'articolo 32 (misure tecniche-organizzative adeguate);
- rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro Responsabile del trattamento;
- tenendo conto della natura del trattamento, assista il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
- assista il Titolare del trattamento nel garantire il rispetto degli obblighi in tema di data-breach, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento;
- metta a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

L'Atto di nomina deve essere sottoscritto prima dell'erogazione del servizio e deve essere integrato/rivisto ogniqualvolta cambino i trattamenti o le relative misure di sicurezza.

Una volta predisposta la modulistica privacy, il contratto e gli allegati verranno trasmessi al Fornitore per sua opportuna revisione e firma.

Il Fornitore a questo punto dovrà leggere attentamente il contenuto e comprendere le informazioni dell'atto di nomina. Successivamente, il Fornitore dovrà sottoscriverlo e inviarlo nuovamente al Titolare.

Il Settore referente privacy, DEC e il RUP, ricevuto l'atto di nomina dal Fornitore, dovranno verificare – informando il Delegato del Titolare – la presenza di eventuali modifiche alle clausole contrattuali privacy inserite nel contratto o agli allegati in materia di trattamento dei dati personali, ed infine dovranno fornire un riscontro inviando copia sottoscritta del contratto e degli allegati.

L'atto di nomina del Fornitore a Responsabile del trattamento richiede il costante monitoraggio e, se necessario, l'aggiornamento al fine di garantire la sua piena conformità alla normativa vigente. In caso di qualsivoglia modifica / aggiornamento, l'atto di nomina modificato / aggiornato dovrà essere inviato al Fornitore per la sua sottoscrizione.

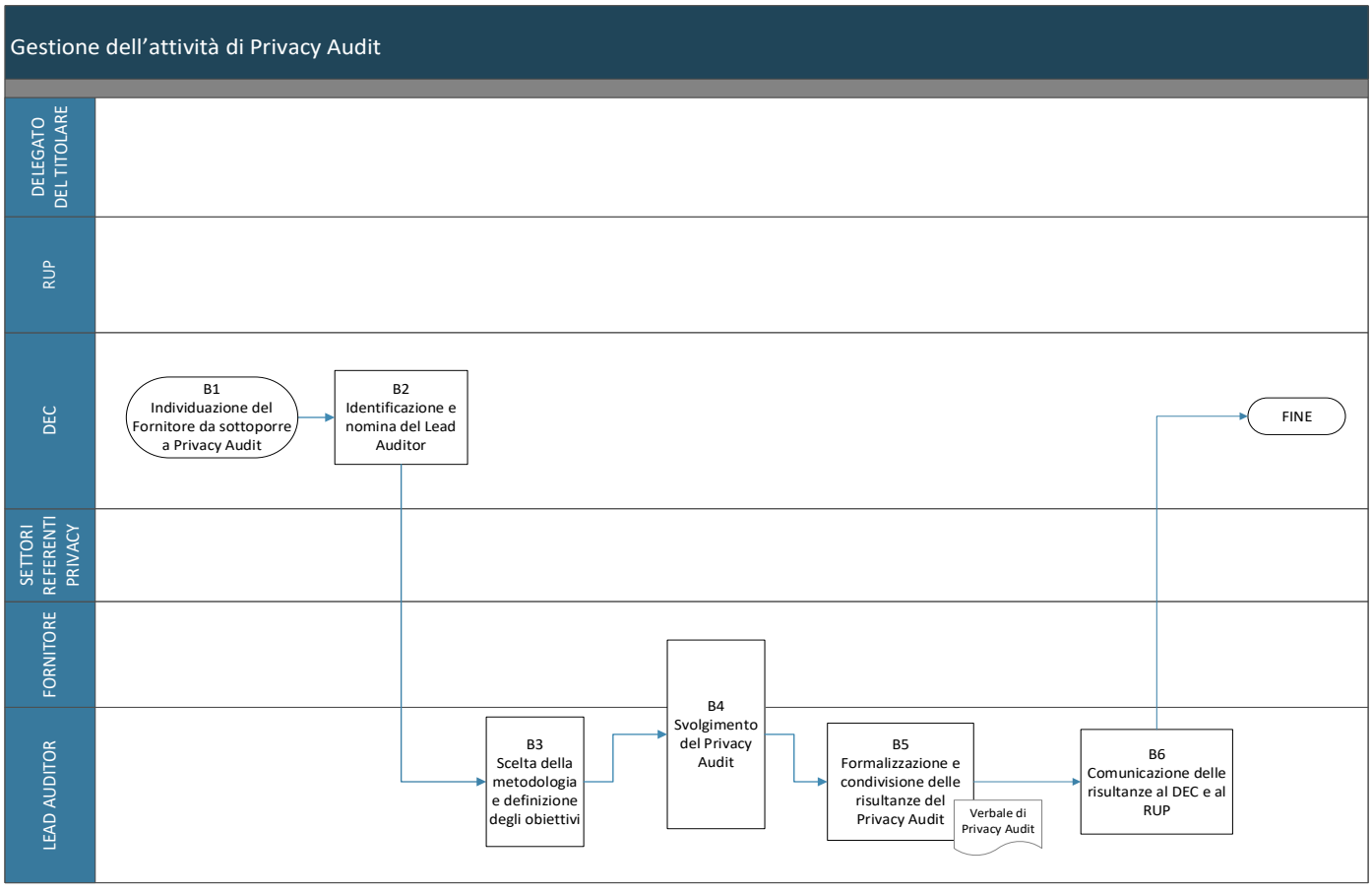
Inoltre, ogni Dipartimento / Struttura Equiparata e Settore di Regione Calabria dovrà, nell'attività di censimento e aggiornamento dei trattamenti di dati personali, segnalare all'interno della piattaforma Trades l'esistenza dell'Atto di nomina a Responsabile del trattamento sottoscritto.

