R.R. N. 8/2025 ORIGINALE

Deliberazione Giunta n. 188 del 3 aprile 2025

OGGETTO: Adozione del regolamento concernente “Modifiche al Regolamento regionale 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale) e successive modificazioni.”

PUBBLICATA: BUR Lazio 8 aprile 2025, n. 28

Regolamento regionale 4 aprile 2025 n. 8

OGGETTO: Modifiche al Regolamento regionale 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale) e successive modificazioni.

PUBBLICATO: BUR Lazio 8 aprile 2025, n. 28

(TESTO DEL REGOLAMENTO DA INSERIRE)

Art. 1

(*Inserimento dell’articolo 28 ter al regolamento regionale 6 settembre 2002, n. 1 e successive modificazioni)*

1. Dopo l’articolo 28 bis del r.r. 1/2002 e successive modifiche, è inserito il seguente:

“Art. 28 ter
(*Sistema di Contrasto al Riciclaggio e al finanziamento del Terrorismo*)

1. Per le finalità di contrasto al riciclaggio e al finanziamento del terrorismo, in conformità con le disposizioni di cui all’articolo 10 del decreto legislativo 21 novembre 2007, n. 231, le strutture organizzative della Giunta regionale applicano il Sistema di Contrasto al Riciclaggio ed al finanziamento del Terrorismo (SiCoRiTe), previsto nell’Allegato “SS” al presente regolamento.”.

Art. 2

(Modifiche all’articolo 474 del regolamento regionale 6 settembre 2002, n. 1 e successive modificazioni)

1. All’articolo 474 del r.r. 1/2002 e successive modificazioni, sono apportate le seguenti modifiche:

a) alla fine della lettera d) del comma 3, sono aggiunte le parole: “, fatto salvo il ruolo di Titolare autonomo per quanto concerne le attività giudiziarie”;
b) dopo il comma 3, è inserito il seguente:
“3 bis. I soggetti designati possono essere inoltre individuati dal Titolare, anche al di fuori delle strutture regionali, se, pur agendo sotto l’autorità del Titolare, svolgano compiti e funzioni attribuiti dalla legge con autonomi poteri di iniziativa e controllo. Il Titolare definisce in uno specifico atto di designazione, il perimetro e le modalità di esercizio delle attività di trattamento.”;
c) al comma 5, le parole: “e i soggetti designati di cui al comma 3, autorizzano;” sono sostituite dalle seguenti: “, per il tramite dei soggetti designati, previsti nel comma 3, autorizza,”.

Art. 3

(Modifiche all’articolo 474 ter del regolamento regionale 6 settembre 2002, n. 1 e successive modificazioni)

1. All’articolo 474 ter del r. r. 1/2002 e successive modificazioni, sono apportate le seguenti modifiche:
a) la lettera o) del comma 1, è sostituita dalla seguente:
“o) richiedere al DPO, se ritenuto necessario, il parere circa la valutazione d’impatto effettuata anche ai fini della consultazione preventiva, prevista dall’articolo 36 del RGPD;”;
b) dopo la lettera r-sexies) del comma 1, sono aggiunte le seguenti:
“r-septies) predisporre memorie difensive o controdeduzioni, in caso di avvio di procedimenti da parte del Garante, nonché gli atti necessari al pagamento di eventuali sanzioni amministrative comminate riguardanti trattamenti di propria competenza;
r-octies) designare, sotto la propria responsabilità, anche al di fuori delle strutture regionali, con specifico atto, persone fisiche che, pur agendo sotto l’autorità del Titolare, svolgano compiti e funzioni attribuiti dalla legge con autonomi poteri di iniziativa e controllo.”.

Art. 4

(Modifiche all’articolo 474 quinquies del regolamento regionale 6 settembre 2002, n. 1 e successive modificazioni)

1. All’articolo 474 quinquies del r.r. 1/2002 e successive modificazioni, sono apportate le seguenti modifiche:
a) la rubrica è sostituita dalla seguente: “Soggetti autorizzati”;
b) al comma 1:
   1) le parole: “e i soggetti designati di cui al comma 3 autorizzano” sono sostituite dalle seguenti: “per il tramite dei soggetti designati, previsti nel comma 3 dell’art. 474, autorizza”;
   2) la parola: “incaricati” è sostituita dalla seguente: “autorizzati”;
c) al comma 3, la parola: “incaricati” è sostituita dalla seguente: “autorizzati”.

Art. 5

(Modifiche all'articolo 476 del regolamento regionale 6 settembre 2002, n. 1 e successive modificazioni)

1. All'articolo 476 del r.r. 1/2002 e successive modificazioni, sono apportate le seguenti modifiche:

a) al comma 1, le parole: "in tema di risorse strumentali e di competenze" sono sostituite dalle seguenti: ", per quanto di competenza, fatti salvi i compiti e le funzioni assegnati ai soggetti designati per i sistemi di loro titolarità, ai sensi dell'articolo 474, commi 3 e 7 del presente regolamento."

b) al comma 2:

1) le parole: "gestione della sicurezza delle informazioni" sono sostituite dalle seguenti: "protezione dei dati personali";

2) la lettera c), è sostituita dalla seguente:

"c) supporta le strutture regionali nelle attività di trattamento dei dati personali, nonché nell'applicazione della normativa vigente e delle policy regionali in materia di protezione dei di dati personali.";

3) la lettera d), è abrogata.

Art. 6

(Modifica all'allegato MM al regolamento regionale 6 settembre 2002 n. 1 e successive modificazioni)

1. Alla fine del paragrafo 3 dell'allegato MM del r.r. 1/2002 e successive modificazioni, sono aggiunte le parole: "A insindacabile giudizio del DPO o su esplicita richiesta del Soggetto interessato, anche per fini di rilevante riservatezza degli istanti, è prevista la possibilità che il DPO gestisca direttamente e in piena autonomia, alcuni reclami o segnalazioni in materia di protezione dei dati personali."

Art. 7

(Modifiche allo schema B dell'allegato NN al regolamento regionale 6 settembre 2002, n. 1 e successive modificazioni)

1. Allo schema B dell'allegato NN del r.r. 1/2002 e successive modificazioni, sono apportate le seguenti modifiche:

a) ovunque ricorra la parola "incaricato", questa è sostituita con "autorizzato";

b) ove ricorra la parola "incaricati", questa è sostituita con "autorizzati".

Art. 8

(Modifica allo schema E dell'allegato NN al regolamento regionale 6 settembre 2002, n. 1 e successive modificazioni)

1. Lo schema E dell'allegato NN del r.r. 1/2002 e successive modificazioni, è abrogato.

Art. 9

(Modifica allo schema F dell'allegato NN al regolamento regionale 6 settembre 2002, n. 1 e successive modifiche)

1. Lo schema F dell'allegato NN del r.r. 1/2002 e successive modificazioni, è abrogato.

Art. 10

(Sostituzione dello schema G dell'allegato NN al regolamento regionale 6 settembre 2002, n. 1 e successive modificazioni)

1. Lo schema G dell'allegato NN al r.r. 1/2002 e successive modificazioni, è sostituito dal seguente:

"SCHEMA G

(art. 474, c. 2)

ATTO DI DISCIPLINA DEI TRATTAMENTI SVOLTI DAL RESPONSABILE DEL TRATTAMENTO PER CONTO DEL TITOLARE DEL TRATTAMENTO

AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 679/2016

NOTA ESPLICATIVA: scegliere l'opzione coerente:

- Allegato __ alla determinazione dirigenziale n.___del ___

oppure

- Allegato __ alla deliberazione di Giunta Regionale n._____del ___

TRA

La Giunta Regionale del Lazio, con sede in Via R. Raimondi Garibaldi 7– 00147 Roma, codice fiscale 80143490581, nella persona del/lla Dott./Dott.ssa _____in qualità di Direttore della "*Direzione* _____", autorizzato alla sottoscrizione del presente contratto, in virtù dei poteri conferiti con la Deliberazione di Giunta Regionale n._____ del gg/mese/aaaa, (di seguito anche il "Titolare" o "Regione Lazio");

E

La _____<*indicare ragione e denominazione sociale della Società*>, con sede in _____, n. _____ – cap._____, città _____ nella persona del Dott./Dott.ssa _____, nella sua qualità di _____ in virtù dei poteri conferiti con _____ (di seguito anche la "Società", il "Responsabile" o il "Responsabile del trattamento");

VISTI

- il 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 (di seguito anche "RGPD" o "Regolamento (UE) 2016/679"), il quale garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento al diritto alla protezione dei dati personali;
- il decreto legislativo 196/2003 "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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" e successive modificazioni;
- le Clausole Contrattuali Tipo (anche dette "SCC") tra Titolari del trattamento e Responsabili del trattamento, adottate a norma dell'articolo 28 del Regolamento (UE) 2016/679 (in seguito anche "GDPR") con la Decisione di esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021 che definisce le modalità con le quali il Responsabile del trattamento si impegna ad effettuare per conto del Titolare le operazioni di trattamento dei dati personali;
- l'articolo 474, comma 2, del regolamento regionale 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della Giunta Regionale) e successive modificazioni, il quale prevede che il Titolare del trattamento, con specifico atto negoziale di incarico ai singoli responsabili del trattamento, disciplini i trattamenti affidati al Responsabile, i compiti e le istruzioni secondo quanto previsto dall'articolo 28, paragrafo 3, del Regolamento (UE) 2016/679 e in coerenza con le indicazioni del Responsabile della Protezione dei Dati del Titolare (di seguito anche "DPO"); nell'atto di incarico è, altresì, definita la possibilità di nomina di uno o più sub-responsabili, secondo quanto previsto dall'articolo 28, paragrafi 2 e 4, del Regolamento (UE) 2016/679;

NOTA ESPLICATIVA: aggiungere se ricorre la fattispecie

- il Provvedimento del Garante per la Protezione dei Dati Personali 27/11/2008 (Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema) e successive modificazioni, pubblicato sulla Gazzetta Ufficiale n. 300 del 24/12/2008, il quale prevede la designazione individuale degli Amministratori di Sistema (System Administrator), degli Amministratori di Base Dati (Database Administrator), degli Amministratori di Rete (Network Administrator) e degli Amministratori di Software Complessi, che, nell'esercizio delle proprie funzioni, hanno accesso, anche fortuito, a dati personali (di seguito anche "AdS");
- il provvedimento dell'Agenzia per l'Italia Digitale (di seguito anche "AgID"), (Misure minime di sicurezza ICT per le Pubbliche Amministrazioni"), adottato in attuazione della Direttiva del

Presidente del Consiglio dei ministri 1° agosto 2015 (di seguito per brevità “Misure minime AgID), che ha dettato le regole da osservare per garantire un uso appropriato dei privilegi di AdS;

PREMESSO CHE

- la Giunta Regionale del Lazio, in qualità di Titolare del trattamento che svolge attività che comportano il trattamento di dati personali nell’ambito dei propri compiti istituzionalmente affidati, è tenuta a mettere in atto misure tecniche e organizzative, volte ad attuare in modo efficace i principi di protezione dei dati e adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
- le attività, erogate in esecuzione del Contratto <indicare riferimenti del contratto>, tra la Giunta Regionale del Lazio e <indicare ragione e denominazione sociale della Società>, implicano da parte di quest’ultima, il trattamento dei dati personali di cui è Titolare la Giunta regionale del Lazio, ai sensi di quanto previsto dal Regolamento (UE) 2016/679;
- l’articolo 4, n. 2) del RGPD definisce “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, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- l’articolo 4, n. 7) del RGPD definisce “Titolare del trattamento”: la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; 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;
- l’art. 4, n. 8) del RGPD definisce “Responsabile del trattamento”: la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
- l’articolo 28, punto 6 del RGPD prevede che “Fatto salvo un contratto individuale tra il Titolare del trattamento e il Responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al Titolare del trattamento o al Responsabile del trattamento ai sensi degli articoli 42 e 43”;
- il presente contratto si basa sulle Clausole Contrattuali Tipo tra Titolari del trattamento e Responsabili del trattamento, adottate con la Decisione di esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021 sopra richiamata;
- ai sensi dell’articolo 28, paragrafo 1 del RGPD, la Società presenta garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento dei dati personali di cui la Giunta Regionale Lazio è Titolare soddisfi i requisiti e il pieno rispetto delle disposizioni previste dal RGPD;

Tutto ciò premesso, le parti stipulano e convengono quanto segue:

SEZIONE I

Clausola 1

Scopo e ambito di applicazione

a) scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, 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);
b) il Titolare del trattamento ed il Responsabile del trattamento di cui all'allegato I accettano le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del Regolamento (UE) 2016/679;
c) le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.
d) gli allegati da I a VI costituiscono parte integrante delle clausole;
e) le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il Titolare del trattamento a norma del Regolamento (UE) 2016/679;
f) le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del Regolamento (UE) 2016/679.

Clausola 2

Invariabilità delle clausole

a) le parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati;
b) quanto previsto alla lettera a) non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Clausola 3

Interpretazione

c) quando le presenti clausole utilizzano i termini definiti nel Regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui al Regolamento stesso;
d) le presenti clausole vanno lette e interpretate alla luce delle disposizioni del Regolamento (UE) 2016/679;
e) le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal Regolamento (UE) 2016/679, o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Clausola 4

Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

Clausola 5 *(facoltativa)*

Clausola di adesione successiva

a) qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le parti, aderire alle presenti clausole in qualunque momento, in qualità di Titolare del

trattamento o di Responsabile del trattamento, compilando gli allegati e firmando l'allegato I;

b) una volta compilati e firmati gli allegati di cui alla lettera a), l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un Titolare del trattamento o di un Responsabile del trattamento, conformemente alla sua designazione nell'allegato I;

c) l'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II
OBBLIGHI DELLE PARTI

Clausola 6

Descrizione del trattamento

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del Titolare del trattamento, sono specificati nell'allegato II.

Clausola 7

Obblighi delle parti

7.1. Istruzioni

a) il Responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del Titolare del trattamento, 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 del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il Titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate;

b) il Responsabile del trattamento informa immediatamente il Titolare del trattamento qualora, a suo parere, le istruzioni del Titolare del trattamento violino il Regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. Limitazione delle finalità

Il Responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del Titolare del trattamento.

7.3. Durata del trattamento dei dati personali

Il Responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato II.

7.4. Sicurezza del trattamento

a) Il Responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III, per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza, che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di

applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati;

b) Il Responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento al proprio personale, soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il Responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. Dati "sensibili" o "particolari"

Se il trattamento riguarda dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili» o «particolari», ai sensi dell'articolo 9 del RGPD), il Responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari. Tali garanzie supplementari vanno esplicitate nell'allegato III.

7.6. Documentazione e rispetto

a) le parti devono essere in grado di dimostrare il rispetto delle presenti clausole;
b) il Responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del Titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole;
c) il Responsabile del trattamento mette a disposizione del Titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal Regolamento (UE) 2016/679. Su richiesta del Titolare del trattamento, il Responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il Titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del Responsabile del trattamento;
d) il Titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del Responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole, non inferiore a 10 giorni;
e) su richiesta, le parti mettono a disposizione delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. Ricorso a sub-responsabili del trattamento (ulteriori responsabili)

a) il Responsabile del trattamento ha l'autorizzazione generale del Titolare del trattamento per ricorrere a ulteriori responsabili del trattamento (nel documento anche "sub- responsabili"), sulla base di un elenco concordato. Il Responsabile del trattamento informa per iscritto il Titolare del trattamento in merito all'aggiunta o alla sostituzione di sub-responsabili del trattamento nel suddetto elenco, con un anticipo di almeno 15 giorni, dando così al Titolare del trattamento tempo sufficiente per potersi opporre. Il Responsabile del trattamento fornisce al Titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione;
b) qualora il Responsabile del trattamento ricorra a un sub-Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del Responsabile del trattamento), stipula un contratto che impone al sub-Responsabile del trattamento gli stessi obblighi in materia

di protezione dei dati imposti al Responsabile del trattamento conformemente alle presenti clausole. Il Responsabile del trattamento, si assicura che il sub-Responsabile del trattamento rispetti gli obblighi cui il Responsabile del trattamento è soggetto a norma delle presenti clausole e del Regolamento (UE) 2016/679;

c) su richiesta del Titolare del trattamento, il Responsabile del trattamento fornisce copia del contratto stipulato con il sub-Responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti d'ufficio o altre informazioni riservate, compresi i dati personali, il Responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia;

d) il Responsabile del trattamento resta pienamente Responsabile nei confronti del Titolare del trattamento dell'adempimento degli obblighi del sub-Responsabile derivanti dal contratto che questi ha stipulato con il Responsabile del trattamento. Il Responsabile del trattamento notifica al Titolare del trattamento qualunque inadempimento, da parte del sub-Responsabile del trattamento, degli obblighi contrattuali;

e) il Responsabile del trattamento concorda con il sub-Responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il Responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il Titolare del trattamento ha diritto di risolvere il contratto con il sub- Responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

7.8. Trasferimenti internazionali

a) qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del Responsabile del trattamento è effettuato soltanto su istruzione documentata del Titolare del trattamento o per adempiere ad un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il Responsabile del trattamento, e nel rispetto del capo V del Regolamento (UE) 2016/679;

b) il Titolare del trattamento conviene che, qualora il Responsabile del trattamento ricorra a un sub Responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del Titolare del trattamento) e tali attività comportino il trasferimento di dati personali ai sensi del capo V del Regolamento (UE) 2016/679, il Responsabile del trattamento e il sub-Responsabile del trattamento possono garantire il rispetto del capo V del Regolamento (UE) 2016/679, utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del Regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

Clausola 8

Assistenza al Titolare del trattamento

a) il Responsabile del trattamento notifica prontamente al Titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal Titolare del trattamento;

b) il Responsabile del trattamento assiste il Titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e alla presente lettera, il Responsabile del trattamento si attiene alle istruzioni del Titolare del trattamento;

c) oltre all'obbligo di assistere il Titolare del trattamento in conformità della lettera b), il Responsabile del trattamento assiste il Titolare del trattamento anche nel garantire il rispetto dei

seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del Responsabile del trattamento:

1) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
2) l'obbligo, prima di procedere al trattamento, di consultare le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio;
3) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il Titolare del trattamento qualora il Responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;
4) gli obblighi di cui all'articolo 32 Regolamento (UE) 2016/679;

d) le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il Responsabile del trattamento è tenuto ad assistere il Titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Clausola 9

Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il Responsabile del trattamento coopera con il Titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del Regolamento (UE) 2016/679, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento stesso.