5.2 GESTIONE DELL'ATTIVITÀ DI PRIVACY AUDIT

Di seguito è riportata una panoramica su ruoli e responsabilità per il processo di *Gestione dell'attività di Privacy Audit:*

ID	FASE	DELEGATO DEL TITOLARE	RUP	DEC	SETTORI REFERENTI PRIVACY	DPO / UFFICIO PRIVACY	FORNITORE	LEAD AUDITOR
B1	**Individuazione del Fornitore da sottoporre a Privacy Audit**	I	I	A/R	C	I	I	-
B2	**Identificazione e nomina del Lead Auditor**	I	I	A/R	I		-	I
B3	**Scelta della metodologia e definizione degli obiettivi**	-	I	I	-		I	A/R
B4	**Svolgimento del Privacy Audit**	-	I	I	-	I	R	A/R
B5	**Formalizzazione e condivisione delle risultanze al Responsabile**	I	I	I	-	i	C	A/R
B6	**Comunicazione delle risultanze al DEC e al RUP**	-	I	I	-	-	-	A/R

Di seguito, si illustra il diagramma di flusso relativo all'attività in oggetto:



Il Titolare del trattamento, così come previsto dall'art.28 del GDPR, mediante l'esecuzione di un Privacy Audit sui Fornitori, verifica l'ottemperanza alla normativa cogente su una specifica attività esternalizzata per la quale viene svolto un trattamento di dati personali da parte del Fornitore.

Il Titolare può decidere di svolgere attività di verifica sul Responsabile del Trattamento avvalendosi di personale interno alla propria organizzazione oppure affidando l'attività ad un soggetto esterno.

Tale fase ha l'obiettivo di descrivere i ruoli e le responsabilità, le modalità e le tempistiche nello svolgimento dell'attività di Audit che potrà sostanziarsi in un Privacy Audit sul Responsabile del trattamento o in una Valutazione Checklist Privacy a cura del Responsabile.

Ogni anno il DEC, dopo aver consultato il Settore referente Privacy e informati il Delegato del Titolare, il RUP e il DPO / Ufficio Privacy, è responsabile di avviare la valutazione circa la necessità di svolgere un Privacy Audit sul Fornitore in qualità di Responsabile del trattamento dei dati personali, in base alla prioritizzazione dei Fornitori effettuata da Regione Calabria.

La prioritizzazione dei Fornitori da sottoporre a Audit è effettuata sulla base della criticità dei dati personali trattati dai Fornitori RTD per conto di Regione Calabria e/o dalla criticità dei servizi esternalizzati in toto o in parte a Fornitori da cui i dati personali sono trattati.

A questo punto, il Lead Auditor verrà investito di tutte le competenze relative allo svolgimento del Privacy Audit sul Responsabile, tra cui definire gli obiettivi e le attività in cui si sostanzierà l'Audit, informandone il DEC e il Fornitore stesso.

Una volta identificato e nominato l'Auditor, quest'ultimo può avviare l'attività, di concerto con il DEC e il RUP, secondo due differenti modalità di seguito elencate:

1. Valutazione Checklist Privacy a cura del Responsabile
2. Privacy Audit svolto dall'Auditor

In particolare, la modalità:

- **Privacy Audit svolto dall'Auditor** è un Privacy Audit svolto dall'Auditor nei confronti del Responsabile, mediante l'impiego di adeguate tecnologie digitali (es. Zoom, Teams, etc.) e/o, a discrezione dell'Auditor così come di concerto con il DEC e con il RUP, in loco presso la sede del fornitore oppure presso la sede regionale. A supporto di tale Audit, il Lead Auditor beneficerà del documento "Checklist di Privacy Audit" a supporto delle sue analisi;
- **Valutazione Checklist Privacy a cura del Responsabile**: il Lead Auditor condivide, di concerto con il DEC e con il RUP, al Responsabile il documento "Checklist di Privacy Audit" (di seguito "Checklist"), che dovrà essere compilato da quest'ultimo, corredato da evidenze documentali e rinviato dallo stesso al Lead Auditor.