9.1. Violazione riguardante dati trattati dal Titolare del trattamento

In caso di una violazione dei dati personali trattati dal Titolare del trattamento, il Responsabile del trattamento, assiste il Titolare del trattamento:

a) nel notificare la violazione dei dati personali alle autorità di controllo competenti, senza ingiustificato ritardo, dopo che il Titolare del trattamento ne è venuto a conoscenza (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del Regolamento (UE) 2016/679 devono essere indicate nella notifica del Titolare del trattamento e includere almeno:
    1) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati, nonché le categorie e il numero approssimativo di registrazioni dei dati personali;
    2) le probabili conseguenze della violazione dei dati personali;
    3) le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali, anche, qualora necessario, per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

c) nell'adempiere, in conformità dell'articolo 34 del Regolamento (UE) 2016/679, all'obbligo di comunicare, senza ingiustificato ritardo, la violazione dei dati personali all'interessato, qualora

la violazione degli stessi dati sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2. Violazione riguardante dati trattati dal Responsabile del trattamento

In caso di una violazione dei dati personali trattati dal Responsabile del trattamento, quest'ultimo ne dà notifica al Titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi. Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Le parti stabiliscono nell'allegato III tutti gli altri elementi che il Responsabile del trattamento è tenuto a fornire quando assiste il Titolare del trattamento nell'adempimento degli obblighi che incombono al Titolare stesso ai sensi degli articoli 33 e 34 del Regolamento (UE) 2016/679.

SEZIONE III

DISPOSIZIONI FINALI

Clausola 10

Inosservanza delle clausole e risoluzione

a) Fatte salve le disposizioni del Regolamento (UE) 2016/679, qualora il Responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il Titolare del trattamento può dare istruzione al Responsabile di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il Responsabile del trattamento informa prontamente il Titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole;
b) il Titolare del trattamento ha diritto di risolvere il contratto relativamente al trattamento dei dati personali conformemente alle presenti clausole qualora:
    1) il trattamento dei dati personali da parte del Responsabile del trattamento sia stato sospeso dal Titolare del trattamento ai sensi della lettera a) e il rispetto delle presenti clausole non sia stato adempiuto entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
    2) il Responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del Regolamento (UE) 2016/679;
    3) il Responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o delle autorità di controllo competenti per quanto riguarda i propri obblighi in conformità alle presenti clausole o al Regolamento (UE) 2016/679;
c) il Responsabile del trattamento ha diritto di risolvere il contratto relativamente al trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato, ai sensi della clausola

7.1, lettera b), il Titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili, il Titolare del trattamento insista sul rispetto delle istruzioni stesse;

d) dopo la risoluzione del contratto il Responsabile del trattamento, a scelta del Titolare del trattamento, cancella tutti i dati personali trattati per conto del Titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al Titolare tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il Responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

SEZIONE IV
ULTERIORI DISPOSIZIONI

Clausola 11

Ulteriori Disposizioni

Il Responsabile del trattamento dei dati personali nell'effettuare le operazioni di trattamento connesse all'esecuzione del suddetto contratto dovrà attenersi alle seguenti ulteriori disposizioni operative:

a) i trattamenti dovranno essere svolti nel pieno rispetto delle normative vigenti in materia di protezione dei dati personali, nonché tenendo conto dei provvedimenti e dei comunicati ufficiali emessi dal Garante per la protezione dei dati personali e per le finalità indicate nell'allegato II;

b) il Responsabile è autorizzato a procedere all'organizzazione di ogni operazione di trattamento dei dati nei limiti stabiliti dal contratto in essere tra le parti e dalle vigenti disposizioni contenute nel RGPD;

c) il Responsabile si impegna, già in fase contrattuale, al fine di garantire il rispetto del principio della "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" di cui all'articolo 25 del RGPD, a determinare i mezzi "non essenziali" del trattamento e a mettere in atto le misure tecniche e organizzative adeguate, ai sensi dell'articolo 32 del RGPD, prima dell'inizio delle attività, nei limiti della propria autonomia consentita dalle normative vigenti e dal presente atto;

d) il Responsabile dovrà eseguire i trattamenti funzionali alle attività ad esso attribuite e comunque non incompatibili con le finalità per cui i dati sono stati raccolti. Qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, il Responsabile dovrà informare il Titolare del trattamento ed il Responsabile della protezione dei dati (DPO) della Giunta regionale del Lazio;

e) il Responsabile – per quanto di propria competenza – è tenuto, in forza di normativa cogente e del contratto, a garantire – per sé, per i propri dipendenti e per chiunque collabori a qualunque titolo – il rispetto della riservatezza, integrità, disponibilità dei dati, nonché l'utilizzo dei predetti dati per le sole finalità specificate nel presente documento e nell'ambito delle attività di sicurezza di specifico interesse del Titolare;

f) il Responsabile ha il compito di curare, in relazione alla fornitura del servizio di cui al contratto in oggetto, l'attuazione delle misure prescritte dal Garante per la protezione dei dati personali in merito all'attribuzione delle funzioni di "Amministratore di sistema" di cui al provvedimento del 27 novembre 2008, e successive modificazioni ed integrazioni e, in particolare, di:

1) designare come amministratore di sistema, con le modalità previste dal provvedimento del 27 novembre 2008, le persone fisiche autorizzate ad accedere in modo privilegiato, ai sensi dello stesso provvedimento, ai dati personali del cui trattamento la Giunta regionale del Lazio è Titolare;
2) conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte all'interno della società quali amministratori di sistema, in relazione ai dati personali del cui trattamento la Giunta regionale del Lazio è Titolare;
3) attuare le attività di verifica periodica, con cadenza almeno annuale, sul loro operato secondo quanto prescritto dallo stesso provvedimento; gli esiti di tali verifiche dovranno essere comunicati al Titolare del trattamento su richiesta dello stesso;

g) il Responsabile si impegna a garantire, senza ulteriori oneri per il Titolare, l'esecuzione di tutti i trattamenti individuati al momento della stipula del contratto e dei quali dovesse insorgere in seguito la necessità ai fini dell'esecuzione del contratto stesso;

h) il Responsabile si impegna ad attivare le necessarie procedure aziendali per identificare ed istruire le persone autorizzate al trattamento dei dati personali ed organizzarne i compiti in maniera che le singole operazioni di trattamento risultino coerenti con le disposizioni di cui alla presente nomina, facendo in modo, altresì, che, sulla base delle istruzioni operative loro impartite, i trattamenti non si discostino dalle finalità istituzionali per cui i dati sono stati raccolti e trattati. Il Responsabile garantirà, inoltre, che le persone autorizzate al trattamento siano vincolate da un obbligo, legalmente assunto, di riservatezza;

i) il Responsabile si impegna ad attivare per garantire l'adozione delle misure di sicurezza di cui all'articolo 32 del RGPD. In particolare, tenuto conto delle misure di sicurezza in atto, adottate a protezione dei trattamenti dei dati per conto della Giunta regionale del Lazio, come previste dal contratto vigente, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento e, sulla base delle risultanze dell'analisi dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, che derivano in particolare dalla distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati, porrà in essere le opportune azioni organizzative per l'ottimizzazione di tali misure, al fine di garantire un livello di sicurezza adeguato al rischio.

   Nel valutare l'adeguato livello di sicurezza, il Responsabile terrà conto, in special modo, dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

   Il Responsabile assicura, inoltre, che le operazioni di trattamento dei dati sono effettuate nel rispetto delle misure di sicurezza tecniche, organizzative e procedurali a tutela dei dati trattati, in conformità alle previsioni di cui ai provvedimenti di volta in volta emanati dalle Autorità nazionali ed europee (a ciò autorizzate), qualora le stesse siano applicabili rispetto all'attività effettivamente svolta come Responsabile del trattamento.

   Nel caso in cui, considerata la propria competenza e ove applicabile rispetto alle attività svolte, il Responsabile dovesse ritenere che le misure adottate non siano più adeguate e/o idonee a prevenire/mitigare i rischi sopramenzionati, è tenuto a darne tempestiva comunicazione scritta al Titolare e a porre comunque in essere tutti gli interventi temporanei, ritenuti essenziali e improcrastinabili, in attesa delle soluzioni definitive da concordare con il Titolare.

   L'adozione e l'adeguamento delle misure di sicurezza tecniche devono aver luogo prima di iniziare e/o continuare qualsiasi operazione di trattamento di dati.

Il Responsabile è tenuto a segnalare prontamente al Titolare l'insorgenza di problemi tecnici attinenti alle operazioni di raccolta e trattamento dei dati ed alle relative misure di sicurezza, che possano comportare rischi di distruzione o perdita, anche accidentale, dei dati stessi, ovvero di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta/dei trattamenti.

Il Responsabile, ove applicabile, dovrà, altresì, adottare le misure minime di sicurezza ICT per le pubbliche amministrazioni, di cui alla circolare AgID del 18 aprile 2017, n. 2/2017, nonché le eventuali ulteriori misure specifiche stabilite dal Titolare, nel rispetto dei contratti vigenti;

l) il Responsabile deve adottare le politiche interne e, ai sensi dell'articolo 25 del RGPD, le misure che soddisfano i principi della protezione dei dati personali fin dalla progettazione di tali misure; adotta inoltre ogni misura adeguata a garantire che i dati personali siano trattati in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il tempo strettamente necessario al raggiungimento delle stesse;

m) il Responsabile, ai sensi dell'articolo 30 del RGPD e nei limiti di quanto dallo stesso stabilito, è tenuto a tenere un registro delle attività di trattamento effettuate sotto la propria responsabilità per conto del Titolare e a cooperare con il Titolare stesso e con il Garante per la protezione dei dati personali, laddove ne venga fatta richiesta ai sensi dell'articolo 30, paragrafo 4, del RGPD;

n) il Responsabile è tenuto ad informare di ogni violazione di dati personali (cosiddetta *personal data breach*) il Titolare ed il Responsabile della protezione dei dati (DPO) della Giunta regionale del Lazio, tempestivamente e senza ingiustificato ritardo, entro 24 ore dall'avvenuta conoscenza dell'evento.

Tale notifica, va effettuata tramite PEC da inviare agli indirizzi protocollo@pec.regione.lazio.it, dpo@pec.regione.lazio.it, databreach@pec.regione.lazio.it; la stessa deve essere accompagnata da ogni documentazione utile, ai sensi degli articoli 33 e 34 del RGPD, per permettere al Titolare, ove ritenuto necessario, di notificare questa violazione al Garante per la protezione dei dati personali e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando il Titolare stesso ne è venuto a conoscenza. Nel caso in cui il Titolare debba fornire informazioni aggiuntive alla suddetta autorità, il Responsabile supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per il Garante siano esclusivamente in possesso del Responsabile e/o di suoi sub-responsabili;

o) il Responsabile garantisce gli adempimenti e le incombenze anche formali verso il Garante per la protezione dei dati quando richiesto e nei limiti dovuti, adoperandosi per collaborare tempestivamente, per quanto di competenza, sia con il Titolare sia con il Garante per la protezione dei dati personali. In particolare:
   - fornisce informazioni sulle operazioni di trattamento svolte;
   - consente l'accesso alle banche dati oggetto delle operazioni di trattamento;
   - consente l'esecuzione di controlli;
   - compie quanto necessario per una tempestiva esecuzione dei provvedimenti inibitori, di natura temporanea;

p) il Responsabile si impegna a adottare, su richiesta del Titolare e nel rispetto degli obblighi contrattuali assunti, nel corso dell'esecuzione dei contratti, ulteriori garanzie quali l'applicazione di un codice di condotta applicato o di un meccanismo di certificazione approvato ai sensi degli articoli 40 e 42 del RGPD, laddove adottati. Il Titolare potrà in ogni momento verificare l'adozione di tali ulteriori garanzie;

q) il Responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare e ai patti e alle condizioni previste nel RGPD e nel presente contratto;
r) il Responsabile è tenuto a comunicare al Titolare ed al DPO della Regione Lazio il nome ed i dati del proprio DPO, laddove il Responsabile stesso lo abbia designato, conformemente a quanto prescritto dall'articolo 37 del RGPD. Il DPO collaborerà e si terrà in costante contatto con il DPO della Regione Lazio;
s) il Responsabile è tenuto ad individuare e verificare almeno annualmente l'ambito dei trattamenti consentiti alle persone autorizzate e ad impartire ai medesimi istruzioni dettagliate circa le modalità del trattamento;
t) le persone autorizzate al trattamento sono tenute al segreto professionale e alla riservatezza, anche per il periodo successivo all'estinzione del rapporto di lavoro intrattenuto con il Responsabile, in relazione alle operazioni di trattamento da essi eseguite;
u) il Responsabile è tenuto, altresì, a vigilare sulla puntuale osservanza delle istruzioni allo stesso impartite.

Il Titolare del trattamento **Il Responsabile del trattamento**

_____ _____

ALLEGATO I

Elenco delle parti

TITOLARE DEL TRATTAMENTO:

GIUNTA REGIONALE DEL LAZIO

Sede: Via R. Raimondi Garibaldi 7– 00147 Roma,

<Nome, qualifica e dati di contatto del referente>

Dati di contatto del Responsabile della Protezione dei Dati personali (DPO):

_____

RESPONSABILE DEL TRATTAMENTO

Ragione sociale:

Sede legale:

Tel.:

Mail:

PEC:

Dati di contatto del Responsabile della Protezione dei Dati personali (DPO):

_____

<Nome, qualifica e dati di contatto del referente>

CONTESTO DI RIFERIMENTO

I Rapporti tra le parti sono stati definiti con:

NOTA ESPLICATIVA: scegliere una o più delle seguenti opzioni:

- *deliberazione di Giunta Regionale n._____ del_____ avente ad oggetto "_____";*
- *determinazione dirigenziale n._____ del_____ avente ad oggetto "_____";*
- *contratto sottoscritto in data____, registrato in data al n._____;*
- *Altro_____.*

ALLEGATO II

Descrizione del trattamento

Categorie di interessati i cui dati personali sono trattati:

NOTA ESPLICATIVA: valorizzare la/le opzione/i coerente/i:

[ ] a) Dipendenti/Consulenti
[ ] b) Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
[ ] c) Associati, soci, aderenti, simpatizzanti, sostenitori
[ ] d) Soggetti che ricoprono cariche sociali
[ ] e) Beneficiari o assistiti
[ ] f) Pazienti
[ ] g) Minori
[ ] h) Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
[ ] i) Altro_____
(*Esempio:*
- cittadini,
- disabili,
- referenti aziende clienti;
- rappresentanti legali aziende potenziali;
- personale dipendente delle aziende clienti;
- etc etc da individuare).

Categorie di dati personali trattati*:*

NOTA ESPLICATIVA: valorizzare la/le opzione/i coerente/i:

[ ] a) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
[ ] b) Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
[ ] c) Dati di accesso e di identificazione (username, password, customer ID, altro…)
[ ] d) Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
[ ] e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione Internet, altro…)

[ ] f) Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
[ ] g) Dati di profilazione
[ ] h) Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
[ ] i) Dati relativi all'ubicazione
[ ] l) Dati che rivelano l'origine razziale o etnica
[ ] m) Dati che rivelano le opinioni politiche
[ ] n) Dati che rivelano le convinzioni religiose o filosofiche
[ ] o) Dati che rivelano l'appartenenza sindacale
[ ] p) Dati relativi alla vita sessuale o all'orientamento sessuale
[ ] q) Dati relativi alla salute
[ ] r) Dati genetici
[ ] s) Dati biometrici
[ ] t) Altro_____
[Esempio:
eliminare e/o aggiungere in base ai dati personali effettivamente trattati:
Dati comuni:
- caratteristiche individuali (ad es. peso, altezza ecc.),
- codice fiscale e altri codici identificativi (matricola lavoratore);
- indirizzo di residenza e/o domicilio,
- n. carta d'identità,
- indirizzo IP,
- codice IBAN,
- n. di targa,
- dati personali contenuti nel cedolino dello stipendio;
- dati reddituali e compensi percepiti;
- informazioni presenti nei curriculum vitae;
- Informazioni aventi natura "soggettiva" quali opinioni o valutazioni, anche espresse con codici o in termini numerici (valutazioni della prestazione/capacità lavorativa/l'affidabilità; notizie contenute nelle relazioni/consulenze/perizie; esito di test psicologici/disegni; informazioni contenute sotto forma di testo libero come un messaggio di posta elettronica; etc)]

[ ] u) Dati sensibili/particolari trattati (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, (esempio rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata, tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari):

NOTA ESPLICATIVA: indicare la tipologia di dati particolari trattata:

_____

(Esempio:
Dati sensibili/particolari:

- origine razziale o etnica
- opinioni politiche
- convinzioni religiose o filosofiche
- appartenenza sindacale
- dati genetici
- dati biometrici (immagini registrate da un sistema di videosorveglianza);
- dati relativi alla salute: idoneità al lavoro (compreso informazioni di cui è vietata in ogni caso la pubblicazione a "erogazione ai sensi della legge 104/1992"; "soggetto portatore di handicap"; "anziano non autosufficiente"; "indici di autosufficienza nelle attività della vita quotidiana"; "contributo per ricovero in struttura sanitaria" o per "assistenza sanitaria")
- dati relativi alla vita sessuale o all'orientamento sessuale;

Con riferimento alle categorie particolari di dati (cd. sensibili), il Responsabile del trattamento si impegna ad adottare le prescrizioni contenute nel Provvedimento del Garante Privacy n. 146 del 5 giugno 2019 (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 176 del 29 luglio 2019) per il trattamento di:

NOTA ESPLICATIVA: valorizzare la/le opzione/i coerente/i:

☐ categorie particolari di dati nei rapporti di lavoro, le Prescrizioni di cui all'aut. gen. n. 1/2016;

☐ categorie particolari di dati da parte degli organismi di tipo associativo, delle fondazioni, delle chiese e associazioni o comunità religiose, le Prescrizioni di cui all'aut. gen. n. 3/2016;

☐ categorie particolari di dati da parte degli investigatori privati, le Prescrizioni di cui all'aut. gen. n. 6/2016;

☐ dati genetici e i campioni biologici, le Prescrizioni di cui all'aut. gen. n. 8/2016;

☐ dati personali per scopi di ricerca scientifica, le Prescrizioni di cui all'aut. gen. n. 9/2016;

☐ nessuna delle Prescrizioni di cui sopra.

Il Responsabile deve essere in grado di dimostrare, laddove necessario, il rispetto delle succitate specifiche prescrizioni.

[ ] v) Dati giudiziari:
- informazioni relative a condanne penali e a reati, o a connesse misure di sicurezza.

Natura del trattamento:

Il trattamento è svolto in maniera:

NOTA ESPLICATIVA: valorizzare la/le opzione/i coerente/i:

[ ] manuale;

[ ] informatizzata

[ ] Altro

Finalità per le quali i dati personali sono trattati per conto del Titolare del trattamento e relative basi giuridiche

I dati devono essere raccolti per le seguenti finalità determinate, esplicite e legittime, e quindi trattati secondo modalità compatibili con tale finalità (art. 5 par. 1 lett. b):

NOTA ESPLICATIVA: inserire le finalità del trattamento

Se il Responsabile del trattamento viola il Regolamento (UE) 2016/679, ovvero agisce in modo difforme o contrario rispetto alle legittime istruzioni impartite dal Titolare, determinando le finalità e i mezzi del trattamento ai sensi dell'art. 28, paragrafo 10, del GDPR è da considerarsi Titolare del trattamento in questione.