Per approfondimenti circa la Checklist di Privacy Audit si rimanda al sito della Regione (https://www.regione.calabria.it/website/portaltemplates/view/view.cfm?42273).

La prima modalità di Audit "*Privacy Audit svolto dall'Auditor*" ha inizio con la riunione di apertura, svolta dall'Auditor assieme al personale del Responsabile coinvolto nell'attività. Ove necessario, alla riunione di apertura può essere richiesta la partecipazione del DPO / Ufficio Privacy.

A seguito della riunione di apertura, l'Auditor procede alla condivisione dei temi esplicitati all'interno della "Checklist di Privacy Audit" tramite una specifica riunione svolta con il personale del Responsabile oggetto dell'Audit.
La Checklist contempla uno specifico focus sui seguenti ambiti:

- Registro dei Trattamenti;
- Informativa;
- Base giuridica / condizioni per il consenso;
- Misure di sicurezza tecniche e organizzative;
- Richieste degli interessati;
- Data Breach;
- Data Retention;
- Trasferimenti di dati in paesi Extra UE;
- Formazione Data Protection;
- Gestione dei fornitori.

All'interno della Checklist, per ciascun ambito sopracitato, sono declinati una serie di specifici controlli volti a valutare il livello di maturità del Responsabile rispetto ai requisiti della normativa vigente.

In caso di *"Valutazione Checklist Privacy a cura del Responsabile"*, invece, l'Auditor condivide con il Responsabile la Checklist, il quale sarà tenuto a restituirla allo stesso una volta compilata, entro un periodo di tempo concordato e non superiore a 20 giorni lavorativi dalla data di condivisione della stessa.

In entrambi i casi, grazie alle informazioni reperite tramite la Checklist e alle evidenze condivise, l'Auditor attribuisce un giudizio di conformità a ciascun controllo, scegliendo tra:

- **Adeguato:** il controllo risulta applicato in modo corretto e conforme alla normativa di riferimento;
- **Parzialmente adeguato:** il controllo risulta applicato in modo parzialmente corretto;
- **Non adeguato:** il controllo risulta applicato in modo non corretto e non conforme alla normativa di riferimento;
- **Non applicabile:** il controllo risulta non applicabile al caso specifico.

In entrambe le modalità, una volta esaminati i singoli controlli della Checklist e attribuito un giudizio di conformità sulla base delle evidenze, l'Auditor avvia la stesura del Verbale di Audit.

All'interno del documento verranno formalizzate le risultanze dell'attività, successivamente condivise con tutti gli attori coinvolti.

Ove necessario, l'Auditor potrà richiedere al Responsabile approfondimenti in merito alle informazioni tracciate all'interno della Checklist oppure chiedere di integrare ulteriori evidenze utili.

Le risultanze del Privacy Audit si suddividono in:

- **Raccomandazione:** l'Auditor consiglia al Fornitore oggetto dell'audit un'azione per migliorare il controllo con l'obiettivo di modificare un elemento di carattere tecnico, organizzativo, procedurale o fisico al fine di migliorare le prestazioni e l'efficacia del servizio esternalizzato rispetto ai requisiti normativi.
- **Non conformità minore:** rilevata dall'Auditor in caso si verifichi una delle circostanze di seguito individuate:
    - l'output di una attività o di un processo affidati al Fornitore oggetto dell'audit non soddisfa completamente tutti i requisiti applicabili;
    - nel campione oggetto di esame, un requisito non viene completamente soddisfatto;
    - errore isolato, non sistematico e non ripetuto.
- **Non conformità maggiore:** rilevata dall'Auditor in caso di rischio concreto di mancata conformità di prodotti, processi e servizi affidati al Fornitore oggetto dell'audit che minaccia la compliance Privacy.
- **Controllo adeguato:** rilevato dall'Auditor in caso di conformità ai requisiti dei prodotti, processi e servizi affidati al Fornitore oggetto dell'audit.

L'Auditor deve registrare e, ove necessario, classificare (ad esempio, a seconda della priorità di intervento) all'interno del Verbale di Audit le eventuali non conformità minori e maggiori e le loro evidenze a supporto. Infine, deve riesaminarle direttamente con il Responsabile così da accertare che le evidenze a supporto siano ben circostanziate e le non conformità siano da esso ben comprese.

Una volta consultato il Responsabile, l'Auditor potrà condividere il Verbale di Audit consolidato anche con il DEC e il RUP portando così a conclusione il Privacy Audit sul Fornitore.