Durata del trattamento:

Il trattamento potrà essere svolto fino al termine del rapporto contrattuale definito negli atti sopra richiamati fatti salvi eventuali proroghe e rinnovi.

Al termine o alla cessazione di efficacia del contratto il Responsabile del trattamento deve restituire al Titolare tutti i dati personali trattati per suo conto e cancellare le eventuali copie esistenti in suo possesso (su qualsiasi supporto) secondo le istruzioni ricevute dal Titolare, certificando altresì a quest'ultimo di averlo fatto, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali trattati.

Il Titolare si riserva la facoltà di disporre tale verifica tramite un revisore, anche di terza parte, a condizione che non abbia una relazione competitiva con il Responsabile stesso.

È esplicitamente esclusa la pratica del "blocco da fornitore" (c.d. *Vendor lock-in*).

Finché i dati non sono restituiti e cancellati, il Responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

NOTA ESPLICATIVA: In caso di trattamenti da parte di (sub-)Responsabile/i del trattamento, specificare di seguito gli elementi contenuti nel presente allegato II (categorie di interessati, categorie di dati, natura del trattamento, ecc.) riferiti ad ogni singolo sub-Responsabile.

ALLEGATO III

Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei trattamenti e dei dati

NOTA ESPLICATIVA: le misure tecniche e organizzative devono essere descritte in modo concreto e non genericamente e devono prevedere anche le specifiche misure da adottare al fine di fornire assistenza al Titolare del trattamento. Le misure si devono riferire alla specifica fattispecie. Eliminare le misure non pertinenti e non applicabili e eventualmente aggiungere misure non previste.

Si descrivono di seguito le misure di sicurezza tecniche e organizzative che il Responsabile del trattamento deve mettere in atto, (comprese le eventuali certificazioni in possesso del Responsabile del trattamento pertinenti, ove presenti), per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.

1) PRIVACY BY DESIGN E BY DEFAULT

Il Responsabile del trattamento deve rispettare i principi di protezione dei dati fin dalla progettazione (privacy by design) e protezione dei dati per impostazione predefinita (privacy by default) di cui all'art. 25 GDPR comunicando al Titolare le soluzioni individuate e adottate per rispettare tali principi (cfr. Considerando 78 GDPR).
In attuazione di tali principi, il Responsabile del trattamento, anche quando utilizza sistemi tecnologici realizzati da terzi, dovrà eseguire un'analisi dei rischi e accertarsi che le funzionalità corrispondano alle finalità del trattamento individuate che abbiano una specifica base giuridica.

2) ELENCO AGGIORNATO SUB-RESPONSABILI

Quando il primo Responsabile del trattamento è autorizzato a ricorrere a un altro Responsabile del trattamento per l'esecuzione di specifiche attività, a prescindere dal carattere specifico o generale dell'autorizzazione preliminare scritta del Titolare del trattamento, il primo Responsabile deve tenere un elenco aggiornato degli altri (sub-)responsabili. Su richiesta del Titolare e/o e in caso di accertamenti anche da parte del Garante, il primo Responsabile del trattamento gli fornisce prontamente e non oltre 24 ore copia dell'elenco aggiornato.

3) ATTIVITA' DI REVISIONE, COMPRESE LE ISPEZIONI

Su richiesta del Titolare del trattamento, a intervalli annuali o se vi sono indicazioni di inosservanza, il Responsabile del trattamento consentirà e contribuirà alle attività di revisione delle attività di trattamento di cui alle presenti clausole. Nel decidere in merito a un riesame o a un'attività di revisione, il Titolare del trattamento potrà tenere conto delle pertinenti certificazioni in possesso del Responsabile del trattamento.
Il Titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere

anche ispezioni nei locali o nelle strutture fisiche del Responsabile del trattamento e, se del caso, sono effettuate con un preavviso di almeno 72 ore.

4) TRASFERIMENTO DATI EXTRA UE

È generalmente vietato il trasferimento di dati da parte del Responsabile del trattamento verso un paese terzo o un'organizzazione internazionale, ovvero a sub-responsabili del trattamento che non rientrano nell'ambito di applicazione territoriale del GDPR, compresi trasferimenti successivi. Il Responsabile del trattamento si assicura che anche il sub-Responsabile del trattamento non effettui trasferimenti di dati verso un paese terzo o un'organizzazione internazionale. Il Primo Responsabile, nella scelta di ulteriori fornitori, deve privilegiare, a parità di garanzie in materia di protezione dei dati personali, fornitori che sono situati sul territorio nazionale e dell'Unione europea, istruendoli sulla necessità di conservare i dati all'interno dell'Unione stessa.

In via del tutto residuale, il Primo Responsabile può ricorrere a responsabili situati in Paesi terzi, nel rispetto delle misure previste dal capo V del GDPR.

In presenza di una decisione di adeguatezza, il Primo Responsabile del trattamento è tenuto in ogni caso a chiedere specifica autorizzazione al Titolare, in considerazione degli obblighi connessi ai trasferimenti internazionali di cui al capo V del GDPR.

Ad ogni modo, il trasferimento di dati extra UE può essere effettuato soltanto su istruzione documentata del Titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il Responsabile del trattamento, e nel rispetto del capo V del GDPR.

5) AMMINISTRATORE DI SISTEMA

Nel caso in cui il Responsabile effettua trattamenti, anche in parte, mediante strumenti elettronici, si impegna ad individuare e a designare gli Amministratori di Sistema ("AdS"), conformandosi altresì, nell'affidamento di tale incarico, a tutto quanto previsto dal provvedimento del Garante Privacy del 27 novembre 2008 [doc. web n. 1577499] (G.U. n. 300 del 24 dicembre 2008), come modificato in base al provvedimento del 25 giugno 2009.

Le persone fisiche designate AdS considerate come tali sono le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti nonché altre figure equiparabili quali gli amministratori di base dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Delle misure e degli accorgimenti prescritti con la designazione di Amministratore di Sistema il Responsabile del trattamento è tenuto a darne la prova; deve altresì conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema, tenendo costantemente aggiornato tale documento interno (come da Allegato V) e in caso di accertamenti anche da parte del Garante fornire prontamente e comunque entro 24 ore il medesimo documento al Titolare.

6) MISURE MINIME E MISURE AGID:

Il Responsabile deve dotarsi delle misure minime di sicurezza per limitare il rischio di attacchi informatici.

Per il tramite degli Amministratori di Sistema designati, si impegna a garantire di default le modalità tecniche previste dall'Allegato B del Codice Privacy (Disciplinare tecnico in materia di misure di sicurezza), seppur oggi abrogato.

Il Responsabile si impegna ad installare e mantenere aggiornate, sugli strumenti elettronici oggetto del contratto, tutte le misure e gli accorgimenti eventualmente prescritti dai Provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali (GPDP), dall'Agenzia per l'Italia Digitale (AGID) e dall'Agenzia per la Cybersicurezza Nazionale (ACN), applicabili al servizio commissionato, nonché le ulteriori misure di sicurezza previste nel contratto di fornitura.
Nello specifico, il Responsabile si impegna al rispetto e alla dimostrazione di quanto previsto dall'AGID con:
le Linee guida - Sicurezza nel Procurement ICT (Pubblicato il 19/05/2020 - Aggiornato il 19/05/2020)
Linee guida per lo sviluppo del software sicuro (Ultimo aggiornamento 06-05-2020), disponibile alla seguente url: https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro
le «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)». (17A03060) (G.U Serie Generale n.103 del 05-05-2017), disponibili anche alla seguente url: https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

7) MISURE ULTERIORI:

NOTA ESPLICATIVA: adattare alla singola fattispecie – eliminare le misure non pertinenti e non applicabili.

Il Responsabile del trattamento, ferma la dimostrazione della loro adozione, si impegna a mettere in atto e adottare le seguenti ulteriori e più specifiche misure tecniche e organizzative:
a) mezzi che permettono di garantire la confidenzialità, l'integrità, la disponibilità e la resilienza costante dei sistemi e dei servizi di trattamento.
a.1) la capacità di assicurare la riservatezza dei dati trattati, facendo in modo che le password relative alle utenze dei soggetti autorizzati siano di lunghezza non inferiore a otto caratteri e siano sottoposte a un controllo automatico di qualità che impedisca l'uso di password "deboli" e che le medesime password siano modificate almeno al primo utilizzo;
a.2) la capacità di assicurare la riservatezza dei dati trattati, facendo in modo che l'autenticazione dei soggetti autorizzati avvenga tramite un processo di autenticazione multifattoriale (MFA);
a.3) la capacità di contrastare efficacemente attacchi informatici di tipo brute force sul sistema di autenticazione online, anche introducendo limitazioni al numero di tentativi infruttuosi di autenticazione;
a.4) crittografia dei dati che i dispositivi del fornitore/Responsabile (computer, portatili, tablet, ecc.) devono rispettare;
a.5) l'accesso alla rete locale dell'amministrazione da parte del fornitore/Responsabile deve essere configurato con le abilitazioni strettamente necessarie alla realizzazione di quanto contrattualizzato, vale a dire consentendo l'accesso esclusivamente alle risorse necessarie. L'accesso dall'esterno mediante VPN deve essere consentito, solo se strettamente necessario, utilizzando account VPN personali configurati e abilitati opportunamente. Gli accessi dovranno poter essere tracciati per eventuali successivi audit;

a.6) nelle forniture di sviluppo e manutenzione, l’utilizzo dei dati dell’amministrazione per la realizzazione di quanto contrattualizzato deve essere consentito esclusivamente su server/database di sviluppo nei quali sono stati importati i dati necessari per gli scopi del progetto. Tale misura consiste nel gestire l’accesso ai server e ai DB in modo da rispettare questa regola generale, tracciando le eventuali eccezioni che dovessero verificarsi.
b) mezzi che permettono di ristabilire la disponibilità dei dati a carattere personale e l’accesso a questi nei tempi appropriati in caso di incidente fisico o tecnico;
c) rilevare e detenere a norma di legge copia dei log di accesso all’applicativo e di sistema;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
e) nomina di un DPO, nei casi previsti dall’art. 37 GDPR ovvero per i soggetti privati obbligati alla sua designazione. Nel caso in cui il Responsabile del trattamento ritenesse tale nomina non obbligatoria, alla luce del principio di accountability è tenuto a dare la prova della mancanza dei criteri di nomina (cfr. Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato, punto nn. 3 e 4);
f) poter dimostrare che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati, se non è istruito in tal senso dal Responsabile del trattamento e non abbia ricevuto idonea formazione;
g) una procedura per la gestione degli incidenti di sicurezza e delle violazioni di dati personali (cd. “Data Breach”);
h) sottoscrizione di polizze assicurative che tengano conto dei risarcimenti danni di cui all’art. 82 del GDPR con massimali adeguati;
i) una Valutazione del Rischio per la sicurezza dei dati che tenga in considerazione i rischi presentati dal trattamento come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l’accesso non autorizzati (cfr. considerando 83 GDPR).
l) Sulle reti messe a disposizione dal fornitore devono essere presenti di dispositivi di sicurezza perimetrale con funzioni di sicurezza (ad esempio Firewall e sistemi di Network Detection ed Event & Log Monitoring, SIEM, ecc.) necessari a rilevare e contenere eventuali incidenti di sicurezza ICT e in grado di gestire gli IoC (Indicator of Compromise);
m) Il fornitore deve usare protocolli cifrati e meccanismi di autenticazione nell’ambito dei servizi erogati;
n) Qualora il fornitore subisca un attacco, in conseguenza del quale vengano compromessi sistemi del committente da lui gestiti, deve farsi carico delle bonifiche del caso, e riportare i sistemi in uno stato di assenza di vulnerabilità.
o) Il fornitore si impegna a trattare, trasferire e conservare le eventuali repliche dei dati oggetto di fornitura, ove autorizzate dalle amministrazioni, sempre all’interno del territorio dell’UE.

7.1) Verificare la documentazione finale di progetto

Alla fine di ogni singolo progetto, il Titolare verifica che il fornitore/Responsabile rilasci la seguente documentazione:

- documentazione finale e completa del progetto;
- manuale di installazione/configurazione;
- report degli Assessment di Sicurezza eseguiti con indicazione delle vulnerabilità riscontrate e le azioni di risoluzione/mitigazione apportate;

- “libretto di manutenzione” del prodotto (software o hardware), con l’indicazione delle attività da eseguire per mantenere un adeguato livello di sicurezza del prodotto realizzato o acquistato. In particolare, nel libretto di manutenzione deve essere indicato:
    - produttore e versione dei prodotti software utilizzati (ad esempio web server, application server, CMS, DBMS), librerie, firmware;
    - indicazioni per il reperimento dei Bollettini di Sicurezza dei singoli produttori di hardware/software;
    - indicazioni sul processo di installazione degli aggiornamenti sicurezza;
    - documento di EoL (documento che contiene indicazione dei prodotti utilizzati e relativo fine vita/rilascio aggiornamenti sicurezza).

7.2) Distruzione del contenuto logico (wiping) dei dispositivi che vengono sostituiti

Nelle acquisizioni di attività di conduzione CED o di gestione di parchi di PC (fleet management), occorre verificare che l’hardware dismesso venga cancellato e distrutto in modo sicuro, evitando rischi che dati critici possano restare erroneamente memorizzati sull’hardware dismesso stesso.
Nei rapporti contrattuali col Responsabile va definito un processo di verifica strutturato che deve almeno prevedere:
- la consegna di un verbale di avvenuta distruzione da parte del fornitore;
- nel caso di sistemi critici, la programmazione di una azione ispettiva o di altri sistemi di monitoraggio o controllo.

7.3) Manutenzione - aggiornamento dei prodotti:

È fatto obbligo agli amministratori di sistema di eseguire gli aggiornamenti ogni qualvolta sui siti dei produttori vengono rilasciati patch e correzioni per problemi di vulnerabilità.

7.4) Vulnerability Assessment

Il Fornitore/Responsabile deve eseguire, su beni e servizi classificati critici ed esposti sul web, un Vulnerability Assessment a cadenza almeno annuale, e ogniqualvolta si apportano modifiche alla configurazione software/hardware.

7.5) Altre misure tecniche e organizzative:

NOTA ESPLICATIVA: eliminare quelle non pertinenti e aggiungere quelle mancanti:

- misure di pseudonimizzazione e cifratura dei dati personali;
- misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

- misure di identificazione e autorizzazione dell'utente;
- misure di protezione dei dati durante la trasmissione;
- misure di protezione dei dati durante la conservazione;
- misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati;
- misure per garantire la registrazione degli eventi;
- misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita;
- misure di informatica interna e di gestione e governance della sicurezza informatica;
- misure di certificazione/garanzia di processi e prodotti;
- misure per garantire la minimizzazione dei dati;
- misure per garantire la qualità dei dati;
- misure per garantire la conservazione limitata dei dati;
- misure per garantire la Responsabilità;
- misure per consentire la portabilità dei dati e garantire la cancellazione.

8) PERSONALE AUTORIZZATO:

Il Responsabile del trattamento si impegna a produrre e aggiornare in caso di modifiche l'elenco degli operatori autorizzati singolarmente e opportunamente formati in materia di privacy (ivi inclusi gli opportuni aggiornamenti normativi), impartendo per iscritto specifiche istruzioni per trattare i dati degli utenti, nell'ambito della propria attività e con i limiti di legge, curando, in particolare, il profilo della sicurezza di accesso e dell'integrità dei dati ai sensi dell'art. 29 del GDPR. Inoltre, il Responsabile s'impegna a stabilire le modalità di accesso ai dati e l'organizzazione del lavoro degli autorizzati al trattamento, avendo cura di adottare preventivamente misure organizzative adeguate al rischio per diritti e libertà delle persone fisiche. Inoltre, deve garantire che le persone autorizzate siano state istruite sulla procedura di gestione degli incidenti di sicurezza e sulla gestione delle violazioni di dati personali. Il Titolare può richiedere una prova documentata, al fine di verificare tali adempimenti.

9) REGISTRO DEL TRATTAMENTO:

Il Responsabile del trattamento, anche laddove non rientri nelle casistiche definite dall'art. 30, parr. 2 e 5, del GDPR, tiene per iscritto un Registro delle attività relative ai trattamenti svolti per conto del Titolare.

10) ASSISTENZA AL TITOLARE:

In generale, il Responsabile del trattamento è tenuto ad assistere il Titolare nel garantire il rispetto degli obblighi a cui è vincolato quest'ultimo e a rispondere prontamente e comunque non oltre 72 ore dalle richieste di informazioni del Titolare del trattamento.
Il Responsabile comunicherà ogni informazione utile al fine di assistere il Titolare nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti. Qualora il Responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti, informa senza indugio e comunque non oltre 72 ore il Titolare affinché possa garantire che i dati personali siano esatti e aggiornati.

Nel caso in cui riceva richieste degli interessati per l'esercizio dei loro diritti, il Responsabile notifica prontamente e comunque non oltre 72 ore al Titolare del trattamento qualunque richiesta ricevuta dall'interessato in quanto non è autorizzato a rispondere egli stesso alla richiesta.
Inoltre, il Responsabile del trattamento assiste il Titolare nel garantire il rispetto degli obblighi imposti a quest'ultimo ai sensi dell'articolo 32 del GDPR, fornendogli, tra l'altro, le informazioni riguardanti le misure tecniche e organizzative da questi adottate in conformità all'articolo 32 medesimo, unitamente a tutte le altre informazioni necessarie al Titolare del trattamento per conformarsi agli obblighi a lui imposti per garantire un livello di sicurezza adeguato al rischio.
Il Responsabile si impegna a predisporre, condividere e aggiornare periodicamente la valutazione del rischio per la sicurezza dei dati e la valutazione di impatto sulla protezione dei dati e, comunque, a redigere uno o più atti di documentazione delle scelte, dando atto della conformità alla normativa sulla protezione delle persone con riguardo al trattamento dei dati e alla circolazione dei dati., ovvero indicando che il trattamento presenterebbe un rischio elevato.
Laddove la valutazione di impatto sulla protezione dei dati presentasse un rischio elevato, anche in fase di consultazione con la/le autorità di controllo competenti, il Responsabile assisterà il Titolare del trattamento per adottare le misure adeguate per attenuare il rischio.
Il Responsabile si impegna ad adibire apposito ufficio/referente, segnalando un punto di contatto diretto al Titolare del trattamento, alle incombenze relative alla notificazione e comunicazioni previste dal GDPR.

11) COMUNICAZIONE E REGISTRO DI INCIDENTI DI SICUREZZA E DI VIOLAZIONI DI DATI PERSONALI

In caso di incidente di sicurezza e/o di violazione dei dati personali (cd. Data Breach), senza indugio il Responsabile del trattamento coopera con il Titolare e lo assiste nell'adempimento degli obblighi, ai sensi degli artt. 33 e 34 GDPR.
Nel caso di incidente di sicurezza e/o di una violazione dei dati personali trattati dal Responsabile del trattamento, quest'ultimo ne dà comunicazione al Titolare senza ingiustificato ritardo e comunque non oltre 24 ore dopo esserne venuto a conoscenza. La comunicazione iniziale contiene le informazioni disponibili in quel momento e le altre informazioni sono fornite non appena disponibili, senza ingiustificato ritardo. Il Responsabile documenta qualsiasi incidente di sicurezza e/o di violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.
Il Responsabile deve mantenere un Registro degli incidenti di sicurezza, anche qualora non vi siano delle violazioni dei dati personali, per coadiuvare il Titolare nel suo obbligo relativo al paragrafo 5 dell'art. 33 del GDPR.

A seguito del verificarsi di detti incidenti il Titolare può:
- effettuare le succitate attività di revisione, comprese le ispezioni;
- prescrivere l'adozione di misure di sicurezza aggiornate e/o ulteriori anche rispetto a quelle previste dal presente accordo;
- attivare azioni di rivalsa nei confronti del Responsabile;
- applicare le penali contrattuali;
- risolvere il contratto (cfr. la succitata Clausola 10).

Il Responsabile deve adottare procedure tecniche e organizzative volte alla gestione di eventuali incidenti di sicurezza e di violazioni di dati personali; deve disporre altresì di una struttura per la prevenzione e gestione degli incidenti informatici e delle violazioni di dati personali con il compito d'interfacciarsi con le analoghe strutture del Titolare.

12) LINEE GUIDA E PROVVEDIMENTI DELL'AUTORITA' GARANTE PRIVACY:

NOTA ESPLICATIVA: eliminare i provvedimenti non pertinenti e aggiungere quelli applicabili alla fattispecie ove esistenti:

Il Responsabile del trattamento s'impegna a mettere in atto le misure tecniche e organizzative previste da Linee Guida e provvedimenti adottati dalle Autorità europee in materia di protezione dei dati personali, con particolare riferimento a quelli adottati dal Garante Privacy italiano quali:
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015 ((Pubblicato sulla Gazzetta Ufficiale n. 179 del 4 agosto 2015);
- Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008 (G.U. n. 287 del 9 dicembre 2008);
- Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali - 27 novembre 2008 (G.U. n. 287 del 9 dicembre 2008);
- Posta elettronica e internet – 1° marzo 2007;

_____
- Altro

In materia di protezione di dati personali il Responsabile del trattamento si impegna a rispettare e mettere in atto:

☐ Linee guida in materia di conservazione delle password (ACN & GPDP, Provvedimento n. 594 del 7 dicembre 2023)
☐ Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021
☐ Provvedimento in materia di videosorveglianza - 8 aprile 2010;
☐ Adempimenti semplificati per il customer care (inbound) - 15 novembre 2007
☐ RFID Etichette intelligenti: prescrizioni - 9 marzo 2005;
☐ Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014;
☐ Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro - 4 ottobre 2011;
☐ Sistemi di videosorveglianza per il controllo della procedura di raccolta del campione urinario a fini certificatori o di cura della salute 15 maggio 2013;
☐ Trattamento di dati personali per profilazione on line - 19 marzo 2015;
☐ Provvedimento generale in materia di trattamento dei dati personali nell'ambito dei servizi di mobile remote payment – 22 maggio 2014 (Pubblicato sulla Gazzetta Ufficiale n. 137 del 16 giugno 2014)

☐ Trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati – 15 maggio 2014;

☐ Dossier sanitario - 4 giugno 2015

☐ Svolgimento di indagini di customer satisfaction in ambito sanitario - 5 maggio 2011;

☐ Le norme del Codice Privacy non in contrasto con il Regolamento Europeo e non oggetto di abrogazione/modifica

☐ per i trattamenti di dati sensibili svolti dai soggetti pubblici (quelli di cui all'art. 6.1.c) ed e) del GDPR), in considerazione dell'art. 6.2 del GDPR saranno valutate le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 del Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

☐ Le buone prassi in materia di sicurezza o Privacy proposte da ENISA (Agenzia europea per la sicurezza delle reti e dell'informazione);

☐ Le buone prassi in materia di sicurezza o Privacy proposte da associazioni:
(Esempio:
- Center for Internet Security;
- Critical Security Controls for Effective Cyber Defense;
- CIS Benchmarks;
- Altro)

☐ Altro_____

13) CERTIFICAZIONI PERTINENTI:

Per attestare l'adeguatezza delle misure di sicurezza adottate (cfr. art. 28.5 del GDPR), il Responsabile del trattamento aderisce a specifici codici di condotta o a schemi di certificazione come di seguito:

NOTA ESPLICATIVA: valorizzare le certificazioni possedute ed eliminare quelle non pertinenti.

a) visto l'art. 43.1.b) del GDPR, che prevede una certificazione accreditata IS0 17065, il Responsabile del trattamento ha ottenuto il rilascio delle seguenti certificazioni:

[ ] ISDP©10003 (ITA);
[ ] Carpa (LU);
[ ] Europrivacy (LU);
[ ] Europrice (D);
[ ] altra certificazione accreditata IS0 17065 in materia di protezione dei dati personali;

b) visto l'art. 32 (nonché l'art. 25) del GDPR, anche se la norma di accreditamento ISO 17021-1 non è da considerarsi valida ai fini del GDPR, pur tuttavia molti argomenti trattati hanno riscontro in specifici requisiti di legge europei e nazionali, il Responsabile del trattamento possiede le seguenti certificazioni:

[ ] ISO/IEC 27001;
[ ] ISO/IEC 22301;

[ ] ISO/IEC 20000-1;
[ ] ISO/IEC 27701;
[ ] ISO/IEC 27017 e ISO/IEC 27018, integrate, come addendum alla Norma ISO/IEC 27001;
[ ] altra certificazione accreditata (e/o integrata) come addendum alla Norma ISO/IEC 27001;
[ ] altra certificazione accreditata in materia di privacy e gestione della sicurezza delle informazioni;

c) il Responsabile del trattamento ha ottenuto inoltre le seguenti certificazioni:

[ ] ISO 9001;
[ ] ISO 13485;
[ ] altra certificazione accreditata in materia di gestione della qualità;

[ ] ALTRO_____.

d) visto l'art. 106, comma 8, del D. Lgs. n. 36/2023, "Garanzie per la partecipazione alla procedura", ai fini del presente affidamento il Responsabile del trattamento ha ottenuto tra le norme di certificazione ivi previste le seguenti:

[ ] ALTRO_____.

14) INFORMAZIONI SUL TRATTAMENTO E CONSENSO DELL'INTERESSATO:

Nel caso in cui il/i trattamenti oggetto del presente contratto si basino sul consenso l'informativa redatta dal Titolare del trattamento deve essere:
☐ Consegnata a mano all'interessato;
☐ Pubblicata online sul sito XXXX;
☐ Non applicabile;
☐ Consegnata dal Titolare stesso;
☐ Altro (specificare nello spazio sottostante).

Gestione del consenso.

Quando il trattamento si fonda sulla base giuridica del consenso "libero" dell'interessato viene fornita dal Titolare specifica informativa e viene richiesto apposito consenso in mancanza del quale non si procederà al relativo trattamento.
Il consenso va raccolto e registrato tramite:
☐ Informativa e modulo raccolta consenso cartaceo redatto, reso e raccolto a cura del Titolare del trattamento;
☐ Informativa e modulo raccolta consenso cartaceo redatto a cura del Titolare e reso/raccolto da XXXX che dovrà consegnare la modulistica firmata al Titolare del trattamento;
☐ Raccolta e registrazione del consenso tramite sistema informatico XXXX;
☐ Altro;
☐ Non applicabile.

ALLEGATO IV

Elenco dei sub-responsabili del trattamento e/o terzi autorizzati al trattamento

Il Responsabile del Trattamenti si avvale dei seguenti sub-Responsabili del trattamento:

Sub **Responsabile del trattamento** **(Nome, ragione sociale, sede legale)**	**Descrizione del trattamento** (compresa la delimitazione delle responsabilità, qualora siano autorizzati più sub-Responsabili)	**Attività svolte per conto del primo Responsabile**	**Dati di contatto del referente**

ALLEGATO V
Disciplina dei servizi di Amministratore di Sistema

NOTA ESPLICATIVA: da utilizzare quando le prestazioni contrattuali implichino l'erogazione di servizi di amministrazione di sistema

Quando le prestazioni contrattuali implichino l'erogazione di servizi di amministrazione di sistema le persone fisiche designate AdS sono individuate in base ai criteri forniti nel provvedimento del Garante Privacy del 27 novembre 2008 [doc. web n. 1577499] (G.U. n. 300 del 24 dicembre 2008), come modificato in base al provvedimento del 25 giugno 2009, che considera come tali le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti nonché altre figure equiparabili quali gli amministratori di base dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
Il Responsabile del trattamento tiene un registro aggiornato di tutti gli Amministratori di Sistema (AdS) nonché di quegli Amministratori di Sistema la cui attività riguarda anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori (AdS/L) nominati al momento della sottoscrizione del presente contratto. Ciò anche al fine di consentire al Titolare di rendere nota o conoscibile l'identità degli AdS/L in relazione ai diversi servizi informatici cui questi sono preposti.

Il Responsabile tiene costantemente aggiornato il registro nella forma di seguito indicata e informa per iscritto il Titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di Amministratori di Sistema.

Col. 1 Cognome e Nome della persona fisica designata AdS	**Col. 2** Società e Organizzazione di appartenenza	**Col. 3** Ubicazione di lavoro dell'Ads	**Col. 4** Funzioni attribuite all'AdS: ambito di operatività per settori o per aree operative (*job description*)	**Col. 5** Banca dati gestita e trattamenti consentiti	**Col. 6** La persona in questione tratta informazioni di carattere personale dei lavoratori (AdS/L)?	
					SI	NO

Legenda:
Colonna 1: Cognome e Nome: cognome e nome della persona fisica che è stata designata, per iscritto, Amministratore di Sistema
Colonna 2: *Organizzazione di appartenenza*: indica la ragione sociale della Società di appartenenza dell'AdS e gli estremi identificativi dell'unità organizzativa nella quale l'AdS opera.
Colonna 3: Ubicazione: indica l'ubicazione di lavoro nella quale l'AdS svolge normalmente la sua attività
Colonna 4: Funzioni attribuite: descrive l'elenco dei servizi informatici assegnati alla persona, l'ambito di operatività per settori o per aree operativa. Vale a dire la *job description* dell'AdS.
Colonna 5: *Banca dati gestita e trattamenti consentiti:* indica le banche dati a cui l'AdS è autorizzato ad accedere e il tipo di operazioni consentite sui dati ivi contenuti. Vale adire il "profilo di autorizzazione" dell'AdS.
Colonna 6: Trattamento di informazioni dei lavoratori (AdS/L): la colonna "SI" indica quegli AdS la cui attività, in relazione ai diversi servizi informatici cui sono preposti, riguarda anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori (per brevità: "AdS/L"). Il dato viene fornito in adempimento a quanto prescritto dal Provvedimento del Garante che pone a carico dei Titolari del trattamento l'obbligo di rendere nota, nell'ambito della propria organizzazione, l'identità degli AdS/L al fine di richiamare l'attenzione sulla rilevanza e la criticità insite nello svolgimento della loro mansione.

Il Responsabile del trattamento, si impegna più specificamente a:

1) individuare i soggetti ai quali affidare il ruolo di Amministratori di Sistema (System Administrator), Amministratori di Base Dati (Database Administrator), Amministratori di Rete (Network Administrator) e/o Amministratori di Software Complessi e, sulla base del successivo atto di designazione individuale, impartire le istruzioni a detti soggetti, vigilando sul relativo operato;

2) assegnare ai suddetti soggetti una user id che contenga riferimenti agevolmente riconducibili all'identità degli Amministratori e che consenta di garantire il rispetto delle seguenti regole:
    a. divieto di assegnazione di user id generiche e già attribuite anche in tempi diversi;
    b. utilizzo di utenze amministrative anonime, quali "root" di Unix o "Administrator" di Windows, solo per situazioni di emergenza; le relative credenziali devono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso;
    c. disattivazione delle user id attribuite agli Amministratori che non necessitano più di accedere ai dati;
3) associare alle user id assegnate agli Amministratori una password e garantire il rispetto delle seguenti regole:

a) utilizzare password con lunghezza minima di almeno 14 caratteri, qualora l'autenticazione a più fattori non sia supportata;
b) cambiare la password alla prima connessione e successivamente almeno ogni 30 giorni (password aging).
c) le password devono differire dalle ultime 5 utilizzate (password history);
d) conservare le password in modo da garantirne disponibilità e riservatezza;
e) registrare tutte le immissioni errate di password. Ove tecnicamente possibile, gli account degli Amministratori devono essere bloccati dopo un numero massimo di tentativi falliti di login;
f) assicurare che l'archiviazione di password o codici PIN su qualsiasi supporto fisico avvenga solo in forma protetta da sistemi di cifratura;

4) assicurare la completa distinzione tra utenze privilegiate e non privilegiate di amministratore, alle quali devono corrispondere credenziali diverse;
5) assicurare che i profili di accesso, in particolare per le utenze con privilegi amministrativi, rispettino il principio del need-to-know, ovvero che non siano attribuiti diritti superiori a quelli realmente necessari per eseguire le normali attività di lavoro. Le utenze con privilegi amministrativi devono essere utilizzate per il solo svolgimento delle funzioni assegnate;
6) mantenere aggiornato un inventario delle utenze privilegiate (Anagrafica AdS), anche attraverso uno strumento automatico in grado di generare un alert quando è aggiunta una utenza amministrativa e quando sono aumentati i diritti di una utenza amministrativa;
7) adottare sistemi di registrazione degli accessi logici (log) degli Amministratori ai sistemi e conservare gli stessi per un congruo periodo non inferiore a 6 mesi. Qualora la Società utilizzi sistemi messi a disposizione dalla Regione, comunicare agli Amministratori che la Regione stessa procederà alla registrazione e conservazione dei log;
8) impedire l'accesso diretto ai singoli sistemi con le utenze amministrative. In particolare, deve essere imposto l'obbligo per l'Amministratore di accedere con una utenza normale e solo successivamente dargli la possibilità di eseguire, come utente privilegiato, i singoli comandi;

9) utilizzare, per le operazioni che richiedono utenze privilegiate di amministratore, macchine dedicate, collocate in una rete logicamente dedicata, isolata rispetto ad internet. Tali macchine non devono essere utilizzate per altre attività;
10) comunicare al momento della sottoscrizione del presente atto, e comunque con cadenza almeno annuale ed ogni qualvolta se ne verifichi la necessità, alla Regione gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema, di Base Dati, di Rete e/o di software Complessi, specificando per ciascuno di tali soggetti:
a) il nome e cognome;
b) la user id assegnata agli Amministratori;
c) il ruolo degli Amministratori (ovvero di Sistema, Base Dati, di Rete e/o di Software Complessi);
d) i sistemi che gli stessi gestiscono, specificando per ciascuno il profilo di autorizzazione assegnato;
11) eseguire, con cadenza almeno annuale, le attività di verifica dell'operato degli Amministratori e consentire comunque alla Regione Lazio, ove ne faccia richiesta, di eseguire in proprio dette verifiche;
12) nei limiti dell'incarico affidato, mettere a disposizione del Titolare e del DPO della Regione quando formalmente richieste, le seguenti informazioni relative agli Amministratori: log in riusciti, log in falliti, log out. Tali dati dovranno essere resi disponibili per un congruo periodo non inferiore a 6 mesi;
13) durante l'esecuzione dei Contratti, nell'eventualità di qualsivoglia modifica della normativa in materia di protezione dei dati personali, che generi nuovi requisiti (ivi incluse nuove misure di sicurezza di natura fisica, logica e/o organizzativa), la Società. si impegna a collaborare, nei limiti delle proprie competenze tecniche/organizzative e delle proprie risorse, con il Titolare affinché siano sviluppate, adottate ed implementate misure correttive di adeguamento ai nuovi requisiti.

ALLEGATO VI

Privacy by design e by default

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (privacy by design e by default)

Nel trattare i dati per conto del Titolare, o nel fornire al Titolare soluzioni di trattamento, il Responsabile deve rispettare i principi di protezione dei dati fin dalla progettazione (privacy by design) e protezione dei dati per impostazione predefinita (privacy by default) di cui all'art. 25 GDPR comunicando al Titolare le soluzioni individuate e adottate per rispettare tali principi (cfr. Considerando 78 GDPR).

Al riguardo il Titolare fornisce al Responsabile del trattamento le seguenti istruzioni:

1. la protezione dei dati deve essere presa in considerazione sin dalle fasi iniziali della pianificazione di un trattamento e ancor prima di definirne i mezzi;
2. se il Responsabile del trattamento è coadiuvato da un Responsabile della protezione dei dati (RPD), questo deve essere coinvolto per integrare la protezione dei dati fin dalla progettazione e protezione per impostazione predefinita nelle procedure di acquisizione e sviluppo, nonché lungo l'intero ciclo di vita del trattamento;
3. il Responsabile del trattamento deve essere in grado di dimostrare che la protezione dei dati fin dalla progettazione e protezione per impostazione predefinita è parte integrante del ciclo di vita dello sviluppo delle soluzioni adottate per il trattamento;
4. il Responsabile del trattamento deve tenere conto degli obblighi di fornire una tutela specifica ai minori e ad altri interessati vulnerabili, nel rispetto della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita;
5. il Responsabile del trattamento deve agevolare l'attuazione della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita al fine di supportare il Titolare nell'adempimento degli obblighi previsti dall'articolo 25 del RGPD;
6. il Responsabile del trattamento deve svolgere un ruolo attivo nel garantire che siano soddisfatti i criteri relativi allo «stato dell'arte» e notificare ai titolari del trattamento qualunque modifica a tale «stato dell'arte» che possa compromettere l'efficacia delle misure adottate; il Responsabile del trattamento deve essere in grado di dimostrare in che modo i propri mezzi (hardware, software, servizi o sistemi) permettano al Titolare di soddisfare i requisiti in materia di responsabilizzazione in conformità della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, per esempio utilizzando indicatori chiave di prestazione (KPI) per dimostrare l'efficacia delle misure e delle garanzie nell'attuazione dei principi e dei diritti;
7. il Responsabile del trattamento deve consentire al Titolare del trattamento di essere corretto e trasparente nei confronti degli interessati per quanto concerne la valutazione e dimostrazione dell'effettiva attuazione della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, analogamente a quanto si verifica nella dimostrazione della loro conformità con il RGPD in base al principio di responsabilizzazione;
8. le tecnologie di rafforzamento della protezione dei dati (PET, privacyenhancing technologies) che hanno raggiunto lo stato dell'arte possono essere utilizzate fra le misure da adottare in conformità dei requisiti della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, se del caso, secondo un approccio basato sul rischio. Si ricorda che di per sé, le PET non coprono necessariamente gli obblighi di cui all'articolo 25 del RGPD;
9. il Responsabile del trattamento deve tenere conto che i sistemi preesistenti sono soggetti agli stessi obblighi in materia di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita ai quali soggiacciono i sistemi nuovi, cosicché, ove non siano già conformi ai principi della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita e non sia possibile effettuare modifiche per adempiere ai relativi obblighi, i sistemi preesistenti non sono conformi agli obblighi del RGPD e non possono essere utilizzati per trattare dati personali;
10. il Responsabile del trattamento deve trattare solo i dati personali che sono adeguati, pertinenti e limitati a quanto necessario per la finalità. La minimizzazione dei dati realizza

e rende operativo il principio di necessità. Nel proseguire il trattamento, il Responsabile deve valutare periodicamente se i dati personali trattati siano ancora adeguati, pertinenti e necessari o se occorra cancellarli o renderli anonimi.