5.2 CONTROLLI PRIVACY E SICUREZZA NELLA GESTIONE DEI FORNITORI

L'attività di verifica nell'ambito della gestione dei Fornitori in qualità di Responsabili del trattamento non si ferma al controllo circa il rispetto di requisiti Privacy, ma si estende all'adozione di un approccio proattivo alla sicurezza dei dati personali.

Ciò implica l'impiego di adeguate misure di sicurezza tecniche e organizzative volte a proteggere i dati durante l'intero ciclo di vita degli stessi, prevenendo altresì incidenti informatici ex-ante o mitigandone gli effetti ex post. Ad esempio, per prevenire le possibili conseguenze dannose di un incidente di sicurezza, si

potrebbero adottare, così come suggerito dal GDPR, misure di sicurezza tecniche come l'anonimizzazione, la pseudonimizzazione, o la cifratura dei dati per tutelare la riservatezza delle informazioni personali, prevenendo in tal modo l'accadimento di Data Breach.

In ragione di quanto appena detto, i Fornitori aventi un contratto di fornitura in essere con Regione Calabria devono rispettare i requisiti minimi di sicurezza informatica così come definito dagli standard e framework normativi di riferimento (e.g. ISO27001, NIST cybersecurity framework, Linee guida dell'ENISA, Direttive NIS, etc.) e in accordo al corpus documentale / procedurale della Regione stessa.

A tal fine, la Direttiva del Presidente del Consiglio dei Ministri del 1° agosto 2015 "*Misure minime di Sicurezza ICT per le Pubbliche Amministrazioni*" mette a disposizione di tutte le Pubbliche Amministrazioni criteri di riferimento volti a stabilire l'adeguatezza del livello di protezione informatica garantita dal Fornitore in qualità di Responsabili del trattamento.

Perciò, Regione Calabria ha l'onere di verificare sistematicamente, non solo il rispetto della normativa vigente, ma anche il soddisfacimento dei requisiti definiti in fase di acquisizione del servizio offerto dal Fornitore presenti nel capitolato di gara e nelle dichiarazioni presenti nell'offerta tecnica dello stesso.

Il Fornitore dovrà dimostrare la conformità ai requisiti di sicurezza attraverso evidenze documentali atte a dare prova del rispetto dei controlli previsti all'interno del capitolato tecnico (e.g. esecuzione annuale di vulnerability assessment e penetration test, analisi statica e dinamica di sicurezza del codice, etc.). Regione Calabria si riserva il diritto di verificare o rieseguire autonomamente i controlli di cui sopra, mediante l'ausilio anche di soggetti terzi al bisogno abilitati. Tutte le eventuali vulnerabilità rilevate dovranno essere mitigate entro e non oltre le tempistiche stabilite da Regione Calabria, a seconda del caso di specie.

Al fine di consentire un approfondimento più ampio di quanto in parte dettagliato nel presente paragrafo circa una gestione sicura delle Terze Parti (qui unicamente Fornitori in qualità di Responsabili del trattamento), la presente Procedura rinvia al documento "*Linea guida Gestione del rischio di Terze parti*" adottato da Regione Calabria che costituisce una linea guida riportante indicazioni tecnico-amministrative e buone prassi da adottare al fine di garantire adeguati livelli di sicurezza per la gestione delle attività di procurement nell'ambito ICT.

5.3 GESTIONE DEI SUB-RESPONSABILI DEL TRATTAMENTO

Sulla base di quanto stabilito dalla normativa, un Responsabile del trattamento può avvalersi, se espressamente autorizzato dal Titolare, di sub-Fornitori (c.d. sub-Responsabili) nell'ambito delle attività di trattamento.

Tuttavia, qualora il sub-Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del sub-Responsabile.

Il terzo soggetto deve, comunque, ricoprire il ruolo di sub-Responsabile mediante opportuna nomina (in Regione Calabria "*Richiesta autorizzazione nomina Sub-responsabili del trattamento*") che lo vincoli ai medesimi obblighi contrattualizzati dal Responsabile verso il Titolare.

Ciò significa che il Responsabile dovrà sottoporre la nomina del sub-Responsabile al Titolare, al fine di ottenerne l'autorizzazione; questa si intenderà rilasciata se il Titolare non notifica la propria opposizione al Responsabile nei tempi previsti.

A questo punto, il dovere del Titolare di garantire ai soggetti interessati la conformità alla normativa vigente si estenderà anche al sub-Responsabile, il quale sarà obbligato a fornire tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa, consentendo e contribuendo alle attività di revisione effettuate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

6. ALLEGATI ALLA PROCEDURA

Titolo Allegato	Codice Allegato
Atto di nomina del Responsabile del trattamento dei dati personali	Allegato A
Richiesta autorizzazione nomina Sub-responsabili del trattamento	Allegato B
Checklist Privacy Audit	Allegato C
Modello Verbale di Privacy Audit	Allegato D

ALLEGATO A

Atto di nomina del Responsabile del trattamento dei dati personali

ai sensi dell'art. 28 del Regolamento (UE) 2016/679

VISTO il contratto CIG n. *<inserire numero>*, stipulato in data *<inserire data>*, concernente il "*<inserire titolo>*" (di seguito Contratto), con cui Regione Calabria ha affidato le attività ivi descritte *<inserire "alla società" nome-società, oppure, nel caso di raggruppamenti, inserire ad esempio "al Raggruppamento Temporaneo d'Imprese costituito da" nome-mandataria (mandataria), nome-mandante-1 (mandante), nome-mandante-2 (mandante), etc.>*

CONSIDERATO che le attività oggetto del Contratto comportano o possono comportare il trattamento di dati personali, ai sensi del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito Regolamento) nonché del D. Lgs. 196/2003 e ss.mm.ii recante il Codice in materia di protezione dei dati personali (di seguito Codice);

VISTO, in particolare, l'art. 4, paragrafo 1, n. 7) del Regolamento, che individua il Titolare del trattamento ne "*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 […]*" e visto altresì l'art. 4, paragrafo 1, n. 8) del Regolamento, che identifica il Responsabile del trattamento ne "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*";

VISTO l'art. 28, paragrafo 1 del Regolamento, secondo cui "*qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*";

CONSIDERATA l'idoneità, alla luce dell'attività istruttoria e di gara già svolta, di *<inserire responsabile trattamento>* rispetto alle garanzie richieste dalla normativa regolamentare europea con riferimento all'adeguatezza delle misure tecniche e organizzative per la tutela dei diritti dell'interessato;

REGIONE CALABRIA

con sede legale c/o Cittadella Regionale - Viale Europa, Località Germaneto 88100 - Catanzaro, in persona del dott. *<inserire nome delegato del titolare del trattamento>*, dirigente del *<inserire dipartimento o settore>*, in qualità di delegato del Titolare del trattamento dei dati personali con riferimento alle attività oggetto del Contratto,

NOMINA

la società *<inserire responsabile trattamento>* p. iva *<inserire p.iva>*, in persona del dott. *<inserire nome legale rappresentante>*, Legale Rappresentante *pro tempore*, con sede legale in *<inserire città>*, *<inserire indirizzo>*, quale **Responsabile del trattamento dei dati personali**, ai sensi e per gli effetti dell'art. 28 del Regolamento, con riferimento alle attività di cui al Contratto che qui si intente integralmente richiamato.

Il Responsabile effettua, per conto del Titolare, il trattamento dei dati personali necessario per lo svolgimento delle attività disciplinate dal Contratto.

In particolare, il trattamento dei dati personali è così individuato:

- Oggetto: *<inserire una descrizione sommaria delle attività/servizi di cui al Contratto, con particolare focus sulla specifica attività che coinvolge il trattamento di dati personali>*;
- Durata: sino alla scadenza del Contratto;
- Finalità: esecuzione del Contratto;
- Tipologia di dati personali trattati: *<inserire tipologie di dati>*;
- Categorie di interessati: *<inserire categorie interessati (sempre persone fisiche)>*.

Per la durata del Contratto e per le attività in esso disciplinate, il Responsabile del trattamento dei dati personali designato, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, della tipologia di dati personali trattati, delle categorie di interessati nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, si impegna nei confronti del Titolare a:

1 trattare i dati personali nel rispetto dei princìpi e delle disposizioni previsti dal Codice, dal Regolamento, dagli indirizzi e dai provvedimenti a carattere generale emanati dal Garante in materia di protezione dei dati personali e da ogni altra vigente normativa in materia di protezione dei dati personali;

2 non trasferire, né in tutto né in parte, in un Paese terzo o a un'organizzazione internazionale i dati personali trattati ai sensi del Contratto, senza la previa autorizzazione del Titolare;

3 nel trattare i dati personali per conto del Titolare, attenersi alle istruzioni documentate fornite dal Titolare stesso, anche in caso di eventuale trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o la normativa nazionale; in tal caso, il Responsabile del trattamento si impegna a informare il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

Sono considerate istruzioni documentate le prescrizioni previste dal Contratto, dagli eventuali suoi allegati e dalla presente designazione, le "*Misure minime di sicurezza ICT per le pubbliche amministrazioni*" e le "*Linee guida per lo sviluppo del software sicuro*" pubblicate dall'AGID, quando applicabili, e ogni altra eventuale comunicazione scritta del Titolare concernente le modalità di trattamento dei dati da parte del Responsabile.