11. la minimizzazione può anche riferirsi al grado di identificazione. Se la finalità del trattamento non richiede che i set di dati definitivi si riferiscano a una persona fisica identificata o identificabile (come nelle statistiche), ma lo richiede il trattamento iniziale (ad es. prima dell'aggregazione dei dati), il Responsabile cancella o rende anonimi i dati personali non appena non sia più necessaria l'identificazione. Se l'identificazione continua a essere necessaria per le altre attività di trattamento, i dati personali dovrebbero essere pseudonimizzati al fine di ridurre i rischi per i diritti degli interessati.".

Art. 11

(Modifiche all'allegato OO al regolamento regionale 6 settembre 2002, n. 1 e successive modificazioni)

1. All'allegato OO del r.r. 1/2002 e successive modificazioni, sono apportate le seguenti modifiche:

a) alla sezione "1. Segnalazione" ovunque ricorra l'indirizzo PEC "databreach@regione.lazio.legalmail.it", questo è sostituito da "databreach@pec.regione.lazio.it";

b) alla sezione "3. Valutazione", dopo le parole "All'esito di questa fase, il livello di "gravità" del Personal Data Breach, che deve essere comunicato al Direttore Generale (DG), potrà essere:", la tabella è sostituita dalla seguente:

Livello	Descrizione
Basso	Gli individui non saranno interessati dalla violazione o potrebbero incontrare alcuni inconvenienti, che supereranno senza alcun problema (tempo trascorso a reinserire informazioni, fastidi, etc.).
Medio	Gli individui possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, etc.).
Alto	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in black-list, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, etc.).
Molto alto	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (difficoltà finanziarie, incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, etc.).

c) alla sezione "4. Gestione e risposta", dopo le parole "Il SDC procede secondo le regole sintetizzate in tabella", la tabella è sostituita dalla seguente:

Livello di rischio	Ove possibile entro le 72 ore	Senza ingiustificato ritardo
	Notifica al Garante	*Comunicazione all'interessato*
Molto alto	SI	SI
Alto	SI	NO
Medio	NO	NO
Basso	NO	NO

d) all'allegato B "Data Breach Report", nella sezione "Tipologie di Dati personali", nella riga "Dati particolari - patrimoniali", la parola: "- patrimoniali" è soppressa.

Art. 12

(Aggiunta degli allegati PP, QQ, RR e SS al regolamento regionale 6 settembre 2002, n. 1 e successive modificazioni)

1. Dopo l'allegato "OO" del r.r. 1/2002 e successive modificazioni, sono aggiunti gli allegati PP, QQ, RR e SS del presente regolamento.

Art. 13

(Entrata in vigore)

1. Il presente regolamento entra in vigore il giorno successivo alla sua pubblicazione sul Bollettino Ufficiale della Regione.

ALLEGATO PP

PRIVACY BY DESIGN & BY DEFAULT POLICY

- versione 1.0 -

1. INTRODUZIONE

1.1 Glossario

1.2 Premessa

1.3 Scopo

2. PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE (*privacy by design*) E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA (*privacy by default)*

2.1 PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE - *PRIVACY BY DESIGN* (ART. 25 PAR. 1 RGPD)

2.1.1 Elementi da valutare nella determinazione delle misure

a. Stato dell'arte
b. Costi di attuazione
c. Natura, ambito di applicazione, contesto e finalità del trattamento
d. Rischi per i diritti e le libertà degli interessati dal trattamento
e. Fattore temporale

2.1.2 Mantenimento e verifica dei requisiti in materia di protezione dei dati e sistemi preesistenti

2.2 PROTEZIONE DEI DATI PER IMPOSTAZIONE PREDEFINITA - *PRIVACY BY DEFAULT* (ART. 25 PAR. 2 RGPD)

3. *PRIVACY BY DESIGN E BY DEFAULT* NELL'ATTUAZIONE DEI PRINCIPI DI PROTEZIONE DATI

3.1 Trasparenza
3.2 Liceità
3.3 Correttezza
3.4 Limitazione delle finalità
3.5 Minimizzazione dei dati
3.6 Esattezza
3.7 Limitazione della conservazione
3.8 Integrità e riservatezza
3.9 Responsabilizzazione

4. UTILIZZO DELLE CERTIFICAZIONI (art. 25, paragrafo 3 RGPD)

5. *PRIVACY BY DESIGN E BY DEFAULT* NEI TRATTAMENTI BASATI SU SISTEMI DI INTELLIGENZA ARTIFICIALE

6. CONSEGUENZE DELLA NON CONFORMITA' DEL TRATTAMENTO AI PRINCIPI DI *PRIVACY BY DESIGN E BY DEFAULT*

1. INTRODUZIONE

La presente *policy* descrive i principi di *privacy by design e by default* e fornisce indicazioni per la sua applicazione pratica e per la conduzione del processo di *Data Protection by Design-by Default*. La *policy* si applica a tutte le attività di trattamento poste in essere dalla Giunta Regionale in qualità di Titolare del trattamento anche per il tramite di Responsabili/Sub-responsabili del trattamento individuati ai sensi dell'art. 28 del RGPD relativamente alle funzioni e alle competenze dell'Ente.

1.1 Glossario

Ai fini della presente *policy* si intende per:

- **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 (Art. 4 par. 1 RGPD).*
- **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, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (Art. 4 par. 2 RGPD):*
- **raccolta**: attività di acquisizione del dato;
- **registrazione**: memorizzazione dei dati su un qualsiasi supporto;
- **organizzazione**: classificazione dei dati secondo un metodo prescelto;
- **strutturazione**: attività di distribuzione dei dati secondo schemi precisi;
- **conservazione**: mantenere le informazioni su un qualsiasi supporto;
- **elaborazione**: attività con la quale il dato personale subisce una modifica sostanziale (la modificazione può riguardare anche solo parte minima del dato personale);
- **estrazione**: attività di estrapolazione di dati da gruppi già memorizzati;
- **consultazione**: lettura dei dati personali (anche la semplice visualizzazione);
- **uso**: attività generica che ricopre qualsiasi tipo di impiego di dati;
- **comunicazione**: dare conoscenza di dati personali ad uno o più soggetti diversi dall'interessato, dal responsabile o dagli autorizzati (dato trasferito a terzi), comunque in numero determinato;
- d**iffusione** si intende invece il dare conoscenza a soggetti indeterminati, in qualunque forma;
- **raffronto**: operazione di confronto tra dati, sia in conseguenza di elaborazione che di consultazione;
- **interconnessione**: utilizzo di più banche dati;
- **limitazione**: conservazione con sospensione temporanea di ogni altra operazione di trattamento;

- **cancellazione**: eliminazione di dati tramite utilizzo di strumenti elettronici;
- **distruzione**: attività di eliminazione definitiva dei dati.
- **Titolare del trattamento**: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; 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 (Art. 4 par. 7 RGDP).*
- **Responsabile del trattamento**: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento (Art. 28 RGPD).*
- **Destinatario**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi (*Art. 4, par. 1, n. 9 del RGDP*).
- **Registro dei trattamenti**: *documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del RGPD) relative alle operazioni di trattamento svolte dal Titolare e, se nominato, dal responsabile del trattamento. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.*
- **Principio di responsabilizzazione (*accountability*):** *adozione di comportamenti proattivi da parte del Titolare o del Responsabile del trattamento, tali da dimostrare e documentare la concreta adozione di misure finalizzate ad assicurare l'applicazione del RGPD alle attività di trattamento.*
- **Minaccia**: *identifica una situazione di "pericolo" la cui realizzazione potrebbe incidere sulla riservatezza, e/o integrità, e/o disponibilità dei dati e sui diritti e le libertà degli interessati.*
- **Probabilità***: corrisponde alla possibilità di realizzazione di una minaccia.*
- **Impatto:** *corrisponde alle conseguenze negative sui diritti e le libertà degli interessati nel caso in cui si concretizzi la minaccia.*
- **Valutazione del rischio***: è il processo di valutazione che analizza lo scenario del rischio in relazione alla probabilità combinata con i possibili impatti negativi sulle libertà e i diritti degli interessati tenendo conto delle misure tecniche e organizzative che il Titolare ha adottato o intende adottare per mitigare il rischio stesso.*
- **Rischio inerente:** *è determinato dal valore del rischio in relazione alla probabilità di accadimento della minaccia e dell'impatto al concretizzarsi della stessa in assenza di misure di mitigazione.*
- **Rischio residuo:** *è determinato dal valore del rischio dopo l'applicazione da parte del Titolare delle misure tecniche e organizzative finalizzate alla mitigazione del rischio inerente.*
- **DPIA:** è *la valutazione di impatto sulla protezione dei dati (Data Protection Impact Assessments) da effettuare ogniqualvolta, all'esito della valutazione del rischio, il trattamento dei dati continua a comportare un rischio residuo elevato per i diritti e le libertà degli interessati e in tutti gli altri casi previsti dall'articolo 35 del RGPD.*

Per quanto non espressamente previsto nel presente paragrafo si applicano le definizioni contenute nel RGPD.

1.2 Premessa

Il rispetto dei principi di protezione dei dati fin dalla progettazione (*privacy by design*) e di protezione per impostazione predefinita (*privacy by default*) stabilito dall'articolo 25 del RGPD costituisce un obbligo per il Titolare del trattamento che è chiamato a predisporre le misure adeguate e le garanzie finalizzate ad una attuazione efficace dei principi del trattamento dei dati nonché alla massima protezione dei diritti e delle libertà degli interessati.

Il Titolare deve applicare i principi di *privacy by design e by default:*

- prima di iniziare una nuova attività di trattamento e sin dalla progettazione della stessa;
- durante lo svolgimento dell'attività di trattamento verificando costantemente l'efficacia delle misure adottate e delle garanzie individuate.

L'applicazione dei principi di *privacy by design e by default* si riferisce anche alle attività di trattamento nell'ambito di sistemi preesistenti, anche ante RGPD.

Inoltre, la presente policy deve essere presa sistematicamente in considerazione nell'ambito degli appalti pubblici: la Regione è tenuta ad assicurare il rispetto degli obblighi di *privacy by design e by default* in relazione al trattamento svolto dai rispettivi responsabili e sub-responsabili e, pertanto, deve tenerne conto quando stipula contratti con tali soggetti.

La presente *policy*, tenuto conto del contesto specifico del trattamento, esamina gli elementi chiave della progettazione (*by design*) e dell'impostazione predefinita (*by default*) e la loro applicazione pratica, al fine di fornire indicazioni per un'efficace attuazione dei principi di protezione dei dati contenuti nell'articolo 5 del RGPD.

In attuazione di tali principi, il Titolare del trattamento, anche quando utilizza sistemi tecnologici realizzati da terzi, deve eseguire un'analisi dei rischi ed eventualmente una valutazione d'impatto e accertarsi che le funzionalità corrispondano alle finalità del trattamento individuate che abbiano una specifica base giuridica.

1.3 Scopo

Lo scopo della presente *policy* è quello di fornire indicazioni volte ad applicare i principi di *privacy by design & by default* nelle fasi di definizione e di attuazione di un processo[1] nel caso in cui lo stesso contempli l'uso di dati personali, in modo che il Titolare possa essere in grado di dimostrare e documentare che le proprie attività siano assistite da misure di sicurezza e garanzie adeguate ad assicurare il rispetto dei principi di protezione dei dati e la tutela dei diritti e delle libertà degli interessati.

2. PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE (*privacy by design*) E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA (*privacy by default)*

2.1 PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE - *PRIVACY BY DESIGN* (ART. 25 PAR. 1 RGPD)

[1] Si intende per processo l'insieme di operazioni/azioni, poste in essere da soggetti o strutture organizzative finalizzate al raggiungimento di uno specifico scopo. Rientrano nel concetto di processo riferito alle attività e alle funzioni della Giunta Regionale, a titolo esemplificativo e non esaustivo: le proposte di leggi regionali, i regolamenti, gli atti amministrativi generali, gli atti di organizzazione, i bandi di concorso e le procedure di reclutamento, i bandi di gara e i contratti pubblici, l'erogazione di contributi, le campagne di comunicazione e informazione, lo sviluppo e la gestione di sistemi informativi, ecc.

L’obbligo del rispetto del principio della protezione dati fin dalla progettazione (*privacy by design*) consiste nell’obbligo del Titolare del trattamento di attuare le misure tecniche e organizzative adeguate[2] e le necessarie garanzie a tutela dei diritti e delle libertà degli interessati prima che inizi qualunque attività di trattamento.

Le misure tecniche e organizzative adottate dal Titolare devono essere:

- adeguate: funzionali all’attuazione dei principi del trattamento di cui all’art. 5 del RGPD e della conseguente tutela dei diritti degli interessati;
- efficaci:
  - perseguire i risultati previsti dal Titolare;
  - individuate in relazione allo specifico trattamento e in rapporto alla valutazione dei rischi dello stesso;
  - definite all’esito della valutazione degli elementi di cui al paragrafo che segue;
- documentate e dimostrabili: il Titolare del trattamento deve disporre della documentazione relativa alle misure tecniche e organizzative applicate dalla quale si evinca la dimostrazione dell’efficacia delle misure stesse (ad esempio attraverso l’uso di indicatori di efficacia[3]).

2.1.1 Elementi da valutare nella determinazione delle misure

Il Titolare, quando determina le misure tecniche e organizzative relative ad uno specifico trattamento deve tenere conto, dei seguenti elementi:

a. stato dell’arte;
b. costi di attuazione;
c. natura, ambito di applicazione, contesto e finalità del trattamento;
d. rischi per i diritti e le libertà degli interessati dal trattamento;
e. fattore temporale.

a. Stato dell’arte

La valutazione di questo elemento è applicabile sia alla determinazione delle misure tecniche che alla determinazione di quelle organizzative integrate nel trattamento.

La valutazione dello stato dell’arte nella determinazione delle misure tecniche consiste prevalentemente nelle seguenti attività del Titolare del Trattamento:

- valutazione dello stato della tecnologia applicata allo specifico trattamento disponibile sul mercato;
- valutazione dei rischi che la tecnologia applicata determina sul trattamento;
- valutazione dello stato delle misure e delle garanzie disponibili ed efficaci in rapporto all’evoluzione del panorama tecnologico.

[2] Le misure adottate dal Titolare, tenuto conto del contesto del trattamento, possono comprendere, a titolo esemplificativo e non esaustivo: la pseudonimizzazione dei dati personali, la memorizzazione di dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico, la possibilità per gli interessati di intervenire nel trattamento, l’informazione sulla conservazione dei dati personali, la disponibilità di sistemi di rilevamento di malware, la formazione dei dipendenti, l’istituzione di sistemi di gestione della privacy e della sicurezza delle informazioni, l’obbligo contrattuale per i responsabili del trattamento di attuare prassi specifiche di minimizzazione dei dati, adozione di standard, migliori prassi e codici di condotta riconosciuti da associazioni e da altri organismi.

[3] Gli indicatori possono essere quantitativi (es. riduzione di reclami e/o segnalazioni, diminuzione dei tempi di risposta alle istanze dei diritti degli interessati, ecc) o qualitativi (es. valutazioni delle prestazioni, ecc.).

La valutazione dello stato dell'arte nella determinazione delle misure organizzative consiste prevalentemente nelle seguenti attività del Titolare del Trattamento:

- valutazione delle politiche interne adottate ed eventualmente della necessità del loro adeguamento;
- valutazione del livello della formazione del personale con particolare riferimento al contesto tecnologico;
- valutazione delle politiche di gestione e di governance della sicurezza informatica.

Nelle valutazioni sopra richiamate il Titolare può:

- prendere a riferimento standard, certificazioni e/o codici di condotta esistenti e riconosciuti che possono contribuire a indicare lo "stato dell'arte" nello specifico ambito;
- utilizzare i livelli di protezione previsti negli standard sopra richiamati ai fini della progettazione e dell'attuazione delle misure di protezione dei dati.

Lo stato dell'arte è un concetto dinamico, soggetto ad una valutazione continua, soprattutto se riferito al contesto tecnologico; pertanto, il Titolare è tenuto a periodiche valutazioni finalizzate alla verifica che le misure individuate garantiscano un livello di protezione adeguato e provvedere, all'occorrenza al loro aggiornamento; una condotta difforme determina la mancata osservanza dell'articolo 25 del RGPD.

b. Costi di attuazione

La valutazione di questo elemento è applicabile sia alla determinazione delle misure tecniche che alla determinazione di quelle organizzative integrate nel trattamento. Il concetto di "costo di attuazione" ha una accezione ampia e contempla la valutazione delle risorse legate a diversi fattori: tempo, risorse umane, dotazioni strutturali, risorse economiche, ecc.

La valutazione del "costo di attuazione" nella determinazione delle misure tecniche e organizzative consiste prevalentemente nelle seguenti attività del Titolare del Trattamento:

- valutazione dell'economicità intesa come impiego di quantità di risorse proporzionata all'efficacia al fine di evitare soluzioni eccessivamente dispendiose e di adottare, in caso di efficacia equivalente, soluzioni più economiche;
- gestione dei costi complessivi come sopra determinati al fine di attuare con efficacia i principi di protezione dati e la tutela dei diritti degli interessati.

Il Titolare, per non incorrere nella mancata osservanza dell'articolo 25 del RGPD, è comunque tenuto ad assicurarsi che, indipendentemente dal costo, le misure individuate garantiscano che l'attività di trattamento sia conforme ai principi di cui all'art. 5 del RGPD.

c. Natura, ambito di applicazione, contesto e finalità del trattamento

La valutazione di questi elementi è applicabile sia nella determinazione delle misure tecniche che nella determinazione di quelle organizzative integrate nel trattamento. Allo scopo di integrare principi di protezione dei dati nella progettazione del trattamento, questi fattori devono essere interpretati in coerenza con altre disposizioni del RGPD, tra cui gli artt. 24, 32 e 35.