Il Responsabile informerà il Titolare qualora ritenga che un'istruzione impartitagli da quest'ultimo violi il Regolamento o altre disposizioni europee o nazionali relative alla protezione dei dati;

4 attraverso misure tecniche e organizzative adeguate alla natura del trattamento, assistere il Titolare nell'adempimento dei propri obblighi derivanti dall'esercizio, da parte degli interessati, dei diritti di cui alla Sezione 3 del Regolamento;

5 adottare tutte le misure di sicurezza di cui all'art. 32 del Regolamento.

Nel caso in cui il trattamento, per la propria natura, il contesto e/o le tecnologie utilizzate, necessitasse di una valutazione d'impatto sulla protezione dei dati e/o evidenziasse la necessità di approntare ulteriori misure di sicurezza, il Titolare potrà richiedere al Responsabile l'implementazione di tali misure.

Nei casi in cui si evidenziasse una non piena corrispondenza tra la tipologia di trattamento prevista dal Contratto e le misure di sicurezza richieste, il Responsabile si impegna a comunicarlo per scritto al Titolare, fornendo al medesimo l'effettuata analisi del rischio e indicando le misure di sicurezza ritenute adeguate;

6 assistere il Titolare nel garantire il rispetto degli obblighi concernenti la sicurezza dei dati personali (in particolare: sicurezza del trattamento, notifica della violazione dei dati personali al Garante per la protezione dei dati personali e relativa comunicazione all'interessato), la valutazione d'impatto sulla protezione dei dati e la consultazione preventiva con il Garante, ai sensi degli articoli da 32 a 36 del Regolamento, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile;

7 non ricorrere a un altro Responsabile senza la previa autorizzazione scritta del Titolare.

Ogniqualvolta il Titolare autorizzi il ricorso del Responsabile ad altro Responsabile per l'esecuzione di specifiche attività di trattamento, a tale altro Responsabile sono imposti, mediante la stipula di un

contratto o altro atto giuridico sottoscritto dai Responsabili stessi, i medesimi obblighi in materia di protezione dei dati personali contenuti nella presente designazione, con l'espressa presa d'atto dell'odierno Responsabile in merito alla sussistenza, in capo al Responsabile dal medesimo designato, delle garanzie sufficienti alla messa in atto delle misure tecniche e organizzative adeguate richieste dal Regolamento.

Qualora il Responsabile del trattamento designato dall'odierno Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, l'odierno Responsabile conserva, nei confronti del Titolare del trattamento, l'intera responsabilità dell'adempimento di tali obblighi;

8 garantire che i propri dipendenti e/o le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza e, in ogni caso, che abbiano ricevuto la formazione necessaria;

9 ai sensi dell'art. 30, comma 2 del Regolamento, tenere il registro delle categorie di attività relative al trattamento dei dati personali effettuate per conto del Titolare e, su richiesta, mettere tale registro a disposizione del Titolare e/o del Garante per la protezione dei dati personali;

10 mettere a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di cui alla presente designazione e di cui all'art. 28 del Regolamento nonché consentire e contribuire alle attività di revisione, comprese le ispezioni, eseguite dal Titolare o da altro soggetto da questi incaricato;

11 a scelta e su richiesta del Titolare, cancellare o restituire al medesimo tutti i dati personali al termine del Contratto o comunque della prestazione dei servizi relativi al trattamento nonché cancellare le copie esistenti, salvo che il diritto dell'Unione o la normativa nazionale prevedano la conservazione dei dati.

Per quanto non espressamente previsto dalla presente designazione, si fa espresso riferimento alla normativa, sia europea sia nazionale, in materia di protezione dei dati personali nonché al Contratto.

<inserire luogo e data>

REGIONE CALABRIA

<inserire nome delegato del titolare, timbro e firma>

<inserire nome-società>

<inserire nome legale rappresentante, timbro e firma>

ALLEGATO B

Richiesta autorizzazione nomina Sub-responsabili del trattamento

ai sensi dell'art. 28 del Regolamento (UE) 2016/679

In riferimento al contratto esecutivo CIG n. <inserire numero> stipulato in data <inserire data> (nel seguito "Contratto") e alla nomina del Responsabile del trattamento dei dati, prot. n. <inserire protocollo> del <inserire data>,

la società <inserire dati societari> (nel seguito "Fornitore"), in qualità di Responsabile del trattamento dei dati personali, nominata da Regione Calabria,

PREMESSO CHE

- per l'esecuzione di specifiche attività di trattamento connesse all'esecuzione del Contratto citato è necessario avvalersi di soggetti esterni alla propria organizzazione,
- a tal fine sono state individuate le società indicate nella tabella riportata a seguire,
- ai sensi dell'art. 28 del Regolamento (UE) 2016/679, tali società devono essere nominate Sub-responsabili del trattamento,

TUTTO CIÒ PREMESSO

il Fornitore chiede a Regione Calabria l'autorizzazione a nominare le società indicate nella tabella riportata a seguire quali Sub-responsabili del trattamento dei dati personali dei quali Regione Calabria è Titolare del trattamento.