L'analisi di questi fattori nella determinazione delle misure consiste nelle seguenti attività del Titolare del Trattamento riferite al singolo fattore:

- natura: valutazione delle caratteristiche intrinseche del trattamento;
- ambito di applicazione: valutazione della dimensione e dell'ampiezza del trattamento;

- contesto: valutazione delle circostanze che possono influenzare le aspettative degli interessati dal trattamento;
- finalità: determinazione degli obiettivi del trattamento.

d. Rischi per i diritti e le libertà degli interessati dal trattamento

Al fine di individuare le misure tecniche e organizzative adeguate alla tutela delle persone fisiche e dei loro dati personali e di adempiere ai requisiti previsti dal RGPD, il Titolare del trattamento, nel determinare le misure tecniche e organizzative adotta un approccio basato sul rischio (artt. 24, 25, 32 e 35 RGPD).

La valutazione del rischio per la sicurezza dei dati - e del trattamento - nella determinazione delle misure tecniche e organizzative consiste in un esame sistematico e approfondito del trattamento e determina le seguenti attività in capo al Titolare del Trattamento:

- individuazione dei rischi inerenti presentati dal trattamento dei dati personali;
- determinazione della probabilità di accadimento della minaccia e dell'impatto della stessa sui diritti degli interessati;
- individuazione di misure efficaci a mitigare il rischio individuato;
- valutazione del rischio residuo;
- esecuzione di una DPIA qualora il trattamento dei dati continui a comportare un rischio residuo elevato per i diritti e le libertà degli interessati.

Il Titolare nella valutazione dei rischi del trattamento, al fine di affrontare rischi simili in situazioni analoghe (natura, ambito di applicazione, contesto e finalità del trattamento) può utilizzare anche dati di riferimento derivanti dalle migliori prassi e/o standard, ma anche in questo caso è comunque chiamato a:

- effettuare una valutazione del rischio per la sicurezza dei dati e del trattamento per ogni attività di trattamento;
- verificare l'efficacia delle misure adottate e delle garanzie proposte;
- valutare se il trattamento necessita di una valutazione d'impatto (DPIA) ex art. 35 RGPD;
- aggiornare periodicamente la valutazione del rischio e la valutazione di impatto e verificare la conformità del trattamento.

e. Fattore temporale

Il Titolare del trattamento deve integrare i principi di protezione dei dati nella progettazione del trattamento in fase precoce, sin dal "*momento di determinare i mezzi del trattamento";* i "*mezzi del trattamento*" rappresentano gli elementi generali della progettazione di un trattamento, e individuano come effettuare il trattamento stesso e i meccanismi impiegati per attuarlo.

L'applicazione del fattore temporale impone al Titolare, al momento di definire l'architettura, la procedura e i protocolli applicabili al trattamento, di mettere in atto le seguenti attività:

- valutazione delle misure e delle garanzie adeguate ad attuare efficacemente i principi e tutelare i diritti degli interessati;
- valutazione dei rischi e di tutti gli altri elementi che concorrono all'applicazione concreta del principio di privacy *by design* sopra analizzati (stato dell'arte, costo di attuazione, natura del trattamento, ambito di applicazione, contesto e finalità);

- valutazione dei tempi e dei costi/benefici dei servizi necessari al trattamento dati *ex ante* (es. software e hardware), in modo da scongiurare modifiche successive su trattamenti già progettati, pianificati e definiti.

2.1.2 Mantenimento e verifica dei requisiti in materia di protezione dei dati e sistemi preesistenti

Una volta avviato il trattamento, al fine di dare un'attuazione efficace e costante ai principi nonché di tutelare i diritti, il Titolare è tenuto a mantenere su base continuativa l'applicazione dei principi di *privacy by design e by default.* L'ambito di applicazione, il contesto delle operazioni di trattamento, nonché il rischio possono mutare nel corso del trattamento; pertanto, è fatto obbligo al Titolare di verificare e riesaminare periodicamente l'efficacia delle misure e delle garanzie poste in essere.

Tale obbligo si applica anche:

- ai sistemi preesistenti: i sistemi progettati prima dell'entrata in vigore del RGPD devono essere sottoposti a verifiche e manutenzione per garantire l'applicazione di misure e garanzie adeguate ed efficaci;
- ai trattamenti svolti per mezzo di Responsabili del trattamento: le operazioni di trattamento effettuate dai Responsabili devono essere regolarmente esaminate e valutate, almeno annualmente, dal Titolare per garantire che continuino a rispettare i principi e permettano ai Titolari stessi di adempiere agli obblighi in materia di protezione dei dati personali.

2.2 PROTEZIONE DEI DATI PER IMPOSTAZIONE PREDEFINITA - *PRIVACY BY DEFAULT* (ART. 25 PAR. 2 RGPD)

L'espressione *privacy by default* (per impostazione predefinita) si riferisce all'obbligo del Titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento. L'impostazione predefinita si riferisce alle scelte compiute rispetto a valori di configurazione od opzioni di trattamento (esempio un'applicazione informatica, un servizio ecc.), tali da incidere sulla quantità dei dati personali raccolti, sulla portata del trattamento, sul periodo di conservazione e sull'accesso ai dati.

Ai fini dell'applicazione del principio di *privacy by default* (per impostazione predefinita) il Titolare deve:

- <u>trattare solo dati personali necessari per ogni specifica finalità del trattamento</u>:
  Il Titolare, dopo aver valutato la necessità del trattamento in relazione alle condizioni di liceità previste dal RGPD, deve impostare le attività di trattamento in modo da garantire che venga effettuato solo il trattamento di dati strettamente necessari per conseguire la specifica e lecita finalità dello stesso e conservarli per il periodo strettamente necessario, a tal fine è tenuto:

- a definire in anticipo quali dati personali debbano essere raccolti e trattati per le finalità specifiche, esplicite e legittime dello specifico trattamento;
- a definire, per impostazione predefinita, le misure che garantiscano il trattamento dei soli dati personali necessari;

- ad eseguire, in caso di utilizzo di software di terze parti, una valutazione dei rischi del prodotto ed a disattivare, all'occorrenza, funzioni che non hanno una base giuridica o che non sono compatibili con le finalità del trattamento.
- tenere conto del perimetro dell'obbligo di minimizzazione dei dati di cui all'art. 25, paragrafo 2, RGPD che vale per:
- la quantità dei dati personali raccolti: le impostazioni predefinite non devono includere la raccolta di dati personali che non siano necessari per la specifica finalità del trattamento; tale impostazione prescrive di non raccogliere dati in eccesso rispetto a quelli strettamente necessari, ma anche di non raccogliere dati particolareggiati qualora dati meno granulari siano sufficienti al raggiungimento delle finalità del trattamento;
- la portata del trattamento: le impostazioni predefinite devono garantire che i trattamenti effettuati sui dati personali si limitano alle operazioni strettamente necessarie al raggiungimento delle finalità;
- il periodo di conservazione: le impostazioni predefinite devono garantire che il periodo di conservazione dei dati personali corrisponda al tempo strettamente necessario al raggiungimento della specifica finalità del trattamento. La scelta del tempo di conservazione, in base al principio di responsabilizzazione, deve essere giustificabile e documentabile da parte del Titolare.
- l'accesso ai dati: le impostazioni predefinite devono limitare il più possibile l'accesso ai dati, pertanto il Titolare deve:
- limitare l'accesso ai dati personali esclusivamente a soggetti autorizzati;
- abilitare gli accessi ai dati personali solo dopo la valutazione sull'effettiva necessità del trattamento degli stessi; i dati devono essere resi accessibili a un numero definito di persone fisiche;
- effettuare i controlli sugli accessi per l'intero flusso dei dati per la durata del trattamento.

3. *PRIVACY BY DESIGN E BY DEFAULT* NELL'ATTUAZIONE DEI PRINCIPI DI PROTEZIONE DATI

Il Titolare deve tenere in considerazione gli elementi e i fattori della *privacy by design e by default* richiamati nei paragrafi che precedono in tutte le fasi di progettazione delle attività di trattamento, anche nell'attuazione dei principi di protezione dati indicati nell'articolo 5 e nel considerando 39 del RGPD:

3.1 trasparenza;
3.2 liceità;
3.3 correttezza;
3.4 limitazione delle finalità;
3.5 minimizzazione dei dati;
3.6 esattezza;
3.7 limitazione della conservazione;
3.8 integrità e riservatezza;
3.9 responsabilizzazione.

3.1 Trasparenza

Il principio di trasparenza del trattamento è rinvenibile negli articoli 12, 13, 14 e 34 del RGPD. Il Titolare ha l'obbligo di effettuare attività di trattamento trasparenti al fine di consentire agli interessati di comprendere il trattamento dei dati che li riguardano e, all'occorrenza, di avvalersi dei diritti di cui agli artt. 15 e ss del RGPD.

L'applicazione del principio della trasparenza nella *privacy by design e by default* impone al Titolare che le informazioni agli interessati abbiano le seguenti caratteristiche:

- chiarezza – linguaggio chiaro, semplice, conciso, comprensibile;
- accessibilità – facilità di accesso per gli interessati;
- contestualità – fornite al momento opportuno e nella forma adeguata;
- pertinenza – pertinenti e applicabili all'interessato specifico;
- progettazione universale – rispondere a criteri di accessibilità per tutti gli interessati anche utilizzando linguaggi leggibili da macchine che agevolino e/o automatizzino la leggibilità;
- comprensibilità – gli interessati devono avere una buona comprensione di ciò che possono aspettarsi dal trattamento dei loro dati personali, in particolare quando si tratti di minori o di soggetti appartenenti ad altre categorie vulnerabili;
- multicanalità – devono essere fornite attraverso canali e mezzi di comunicazione diversi per aumentare la probabilità che raggiungano efficacemente l'interessato;
- approccio multilivello – devono essere fornite secondo un approccio multilivello, con l'evidenziazione dei punti più importanti e rendendo facilmente accessibili informazioni più dettagliate con collegamenti a ulteriori punti e concetti (es. attraverso menu a discesa) al fine di garantire un equilibrio tra completezza e comprensibilità.

3.2 Liceità

Il Titolare ha l'obbligo di identificare una base giuridica valida per il trattamento dei dati personali di sua competenza e l'intero ciclo di vita del trattamento deve essere in linea con la base giuridica identificata.

Gli elementi da valutare ai fini del principio di liceità nell'applicazione della *privacy by design e by default* sono:

- pertinenza: il trattamento deve essere riferito a una corretta base giuridica;
- differenziazione: la base giuridica va differenziata e riferita a ciascuna specifica attività di trattamento;
- specificità della finalità: la base giuridica deve essere connessa alla specifica finalità di trattamento;
- necessità: il trattamento deve essere necessario e non soggetto a condizioni affinché la sua finalità sia lecita;
- consenso: il consenso deve essere liberamente espresso, specifico, informato e inequivocabile. Quando il Titolare del trattamento è una pubblica autorità, il consenso costituisce una base giuridica residuale e non dovrebbe potersi considerare un valido fondamento giuridico a causa dello squilibrio tra l'interessato e il Titolare;
- revoca del consenso: qualora la base giuridica del trattamento si identifichi con il consenso per la revoca dello stesso deve essere garantita con la stessa facilità con cui è stato prestato;
- bilanciamento degli interessi: quando la base giuridica è costituita da interessi legittimi, il Titolare deve effettuare un bilanciamento ponderato, considerando in particolare lo squilibrio tra i rapporti di forza, (in particolare in caso di minori o soggetti vulnerabili) e devono essere previste misure e garanzie per attenuare l'impatto negativo sugli interessati. La condizione del legittimo interesse non si applica al trattamento di dati effettuato dalle pubbliche autorità;
- predeterminazione: la base giuridica è stabilita prima di iniziare l'attività di trattamento;
- cessazione; in presenza di una base giuridica non valida il trattamento va immediatamente cessato;
- attribuzione di responsabilità; in caso di contitolarità del trattamento, le parti individuano in modo chiaro e trasparente le basi giuridiche ed elaborano le misure del trattamento in relazione alle stesse.

3.3 Correttezza

La correttezza è un principio di natura trasversale che impone di non trattare i dati in modo dannoso, discriminatorio, imprevisto o fuorviante per l'interessato. Il principio di correttezza integra i diritti e le libertà degli interessati con particolare riferimento al diritto di essere informati (trasparenza), al diritto di intervenire nel trattamento (accesso, cancellazione, portabilità dei dati, rettificazione) e al diritto di limitazione del trattamento, nonché il diritto a non essere sottoposto a un processo decisionale automatizzato e non subire discriminazioni nel contesto di tali processi; il diritto alla portabilità dei dati, ai sensi dell'art. 20, par. 3, del RGPD, non si applica al trattamento effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

Gli elementi da valutare ai fini del principio di correttezza nell'applicazione della *privacy by design e by default* sono:

- interazione: garantire agli interessati l'esercizio dei propri diritti in relazione ai dati personali trattati dal Titolare;
- aspettativa; il trattamento deve corrispondere alle aspettative ragionevoli degli interessati;
- assenza di discriminazione: dal trattamento non deve derivare alcuna discriminazione degli interessati;
- assenza di sfruttamento: il trattamento non deve generare sfruttamento delle vulnerabilità degli interessati;
- rispetto dei diritti: il trattamento deve rispettare i diritti fondamentali degli interessati; eventuali compressioni degli stessi devono essere espressamente previste dalla legge;
- eticità: il trattamento deve essere effettuato nel rispetto dei diritti e della dignità delle persone;
- veridicità: il trattamento deve essere effettuato secondo le modalità comunicate agli interessati.

3.4 Limitazione delle finalità

Il principio della limitazione delle finalità impone al Titolare di raccogliere e trattare dati per finalità specifiche, esplicite e legittime e di non trattarli ulteriormente oltre i limiti delle finalità definite.

Il trattamento in fase di progettazione deve essere sviluppato per conseguire le finalità definite; in caso di trattamento ulteriore, il Titolare ha l'obbligo di verificare periodicamente se lo stesso sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti tenendo conto dei seguenti elementi:

- nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
- contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il Titolare del trattamento;
- natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;
- possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
- esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Gli elementi da valutare ai fini del principio di limitazione delle finalità nell'applicazione della *privacy by design e by default* sono:

- predeterminazione: le finalità sono determinate prima della progettazione del trattamento;

- specificità: le finalità sono specifiche ed esplicite e si riferiscono al motivo per cui i dati personali vengono trattati;
- orientamento in base alla finalità: le finalità orientano la progettazione del trattamento e ne determinano i limiti;
- necessità: la finalità determina quali sono i dati personali necessari per il trattamento;
- compatibilità: eventuali nuove finalità determinano una verifica della compatibilità con la finalità originaria per la quale i dati sono stati raccolti e, ove necessario, modifiche nella progettazione del trattamento;
- limitazione di trattamenti ulteriori: non devono essere effettuati ulteriori trattamenti per finalità diverse che non sono compatibili con quelle originariamente determinate;
- limitazioni del riutilizzo; il Titolare ha l'obbligo di limitare la possibilità di riutilizzo dei dati personali adottando adeguate misure tecniche (es. hashing e/o cifratura) e organizzative (es. politicy, definizione di clausole e obblighi contrattuali);
- riesame periodico: il Titolare ha l'obbligo di verificare periodicamente se il trattamento sia necessario per le finalità per le quali sono stati raccolti i dati e testare la progettazione di tale trattamento con riguardo al principio di limitazione delle finalità.

3.5 Minimizzazione dei dati

Il Titolare può sottoporre a trattamento solo i dati che risultino adeguati, pertinenti e limitati al perseguimento della finalità cui sono sottoposti. Il principio di minimizzazione dei dati obbliga il Titolare, prima di iniziare il trattamento e durante il ciclo di vita dello stesso, ad effettuare le seguenti valutazioni:

- se per le finalità individuate sia necessario trattare i dati personali;
- se sia possibile conseguire ugualmente le finalità individuate trattando una quantità inferiore di dati personali o utilizzando dati meno dettagliati o aggregati;
- se le finalità individuate possano essere conseguite con un minor grado di identificazione dei dati:
- verificare se la finalità sia perseguibile anche con dati statistici e aggregati non riferiti a persone fisiche identificate o identificabili;
- verificare se i dati riferiti alle persone fisiche originariamente necessari per il trattamento iniziale siano ancora necessari;
- cancellare o rendere anonimi i dati personali nel caso in cui non sia più necessaria l'identificazione;
- pseudonimizzare i dati nel caso in cui l'identificazione continui ad essere necessaria per le altre attività di trattamento al fine di ridurre i rischi per i diritti degli interessati.

Gli elementi da valutare ai fini del principio di minimizzazione dei dati nell'applicazione della *privacy by design e by default* sono:

- evitare il trattamento dei dati qualora la finalità sia comunque raggiungibile anche senza di esso;
- limitazione: limitare la quantità di dati personali raccolti a ciò che è necessario per la specifica finalità;
- limitazione dell'accesso: limitare al minimo il numero di persone che accede ai dati personali per esercitare le proprie funzioni;
- pertinenza: limitare l'utilizzo dei dati personali a quelli pertinenti al trattamento; dimostrare tale pertinenza;
- necessità: limitare il trattamento ai dati senza i quali non è possibile conseguire la specifica finalità;
- aggregazione: prediligere ove possibile l'utilizzo di dati aggregati;
- pseudonimizzazione: pseudonimizzare i dati personali quando non è più necessario disporre di dati personali identificabili e memorizzare le chiavi di identificazione separatamente;

- anonimizzazione e cancellazione: rendere anonimi e cancellare tutti i dati personali che non sono più necessari per la specifica finalità;
- flusso dei dati: il flusso dei dati non deve generare copie ulteriori di dati rispetto a quanto necessario alle finalità del trattamento;
- stato dell'arte: applicare tecnologie aggiornate e adeguate a minimizzare il trattamento dei dati.

3.6 Esattezza

Il Titolare ha l'obbligo di adottare adeguate misure tecniche e organizzative per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati affinché i dati personali utilizzati siano esatti e, se necessario, aggiornati. La valutazione del requisito dell'esattezza del dato va effettuata anche in relazione al rischio concreto derivante dall'utilizzo di dati inesatti[4].

Gli elementi da valutare ai fini del principio di esattezza dei dati nell'applicazione della *privacy by design e by default* sono:

- fonte dei dati: utilizzare solo fonti di dati personali attendibili;
- grado di esattezza: ciascun elemento di dato personale deve essere il più esatto possibile in base alle specifiche finalità individuate;
- esattezza misurabile: utilizzare sistemi e applicare misure che riducano al minimo numero di falsi positivi/negativi;
- verifica: verificare la correttezza dei dati personali presso l'interessato prima del trattamento e nelle sue diverse fasi a seconda della natura dei dati, e in relazione alla frequenza delle relative modifiche;
- cancellazione/rettifica: cancellare o rettificare tempestivamente i dati inesatti;
- evitare/limitare la propagazione di errori: al verificarsi dell'errore attenuarne l'effetto nella catena di trattamento;
- accesso: fornire agli interessati adeguate e pertinenti informazioni in modo che gli stessi, all'occorrenza, possano efficacemente esercitare i diritti di cui agli artt. 15 e ss. del RGPD;
- esattezza permanente; assicurare l'esattezza dei dati in tutte le fasi del trattamento ed effettuare verifiche di esattezza nelle fasi critiche;
- aggiornamento: aggiornare i dati personali ogni qualvolta si renda necessario per il raggiungimento della specifica finalità;
- progettazione dei dati: adottare misure organizzative e tecniche di progettazione finalizzate alla limitazione delle inesattezze dei dati (es. limitazione dei campi a testo libero predisponendo la possibilità di scelte predeterminate).

3.7 Limitazione della conservazione

I dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un periodo limitato a quello necessario per le finalità per le quali i dati personali sono trattati. La finalità del trattamento è il criterio principale per stabilire la durata della conservazione dei dati personali.

Gli elementi da valutare ai fini del principio di limitazione della conservazione dei dati nell'applicazione della *privacy by design e by default* sono:

[4] Si riportano di seguito alcuni esempi di conseguenze derivanti dal trattamento di dati inesatti: diagnosi errate, applicazione di errati protocollo sanitari, decisioni erronee conseguenti a processi manuali o automatizzati ecc.

- periodo di conservazione: il periodo di conservazione deve essere riferito alla specifica finalità del trattamento individuata.
- cancellazione e anonimizzazione: predisporre procedure interne per la cancellazione e/o l'anonimizzazione dei dati; l'anonimizzazione può costituire un'alternativa alla cancellazione, a condizione che siano valutati la probabilità e la gravità del rischio ivi compreso quello della eventuale re-identificazione;
- efficacia dell'anonimizzazione/cancellazione: adottare misure efficaci per assicurare la non reidentificazione dei dati anonimizzati o il recupero dei dati cancellati;
- automatizzazione: automatizzare il più possibile la cancellazione dei dati personali non necessari;
- criteri di conservazione: stabilire la durata della conservazione dei dati personali identificandoli rispetto alla specifica finalità;
- giustificazione: capacità di documentare la determinazione del periodo di conservazione rispetto alla finalità individuata;
- applicazione delle politiche di conservazione: adottare politiche di conservazione interne e verificare la loro applicazione;
- registri di eventi: definire i dati personali necessari per i registri di eventi;
- flusso di dati: monitorare il flusso di dati personali e la generazione delle copie, limitandone la conservazione anche temporanea.

3.8 Integrità e riservatezza

Ai dati personali trattati, affinché rimangano integri e riservati, devono essere applicate misure tecniche e organizzative adeguate a garantire la protezione da trattamenti illeciti o non autorizzati nonché da incidenti di violazione dei dati (*data breach*). Sul Titolare grava l'obbligo di valutare costantemente i mezzi del trattamento e le misure di sicurezza scelte attraverso revisioni periodiche delle stesse nonché di dotarsi di una procedura per la gestione delle violazioni dei dati.

Gli elementi da valutare ai fini del principio di integrità e riservatezza dei dati nell'applicazione della *privacy by design e by default* sono:

- sistema di gestione della sicurezza delle informazioni: predisporre strumenti operativi, politiche e procedure per assicurare la sicurezza delle informazioni;
- analisi/valutazione del rischio: valutare costantemente i rischi per la sicurezza dei dati personali e del trattamento, considerando l'impatto sui diritti delle persone, e predisporre misure di contrasto per i rischi identificati;
- standardizzazione delle minacce: definire, attraverso l'analisi riferita alla superficie di attacco di specifici sistemi, una standardizzazione esaustiva, sistematica e realistica delle minacce possibili al fine di ridurre i vettori di attacco e le opportunità di sfruttamento delle vulnerabilità;
- sicurezza fin dalla progettazione: progettare e sviluppare i sistemi tenendo conto dei requisiti di sicurezza appropriati al quadro tecnologico del momento; svolgere costantemente test pertinenti;
- manutenzione: verificare periodicamente software e hardware, sistemi e servizi, prodotti e applicazioni al fine di monitorarne costantemente le vulnerabilità e adottare le relative misure di mitigazione delle stesse;
- gestione del controllo degli accessi: l'accesso ai dati deve essere limitato al solo personale autorizzato differenziando i privilegi di accesso secondo i seguenti criteri:
- limitazione dell'accesso: progettare il trattamento dei dati in modo tale che accedano ai dati un numero minimo di persone;

- limitazione al contenuto dei dati: differenziare e limitare l'accesso ai dati sia rispetto allo svolgimento della singola operazione, sia agli ambiti di competenza del rispettivo dipendente autorizzato al trattamento;
- segregazione dell'accesso: progettare il trattamento in modo da evitare l'accesso totale ai dati degli interessati o di categorie specifiche degli stessi;
- trasferimenti sicuri: proteggere la trasmissione di dati da modifiche e accessi non autorizzati e/o accidentali;
- conservazione sicura: proteggere la conservazione dei dati da modifiche e accessi non autorizzati attraverso procedure per valutare il rischio di conservazione centralizzata o decentrata sulle categorie di dati personali a cui si applicano adottando all'occorrenza misure di sicurezza adeguate. In caso di rischio elevato il Titolare è tenuto ad adottare sistemi di cifratura dei dati personali;
- pseudonimizzazione e cifratura: pseudonimizzare i dati personali e cifrare i backup/registri di eventi come misura di sicurezza per ridurre al minimo i rischi di potenziali violazioni;
- backup/registri di eventi: conservare backup e registri di eventi nella misura necessaria per la sicurezza delle informazioni e utilizzarli su base routinaria al fine di monitorare gli eventi e adempiere ai controlli di sicurezza prevedendo revisioni periodiche;
- ripristino in caso di disastro (*disaster recovery*/continuità operativa): prevedere procedure di ripristino del sistema informativo in caso di disastro al fine di garantire la continuità operativa (*business continuity*) e di ripristinare velocemente la disponibilità dei dati personali in caso di incidenti rilevanti;
- protezione in base al rischio: proteggere le categorie di dati personali contro il rischio di violazioni della sicurezza con misure di sicurezza adeguate; tenere separati i dati che comportano rischi particolari dagli altri dati personali, adottando misure più elevate quali la cifratura;
- gestione della risposta in caso di incidenti legati alla sicurezza: predisporre metodologie e procedure finalizzate a rilevare, limitare, gestire e segnalare le violazioni dei dati e prevedere dei processi di *lesson learned*;
- gestione delle violazioni di dati personali: disporre procedure di gestione degli incidenti di sicurezza e delle violazioni di dati personali, comprese procedure di notifica quali la gestione delle notifiche verso l'Autorità e di comunicazione verso gli interessati.

3.9 Responsabilizzazione

Ai fini dell'applicazione del principio di responsabilizzazione il Titolare deve conoscere ed attuare le norme europee e nazionali in materia di protezione dei dati adempiendo ai relativi obblighi. Il Titolare è responsabile che le attività di trattamento siano conformi a tutti i principi enunciati ai punti che precedono e deve essere in grado di dimostrare e documentare tale conformità, comprovando gli effetti delle misure adottate per tutelare i diritti degli interessati e i motivi per cui tali misure sono considerate adeguate ed efficaci.

4. UTILIZZO DELLE CERTIFICAZIONI (art. 25, paragrafo 3 RGPD)

Ai sensi dell'articolo 25, par. 3 del RGPD il Titolare del trattamento può utilizzare le certificazioni di cui all'articolo 42 RGPD come un elemento per dimostrare la conformità dei trattamenti ai principi di *privacy by design e by default*.

La certificazione di un trattamento svolto da parte di un Titolare o di un Responsabile, ai sensi dell'articolo 42 del RGPD, costituisce, all'occorrenza, un elemento di valutazione della conformità dello stesso con il RGPD, con particolare riferimento ai principi di *privacy by design e by default*, anche da parte dell'Autorità.

Qualora il Titolare voglia avviare una procedura di certificazione può utilizzare, ai fini del conseguimento della stessa, la documentazione *privacy* che dimostra l'applicazione dei principi di *privacy by design e by default* ai trattamenti di competenza.

Anche qualora un trattamento sia certificato ai sensi dell'articolo 42, il Titolare è comunque tenuto a garantire il monitoraggio costante e il miglioramento della conformità ai criteri della *privacy by design e by default* di cui all'articolo 25.

5. *PRIVACY BY DESIGN E BY DEFAULT* NEI TRATTAMENTI BASATI SU SISTEMI DI INTELLIGENZA ARTIFICIALE.

Il Titolare, in coerenza con la normativa europea in tema di intelligenza artificiale[5], è tenuto all'applicazione della presente *policy* anche qualora provveda ad automatizzare le proprie attività ricorrendo a sistemi che utilizzano tecnologie di Intelligenza Artificiale, nella misura in cui comportino il trattamento di dati personali; sia per i trattamenti eseguiti dal Titolare stesso che per quelli eseguiti da un Responsabile del trattamento per suo conto.

Pertanto, tutte le volte in cui un processo algoritmico di Intelligenza Artificiale coinvolga dati personali il Titolare del trattamento ha l'obbligo di conformarsi e di essere in grado di comprovare il rispetto dei principi e degli adempimenti previsti dal RGPD nonché di aver effettivamente tutelato il diritto alla protezione dei dati personali degli interessati fin dalla progettazione *(privacy by design)* e per impostazione predefinita *(privacy by default)* (artt. 5, 24 e 25, par. 1, del RGPD).

Tenuto conto dell'art. 22 del RGPD che sancisce il generale diritto dell'interessato a non essere soggetto ad una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, quando ciò può produrre effetti giuridici che lo riguardano o incidere in modo significativo sulla sua persona, l'applicazione dei principi di *privacy by design e by default* nei trattamenti di dati personali basati sull'utilizzo di sistemi di Intelligenza Artificiale determina in capo al Titolare del trattamento i seguenti obblighi:

- verificare che il trattamento, in un contesto di interesse pubblico quale quello che
- contraddistingue la Regione, sia specificamente previsto da una base giuridica nel diritto nazionale che assicuri il rispetto dei diritti e delle libertà degli interessati;
- informare gli interessati che il trattamento dei dati personali avviene attraverso algoritmi, fornendo informazioni significative sulla logica utilizzata, sì da poterla comprendere (principio di conoscibilità);
- assicurare sempre la possibilità di un intervento umano al fine di garantire l'individuazione di eventuali distorsioni dei processi automatizzati e di assicurare all'interessato di poter esprimere la propria opinione, nonché di contestare eventuali decisioni generate dal sistema (principio di non esclusività della decisione algoritmica);

[5] Il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024 (AI Act), entrato in vigore il 1° agosto 2024, all'art. 3, n. 1), definisce un «sistema di IA» quale *"un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali"*. L'AI Act inoltre fa espressamente salve le discipline di protezione dei dati personali (cfr. Considerando n. 10 e art. 2, par. 7).

- verificare l’imparzialità degli algoritmi utilizzati in modo che gli stessi siano conformi alle finalità del trattamento e imparziali rispetto alle stesse (principio di non discriminazione algoritmica);
- effettuare una attenta valutazione di impatto (DPIA) sui diritti e le libertà degli interessati ai sensi degli artt. 35-36 del RGPD;
- adottare misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati fin dalla progettazione e per impostazione predefinita;
- verificare costantemente che le misure adottate ai fini della tutela dei diritti e delle libertà dell'interessato siano adeguate ed efficaci anche nel tempo prevedendo periodiche verifiche e revisioni.

6. CONSEGUENZE DELLA NON CONFORMITA’ DEL TRATTAMENTO AI PRINCIPI DI *PRIVACY BY DESIGN E BY DEFAULT*

Nelle procedure indicate all’articolo 58 RGPD, la non conformità dei trattamenti all’art. 25 RGPD, può costituire per l’Autorità’ di controllo elemento di valutazione nell’esercizio dei poteri correttivi e sanzionatori ad essa attribuiti che, ai sensi dell’art. 58, par. 2, RGPD possono comprendere avvertimenti, ammonimenti, ingiunzioni di conformarsi ai diritti degli interessati, limitazioni o divieti di trattamento nonché sanzioni amministrative pecuniarie.

L’applicazione dei principi di *privacy by design e by default*, inoltre, ai sensi dell’art. 83 RGPD, rileva anche come elemento di determinazione, da parte dell’Autorità, dell’ammontare delle sanzioni pecuniarie per le violazioni del RGPD.

ALLEGATO QQ

DATA PROTECION IMPACT ASSESSMENT (DPIA) POLICY

Sommario

1. PREMESSA..... 41
2.AMBITO DI APPLICAZIONE..... 41
3.ABBREVIAZIONI E ACRONIMI 41
4.DEFINIZIONI..... 41
5.RIFERIMENTI NORMATIVI..... 43
6.*DPIA E PRINCIPIO DI *PRIVACY BY DESIGN E BY DEFAULT 43
7.INDIVIDUAZIONE DEI CRITERI PER L'ESECUZIONE DELLA DPIA 44
8.CONTENUTI OBBLIGATORI DELLA DPIA..... 47
9.DPIA SU PRODOTTI/SERVIZI CON L'USO DI NUOVE TECNOLOGIE47
10.CONSULTAZIONE PREVENTIVA CON L'AUTORITÀ GARANTE 47

1. PREMESSA

Il Regolamento (UE) 679/2016 (di seguito "RGPD") ha introdotto nuove regole in tema di protezione dei dati personali che prevedono, tra l'altro, la necessità che il Titolare del trattamento sin dal momento di determinare i mezzi del trattamento e per tutta la durata dello stesso, metta in atto misure tecniche e organizzative finalizzate ad attuare in modo efficace i principi di protezione dei dati e adotti garanzie adeguate a soddisfare i principi del RGPD e a tutelare i diritti degli interessati.

Lo scopo principale della presente *policy*, in ossequio al principio di *Privacy by design e by default*, (di seguito "PBDD") stabilito dall'articolo 25 del RGPD, è quello di descrivere le modalità di esecuzione della valutazione d'impatto sulla protezione dei dati (c.d. *Data protection Impact Assessment* di seguito "DPIA") ai sensi dell'art. 35 RGPD.

2. AMBITO DI APPLICAZIONE

La presente *policy* si applica alla Giunta regionale del Lazio (di seguito "Giunta" o "Titolare") in qualità di Titolare del trattamento secondo le responsabilità e i ruoli definiti nel modello organizzativo regionale in materia di protezione dei dati personali di cui al Titolo IX, Capo V del Regolamento Regionale n.1/2002 e successive modifiche e integrazioni.

Il Titolare, in conformità al principio di responsabilizzazione di cui all'art. 5, par. 2, RGPD ("*Accountability*") e al principio di Privacy *by design e by default* di cui all'art. 25 RGPD, in presenza di un rischio elevato per gli interessati e in tutti gli altri casi previsti dall'art. 35 del RGPD, è tenuta, prima dell'inizio delle attività del trattamento, ad eseguire una DPIA.

3. ABBREVIAZIONI E ACRONIMI

- **RGPD*:*** *Reg. UE 2016/679 "Regolamento generale sulla protezione dei dati" (anche GDPR "General Data Protection Regulation");*
- **WP29*:*** *Working Party Article 29 (Gruppo Articolo 29).*

4. DEFINIZIONI

Di seguito si riportano le definizioni dei principali termini utilizzati.

TERMINE	DESCRIZIONE
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 (Art. 4 par. 1 RGPD);
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, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (Art. 4 par. 2 RGPD);*
Interessato	*La persona fisica alla quale i dati personali si riferiscono (vedasi la definizione di Dato Personale);*
Titolare del trattamento	*La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; 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 (Art. 4 par. 7 RGPD). Ai fini della presente Policy il Titolare è la Giunta Regionale del Lazio.*
SDC - Soggetto Designato Competente	*Il Soggetto designato dal Titolare del Trattamento ai sensi degli artt. 474 e 474 ter del RR 1/2002 cui compete il trattamento.*
SDP - Soggetto designato competente in materia di protezione dei dati personali	*Il soggetto designato dal Titolare del Trattamento ai sensi degli artt. 474 e 474 ter del RR 1/2002, competente in materia di protezione dei dati personali.*
DPO (*Data Protection Officer*)	*Soggetto incaricato dal Titolare o dal Responsabile del trattamento per assolvere a funzioni di supporto e di controllo, consultive, di attribuzione di responsabilità e sensibilizzazione, formative e informative relativamente all'applicazione del RGPD (Art. 37 RGPD).*
Principio di protezione dei dati fin dalla progettazione (*privacy by design*)	*Il principio prevede la tutela dei dati personali in fase di progettazione del trattamento attraverso l'adozione di misure tecniche e organizzative adeguate. In tale contesto rilevano parametri quali, la minimizzazione, la pseudonimizzazione dei dati, ovvero tutte le altre misure idonee a ridurre i rischi (Art. 25 par. 1 del RGPD);*
Principio di protezione dei dati per impostazione predefinita (*privacy by default*)	*Il principio prevede, che per impostazione predefinita, il titolare dovrebbe trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. (Art. 25 par. 2 del RGPD);*
Registro dei trattamenti	*Documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del RGPD) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento. Il registro deve avere forma*

	scritta, anche elettronica, e deve essere esibito su richiesta al Garante.
***Data protection Impact Assessment* o DPIA (Valutazione d'impatto sulla protezione dei dati)**	*Procedura prevista dall'articolo 35 del RGPD che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli. Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi. Lo scopo della DPIA è quello di dimostrare che il Titolare abbia messo in atto le misure adeguate nell'esecuzione di un trattamento (Art. 35 RGPD);*
Pseudonimizzazione	*Comporta il trattamento dei dati personali in modo tale che gli stessi dati non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile (Art. 4 par. 5 del RGPD);*
Anonimizzazione	*Tecnica che viene applicata ai dati personali in modo tale che le persone fisiche interessate non possano più essere identificate in alcun modo;*
Finalità del trattamento	*Il principio prevede che i dati personali debbano essere "raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità" (art. 5 par. 1 lett. b) del RGPD).*

Per quanto non espressamente previsto nel presente paragrafo si applicano le definizioni di cui all'art. 4 del RGPD.

5. RIFERIMENTI NORMATIVI

La presente *policy* tiene conto delle seguenti disposizioni nazionali e europee, linee guida e provvedimenti del Garante:

- Regolamento (UE) 2016/679 (di seguito "RGPD");
- D.lgs. 196/2003 (di seguito "Codice in materia di protezione dei dati personali" oppure, per semplicità, "Codice Privacy");
- Linee Guida del Comitato Europeo per la Protezione dei Dati - *European Data Protection Board* "EDPB" - n. 4/2019 concernenti la Data Protection by Design and by Default, ai sensi dell'art. 25 del regolamento 2016/679;
- Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, WP 248 rev. 01, 4 ottobre 2017; Provvedimento del Garante "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679", 11 ottobre 2018 – Allegato 1.

6. DPIA E PRINCIPIO DI *PRIVACY BY DESIGN E BY DEFAULT*

Ai fini dell'applicazione pratica dei principi di PBDD di cui all'art. 25 del RGPD, l'implementazione di misure tecniche e organizzative che garantiscono l'attuazione dei principi generali, è subordinata ad una valutazione del rischio sulle attività di trattamento da parte del Titolare ai sensi dell'art. 32 RGPD nonché ad una valutazione di impatto (DPIA) ai sensi dell'art. 35 RGPD qualora dagli esiti della valutazione del rischio risulti ancora un rischio elevato per i diritti e le libertà degli interessati.