Per ciascuna società indicata nella tabella riportata a seguire, il Fornitore dichiara di aver stipulato un apposito contratto che prevede obblighi e garanzie in materia di protezione dei dati personali.

Nome del Sub-responsabile	**Sede legale e dati societari**	**Luogo del trattamento**	**Servizi erogati**	**Misure trasferimento dati extra UE[1]**

<inserire luogo e data

<inserire nome Fornitore >

<inserire nome legale rappresentante, timbro e firma>

Per accettazione:

REGIONE CALABRIA

<inserire nome delegato del titolare, timbro e firm

[1] Eventuali misure di sicurezza attuate per il trasferimento dei dati extra UE, se applicabile.

ALLEGATO C

Checklist Privacy Audit sui Fornitori Responsabili del trattamento di dati personali

ID	Normativa di riferimento	Articolo	Ambito	Obiettivo del controllo	Descrizione del controllo
1	GDPR	Articolo 30	Registro dei trattamenti	Redazione del Registro dei Trattamenti	Il Fornitore ha mappato nel Registro dei trattamenti, in qualità di Responsabile del Trattamento, i trattamenti di dati svolti nell'ambito dei processi assegnati da Data Processing Agreement?
2	GDPR	Articolo 13	Informativa	Informativa agli interessati	All'interno dell'informativa rilasciata dal Fornitore si chiarisce come viene gestita la raccolta, l'elaborazione e la conservazione dei dati personali dei clienti che potrebbero essere coinvolti nei servizi forniti?
3	GDPR	Articolo 13	Informativa	Informativa agli interessati	L'informativa è facilmente reperibile per il cliente? (es. disponibile all'accesso nella sede del fornitore o da esibire a richiesta di chi accede nelle sedi)
4	GDPR	Articoli 6 e 7	Base giuridica/ condizioni per il consenso	Richiesta consenso	In caso di raccolta del consenso per trattamento dei dati, il Fornitore è in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali?
5	GDPR	Articolo 32	Misure tecniche ed organizzative	Implementazione delle misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio	Il Fornitore adotta misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del regolamento, tutelando i diritti degli interessati?
6	GDPR	Articolo 32	Misure tecniche ed organizzative	Implementazione delle misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio	Il Fornitore adotta misure tecniche ed organizzative adeguate, quali la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento al fine di garantire un livello di sicurezza adeguato al rischio? (Business Continuity)
7	GDPR	Articolo 32	Misure tecniche ed organizzative	Implementazione delle misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio	Il Fornitore adotta misure tecniche ed organizzative adeguate, quali la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico al fine di garantire un livello di sicurezza adeguato al rischio?
8	GDPR	Articolo 32	Misure tecniche ed organizzative	Implementazione delle misure tecniche ed organizzative per	Il Fornitore aggiorna e revisiona le misure di sicurezza al fine di garantire la sicurezza del trattamento?

				garantire un livello di sicurezza adeguato al rischio	
9	GDPR	Articolo 32	Misure tecniche ed organizzative	Implementazione delle misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio	Il Fornitore ha adottato misure per garantire che chiunque tratti i dati personali nell'ambito dell'attività assegnata sia stato autorizzato al trattamento dei dati e adeguatamente istruito?
10	GDPR	Articolo 32	Misure tecniche ed organizzative	Implementazione delle misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio	Il Fornitore ha censito i sistemi IT utilizzati per la gestione dei dati personali nell'ambito delle attività svolte? Sono adottate valutate e implementate adeguate misure di sicurezza IT (es. pseudonimizzazione, cifratura) per prevenire l'accesso non autorizzato ai dati personali mediante questi sistemi? (VA PT)
11	GDPR	Articolo 32	Misure tecniche ed organizzative	Implementazione delle misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio	Il Fornitore ha definito le impostazioni di default dei propri sistemi al fine di garantire che i dati personali non siano resi accessibili a un numero indefinito di persone e che gli interessati siano in grado di controllare la distribuzione dei propri dati personali? (Minimizzazione del dato)
12	GDPR	Articolo 32	Misure tecniche ed organizzative	Implementazione delle misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio	Il Fornitore ha definito le impostazioni dei propri sistemi al fine di garantire che siano raccolti solo i dati necessari per ogni specifica finalità del trattamento? (Limitazione del trattamento)
13	GDPR	Articolo 32	Misure tecniche ed organizzative	Implementazione delle misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio	Il Fornitore comunica prontamente al Titolare di tutte le questioni rilevanti ai sensi del GDPR e della normativa italiana di recepimento?
14	GDPR	Articolo 32	Misure tecniche ed organizzative	Gestione nomina Amministratori di sistema	Qualora per l'espletamento dei servizi forniti sia richiesta la nomina di Amministratori di sistema, l'adempimento è garantito a tutte le disposizioni contenute nella Delibera del 27 novembre 2008 emanata dall'Autorità Garante per la Protezione degli Amministratori di Sistema (Decisione 27 novembre 2008, come successivamente modificato)?
15	GDPR	Articoli 15 e 21	Richieste degli interessati	Comunicazione delle richieste degli interessati	Nel caso in cui pervengano richieste da parte dei soggetti interessati, il Fornitore comunica tempestivamente tali richieste al Titolare?
16	GDPR	Articolo 33	Data Breach Notification	Comunicazione di Data Breach	In caso di Data Breach, il Fornitore ha segnalato la violazione di dati personali avvenuta sui dati trattati

					per conto del Titolare nelle modalità e nelle tempistiche definite all'interno del contratto (DPA)?
17	GDPR	Articolo 5	Data Retention	Gestione Data Retention	Il Fornitore conserva i dati personali secondo i tempi di conservazione definiti? Il Fornitore si è dotato di una policy di data retention? I dati vengono cancellati/anonimizzati dopo la scadenza del periodo di conservazione? Tali operazioni sono documentate?
18	GDPR	Articolo 44 e ss.	Trasferimenti di dati in paesi Extra UE	Gestione dei trasferimenti di dati in paesi Extra UE	Nel caso di trasferimento di dati verso paesi extra UE, il Fornitore ha rispettato le condizioni previste dal Regolamento, conducendo preliminarmente tutte le valutazioni necessarie? Tali valutazioni sono documentate?
19	GDPR	Articolo 29	Formazione Data Protection	Definizione di un piano di formazione privacy interna	Il Fornitore prevede un sistema di formazione interna in ambito privacy?
20	GDPR	Articolo 28	Responsabile del trattamento	Richiesta autorizzazione per la nomina del sub-Fornitore	In caso di nomina di un sub Fornitore, il Fornitore richiede un'autorizzazione (generale o specifica) al Titolare?
21	GDPR	Articolo 28	Gestione dei fornitori	Gestione del contratto con il sub- Fornitore	Nell'atto giuridico stipulato dal Fornitore con un altro Fornitore (sub-responsabile) sono presenti i seguenti elementi: - i ruoli assunti dalle parti - il tipo di dati personali coinvolti nel trattamento e (eventuali) limitazioni al loro utilizzo - il coinvolgimento (eventuale) di ulteriori soggetti terzi che operano quali sub-responsabili del trattamento - le regole per il trasferimento di dati personali verso paesi non appartenenti allo Spazio Economico Europeo (SEE) - le regole per effettuare verifiche e controlli sull'operato del sub-responsabile e, per il suo tramite su altri ed eventuali sub-responsabili - la durata del contratto e le modalità, ove previste, di restituzione e/o cancellazione dei dati al termine del contratto stesso - la presenza di specifiche misure di sicurezza tecniche, fisiche ed organizzative e l'indicazione di chi è responsabile della loro applicazione - il ruolo assunto dalle parti nel caso di violazione dei dati personali (c.d. Data Breach)?
22	GDPR	Articolo 28	Gestione dei fornitori	Gestione del contratto con il sub- Fornitore	Il Fornitore garantisce che i sub-fornitori selezionati assicurino gli stessi obblighi definiti all'interno del contratto tra il Fornitore e Titolare?

23	GDPR	Articolo 28	Gestione dei fornitori	Gestione del contratto con il sub- Fornitore	E' manutenuta una lista di aziende sub-fornitrici da parte del Fornitore? Tale lista è aggiornata e comunicata al Titolare?

ALLEGATO D

Verbale di Privacy Audit sul Fornitore in qualità di Responsabile del trattamento di dati personali

REGIONE CALABRIA	Verbale di Privacy Audit sul Fornitore in qualità di Responsabile del trattamento di dati personali			
Riferimenti Audit	**ID**	**Modalità di svolgimento**	**Norme di riferimento**	
			Regolamento UE 679/2016 "GDPR"	
Data e ora	Il giorno ____/____/____ dalle __:__ alle __:__		**Punti della norma verificati**	In forza dell'art. 28 del GDPR e sono stati verificati la conformità alla normativa vigente del Fornitore in relazione alle attività che lo stesso esegue per conto del Titolare.
Società				
Sede				
Intervistati				
Lead Auditor / Auditor				
Documenti di riferimento				
Evidenze raccolte e analizzate				
Valutazioni				
Raccomandazioni per il miglioramento	-			
Non conformità				

Lead Auditor / Auditor

_____

Nome Cognome

Responsabile Fornitore

_____

Nome Cognome

Luogo, Data __/__/____