Il principio della protezione dei dati fin dalla progettazione (*privacy by design*) di cui all'art. 25 par. 1 RGPD, prevede l'obbligo per il Titolare, fin dalla progettazione del trattamento, di prevedere *l'attuazione delle misure tecniche e organizzative adeguate* ai fini della conformità ai principi di protezione dei dati e della tutela dei diritti e delle libertà degli interessati.

In particolare, l'attuazione delle misure tecniche e organizzative deve essere concepita *in funzione dell'efficace attuazione dei principi applicabili al trattamento dei dati personali* di cui all'art. 5 RGPD.

In assenza di un'adeguata applicazione del principio di protezione dei dati sin dalla progettazione il trattamento non può essere effettuato.

Il principio di protezione dei dati per impostazione predefinita (*privacy by default*), di cui all'art. 25, par. 2, del RGPD prevede inoltre che il Titolare attui le misure tecniche e organizzative adeguate a garantire che nelle attività di trattamento siano trattati solo i dati personali necessari e sufficienti alle finalità previste e per il periodo strettamente necessario al raggiungimento di tale finalità.

Anche le soluzioni tecniche adottate dal Titolare devono perseguire di *default* la tutela e la protezione dei dati personali.

7. INDIVIDUAZIONE DEI CRITERI PER L'ESECUZIONE DELLA DPIA

Per ogni nuovo trattamento/progetto/servizio o modifica ad uno già esistente, fin dalle prime fasi della progettazione (*by design*) deve essere effettuata da parte del Titolare una valutazione finalizzata a verificare i potenziali rischi per la sicurezza dei dati tenuto conto dello stato dell'arte e dei costi d'attuazione nonché della natura dei dati (cfr. anche Considerando 83 RGPD).

Si individuano nella tabella che segue i soggetti coinvolti:

R	A	C	I
SDC	SDC	-	-

R=Esecutore A=Responsabile C=Coinvolto I=Informato

Nell'effettuare la valutazione dei rischi di cui all'art. 32 RGPD, il SDC deve considerare in special modo i rischi presentati dal trattamento che derivano da:

- distruzione accidentale o illegale,
- perdita,
- modifica,
- rivelazioni o accesso non autorizzati,
- divulgazione non autorizzata a dati personali trasmessi, conservati o comunque trattati.

Al termine di tale analisi, qualora il trattamento presenti, comunque, un rischio elevato per i diritti e le libertà delle persone fisiche, prima di dare avvio al trattamento compete al SDC l'esecuzione di una DPIA.
Si individuano nella tabella che segue i soggetti coinvolti:

R	A	C	I
SDC	SDC	DPO*	DPO SDP

R=Esecutore A=Responsabile C=Coinvolto I=Informato

* coinvolgimento eventuale a discrezione del SDC.

Compete al SDC l'esecuzione della DPIA anche qualora il trattamento rientri in uno dei casi contemplati dall'art. 35 Par. 3 del RGPD:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati;
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
Le casistiche sopra richiamate costituiscono un elenco di alto livello dei criteri che richiedono che il trattamento sia sottoposto ad una valutazione d'impatto, alle quali si aggiungono quelle previste nelle *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*, WP 248 rev. 01 del 4 ottobre 2017, e quelle previste nel Provvedimento del Garante *"Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679"*, 11 ottobre 2018 – Allegato 1.
Le Linee guida sopra richiamate individuano ulteriori nove criteri utili per l'identificazione dei trattamenti per i quali il Titolare è tenuto a svolgere una DPIA:

1. valutazione o attribuzione di un punteggio all'interessato;
2. trattamenti basati su decisioni automatizzate (es. tracciamento dei comportamenti online);
3. monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico";
4. trattamento di dati sensibili o dati aventi carattere altamente personale (Artt. 9-10 RGPD);
5. trattamento di dati personali su larga scala;
6. confronto di basi di dati (es. machine learning utilizzato per la trascrizione di parole o il funzionamento di assistenti digitali);
7. trattamento di dati relativi a soggetti vulnerabili (es. minori, migranti, o in genere soggetti che si trovano in condizioni di sudditanza psicologica o di altro tipo rispetto al Titolare);
8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative;
9. il trattamento impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Laddove siano presenti almeno due dei criteri succitati il trattamento deve essere oggetto di una DPIA.

È facoltà del SDC anche nel caso in cui un trattamento risponda soltanto ad uno dei criteri sopra richiamati procedere comunque all'esecuzione di una DPIA.
Il Provvedimento del Garante sopra richiamato, ai sensi dell'art. 35 par. 4 del RGPD, prevede un ulteriore elenco di (dodici) tipologie di trattamenti da sottoporre alla valutazione d'impatto:

1. trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app;
2. trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato;
3. trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc.
4. trattamenti su larga scala di dati aventi carattere estremamente personale: si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
5. trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione);
6. trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, pazienti, richiedenti asilo ecc.);
7. trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.
8. trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;
9. trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment);
10. trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse;
11. trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12. trattamenti di dati genetici tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Qualora un trattamento rientri in almeno una delle tipologie previste nel Provvedimento del Garante il trattamento stesso deve essere oggetto di una DPIA.
Il SDC, quando il trattamento presenta le caratteristiche di seguito indicate può non procedere all'esecuzione della DPIA:

- il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1);
- la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati;
- le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;
- un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10);
- il trattamento è incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5) qualora adottato dal Garante nazionale.

Ai sensi dell'art. 474 ter il SDC all'esito della DPIA, laddove ritenga opportuno richiedere il parere di cui all'art. 474 septies del Regolamento regionale, trasmette la stessa al DPO.

8. CONTENUTI OBBLIGATORI DELLA DPIA

Tenuto conto di quanto stabilito all'art 35 par. 7 RGPD, si definiscono di seguito i contenuti obbligatori della valutazione di impatto:
- una descrizione sistematica del trattamento;
- una valutazione della necessità e della proporzionalità del trattamento in cui sono esplicitate e giustificate le modalità con cui viene garantita la liceità del trattamento, in termini di:
- indicazione delle finalità: devono essere definite le finalità specificate esplicite e legittime;
- minimizzazione dei dati: deve essere limitata la quantità dei dati personali trattati a ciò che risulti strettamente necessario ai fini dell'esecuzione del trattamento;
- limitazione della conservazione: deve essere definito il periodo di conservazione necessario per raggiungere le finalità indicate.
- l'indicazione delle misure previste per affrontare i rischi incluse le garanzie per assicurare la protezione dei dati personali e la dimostrazione della conformità al RGPD tenuto conto anche delle modalità di gestione dei diritti dell'interessato.
  Nel rispetto del principio di PBDD, il Titolare del trattamento procede a un riesame periodico del trattamento dei dati personali al fine di valutare che lo stesso sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati. È fatto comunque obbligo al Titolare di procedere all'aggiornamento della DPIA ogniqualvolta insorgono variazioni del rischio delle attività di trattamento.

9. DPIA SU PRODOTTI/SERVIZI CON L'USO DI NUOVE TECNOLOGIE.

L'obbligo di svolgere la valutazione d'impatto (DPIA) è in capo al Titolare del trattamento; tuttavia, nel caso in cui la Giunta Regionale del Lazio, nel suo ruolo *privacy* di Titolare, stabilisca che il trattamento sia effettuato per suo conto da un fornitore di servizi, prodotti e applicazioni,

Responsabile del trattamento, potrà richiedere di essere assistito da quest'ultimo in conformità al relativo contratto sottoscritto tra le parti e nel rispetto specifico dell'art. 28, par. 3, lett. f), del RGPD.
Qualora il trattamento preveda l'utilizzo di servizi e prodotti con l'uso di nuove tecnologie da parte di Fornitori-Responsabili del trattamento è necessario che il Titolare, fermo l'obbligo dello stesso di svolgere una propria specifica DPIA, acquisisca dal fornitore, quale requisito di accesso alla fase di selezione del contraente, una valutazione di impatto sulla protezione dei dati sul prodotto/servizio da acquistare.

10. CONSULTAZIONE PREVENTIVA CON L'AUTORITÀ GARANTE

Nel caso in cui la Valutazione d'impatto evidenzi un "Rischio elevato residuale", il Soggetto Designato competente (SDC), qualora intenda comunque procedere al trattamento, sentito il DPO, avvia la Consultazione Preventiva con l'Autorità di controllo ai sensi dell'art 36 par. 1 del RGPD.
Si individuano nella tabella che segue i soggetti coinvolti:

R	A	C	I
SDC	SDC	DPO	DPO SDP

R=Esecutore A=Responsabile C=Coinvolto I=Informato

È competenza del SDC, sentito il DPO, redigere l'istanza di consultazione preventiva ai sensi dell'art. 36 par. 3 del RGPD, contenente i seguenti elementi:

- le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento;
- le finalità e i mezzi del trattamento previsto;
- le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del RGPD;
- i dati di contatto del responsabile della protezione dei dati (DPO);
- la valutazione d'impatto sulla protezione dei dati (DPIA) effettuata;
- ogni altra informazione richiesta dall'Autorità di controllo.

L'art. 36, par. 2, del RGPD stabilisce che l'Autorità di controllo, se ritiene che il trattamento previsto non sia conforme al RGPD o che il Titolare non abbia identificato o attenuato sufficientemente il rischio, entro un periodo massimo di otto settimane dalla richiesta di consultazione, fornisce un parere scritto. Questo periodo può essere prorogato di ulteriori sei settimane, tenendo conto della complessità del trattamento previsto. Qualora si applichi la proroga, il Titolare e, ove applicabile, il responsabile del trattamento ne sono informati unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta. Tali periodi possono essere sospesi fino all'ottenimento da parte dell'Autorità di controllo delle informazioni eventualmente richieste ai fini della consultazione.
È inoltre prevista la consultazione del Garante nella casistica dell'art. 36 par. 4 RGPD o nel caso in cui la normativa prescriva che il titolare del trattamento consulti l'autorità di controllo, e ne ottenga l'autorizzazione preliminare, in relazione al trattamento per l'esecuzione di un compito di interesse

pubblico, tra cui rientrano i trattamenti con riguardo alla protezione sociale e alla sanità pubblica (art. 36 par. 4 RGPD).
All'esito della valutazione da parte dell'Autorità Garante e della trasmissione del parere scritto nei termini di cui al par. 2 dell'art. 36 del RGPD, il SDC coadiuvato dal DPO, individua e mette in atto le misure e le azioni necessarie per l'adeguamento alle prescrizioni impartite.".

ALLEGATO RR

Policy per la gestione delle ispezioni da parte del Garante per la protezione dei dati personali

Sommario

1. INTRODUZIONE 50
1.1Scopo ed obiettivi 50
1.2Ambito di applicazione 50
2.DEFINIZIONI 51
3.QUADRO NORMATIVO DI RIFERIMENTO 52
3.1Riferimenti normativi e regolamentari 52
4.TEAM PER LA GESTIONE DELLE ISPEZIONI 53
5.LA GESTIONE DELLE ISPEZIONI 53
5.1Le Ispezioni del Garante 53
5.2Indicazioni di carattere generale relative alle Ispezioni in loco 54
5.3Il ruolo del DPO nella gestione della Ispezioni 54
6.PROCESSO PER LA GESTIONE DELLE ISPEZIONI 55
6.1Processo 55
6.1.1Analisi della richiesta e coinvolgimento dei soggetti competenti 55
6.1.2Predisposizione contributi per rispondere alla richiesta 55
6.1.3Predisposizione e formalizzazione della risposta 55
7.DOCUMENTAZIONE RILEVANTE 56
8.CONSEGUENZE DELLE ISPEZIONI 57
8.1 Ricorso giustizia ordinaria avverso il provvedimento del garante 57
8.2 Azioni successive 59

1. INTRODUZIONE

Il 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* (GDPR) prevede che tutti i titolari del trattamento sono tenuti a mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente allo stesso Regolamento (art. 24, par. 1, GDPR).
Il Regolamento contempla tra i principi applicabili alla protezione dei dati personali anche l'*accountability* (responsabilizzazione) dei titolari e responsabili del trattamento (art. 5, par. 1, GDPR), consistente nell'adozione di comportamenti proattivi, tali da provare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.
In conformità al predetto principio è attribuita al Titolare la "responsabilità generale" del trattamento e l'attuazione di un sistema organizzativo e gestionale che preveda misure reali, efficaci e comprovabili di protezione dei dati (v. Cons. 74 e artt. 5, par. 2, e 24 del GDPR).
Tale approccio implica, oltre alla corretta e puntuale predisposizione degli adempimenti imposti dalla normativa in tema di protezione dei dati, anche l'implementazione di procedure e prassi organizzative atte a conformare i trattamenti al GDPR.
Il Regolamento contempla altresì l'obbligo generale di cooperazione con l'Autorità di controllo da parte del Titolare e responsabile del trattamento (art. 31 e Cons. 82 del GDPR).
La presente policy descrive le procedure relative alla gestione delle ispezioni del Garante per la protezione dei dati personali.
Nell'esercizio dei suoi compiti di controllo il Garante per la protezione dei dati personali (di seguito anche "Autorità" o "Garante"), valutati gli elementi in suo possesso, anche in assenza di reclami, segnalazioni o notificazioni di violazione dei dati personali, può avviare d'ufficio accertamenti per verificare la sussistenza di elementi in ordine a possibili violazioni in materia di protezione dei dati personali.
L'attività ispettiva può essere curata dal dipartimento, servizio o altra unità organizzativa del Garante competente in materia di attività ispettive e di revisione ovvero delegata alla Guardia di Finanza. La stessa può essere altresì effettuata avvalendosi, ove necessario, della collaborazione di altri organi dello Stato.
La programmazione dell'attività ispettiva di iniziativa viene approvata dal Garante su base semestrale con propria deliberazione.
Gli accertamenti, di seguito anche "Ispezioni", possono verificarsi in due modalità:

- istruttoria cartolare;
- accesso ai locali.

1.1 Scopo ed obiettivi

La presente policy descrive le modalità e le fasi per gestire gli eventuali accertamenti ispettivi da parte del Garante per la protezione dei dati personali da parte della Giunta regionale del Lazio (di seguito "Giunta" o "Titolare"), nella sua qualità di Titolare o, quando ricorra la fattispecie, di Responsabile del trattamento, ai sensi del GDPR e del D. Lgs. 196/2003 e ss.mm.ii. (di seguito "Codice in materia di protezione dei dati personali" o anche solo "Codice").

1.2 Ambito di applicazione

La presente Policy si applica alla Giunta e al suo personale, secondo le responsabilità e i ruoli previsti all'interno del modello organizzativo per la protezione dei dati personali di cui al Titolo IX, Capo V del Regolamento Regionale n.1/2002 e successive modifiche.

2.DEFINIZIONI

Di seguito si riportano le definizioni dei termini utilizzati nella presente Policy.

TERMINE	DESCRIZIONE
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 (art. 4 par. 1 GDPR).*
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, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art 4 par. 2 GDPR).*
Interessato	*La persona fisica alla quale i dati personali si riferiscono (vedasi la definizione di Dato Personale).*
Titolare del trattamento	*La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; 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 (art 4 par. 7 RGDP).*
Responsabile del trattamento	*La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento (art 4 par. 8 GDPR).*
Contitolari del trattamento	*La contitolarità si verifica quando due o più soggetti definiscono congiuntamente le finalità e i mezzi del trattamento (art. 26 GDPR).*
Autorizzato al trattamento	*La persona fisica che effettua materialmente le operazioni di trattamento sui dati personali e che opera alle dipendenze del Titolare e/o del Responsabile (art. 29 GDPR e art. 2 quaterdecies del Codice).*
DPO (*Data Protection Officer*)	*Soggetto incaricato dal Titolare o dal Responsabile del trattamento per assolvere a funzioni di supporto e di controllo, consultive, formative e informative, di attribuzione delle responsabilità relativamente all'applicazione del GDPR (Art. 37 GDPR).*

TERMINE	DESCRIZIONE
Categorie particolari di dati personali	*Dati personali che possono rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (Art. 9 GDPR).*
Misure di sicurezza	*Le misure tecniche e organizzative predisposte dal Titolare o dal Responsabile di trattamento ai sensi dell'Art. 32 GDPR.*
Amministratori di sistema	*Figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti ai sensi del Provvedimento del Garante della Privacy del 27 novembre 2008 recante prescrizioni ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema.*
Registro dei trattamenti	*E'un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del GDPR) relative alle operazioni di trattamento svolte dal Titolare e, se nominato, dal responsabile del trattamento. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.*
DPIA (*Data protection Impact Assessment*)	*È una procedura prevista dall'articolo 35 del GDPR che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli. Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.*

3. QUADRO NORMATIVO DI RIFERIMENTO

3.1 Riferimenti normativi e regolamentari

La presente Policy tiene conto delle disposizioni contenute nelle seguenti norme nazionali ed europee:

- Regolamento (UE) 2016/679 in materia di protezione dei dati personali, (in breve "RGPD", meglio conosciuto con l'acronimo inglese "GDPR";
- D.lgs. n. 196/2003 ("Codice in materia di protezione dei dati personali");

in particolare:

- Art. 58 del GDPR "Poteri";
- Art. 83 del GDPR "Condizioni generali per infliggere sanzioni amministrative pecuniarie";
- Considerando 122, 129 e 132 del GDPR;
- Parte III, Titolo II, Capo III del Codice in materia di protezione dei dati personali;
- Art. 157 del Codice "Richiesta di informazioni e di esibizione dei documenti";
- Art. 158 del Codice "Accertamenti";
- Art. 31 GDPR "Cooperazione con l'Autorità di Controllo".

e nei seguenti ulteriori atti e regolamenti:

- Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali approvato con Deliberazione del 4 aprile 2019 del Garante;
- Programmazione dell'attività ispettiva di iniziativa, curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, approvata su base semestrale con deliberazione dell'Autorità;
- Regolamento 1/2000 concernente l'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali.

4. TEAM PER LA GESTIONE DELLE ISPEZIONI

Per far fronte alle ispezioni da parte dell'Autorità la Giunta, in qualità di Titolare del Trattamento, opera per il tramite di un apposito Team preposto all'assistenza dell'attività ispettiva, costituito come segue:

Codice	Attore
SDC	Soggetto Designato competente nelle materie oggetto dell'attività ispettiva.
SDP	Soggetto Designato competente in materia di dati personali
DG	Direttore Generale
DPO	DPO
AR	Avvocatura regionale

5. LA GESTIONE DELLE ISPEZIONI

5.1 Le Ispezioni del Garante

Le Ispezioni del Garante sono volte a verificare che le attività di trattamento dei dati personali di una determinata organizzazione siano conformi alla normativa vigente in ambito protezione dei dati personali. Le Ispezioni possono scaturire da segnalazioni o reclami da parte degli Interessati, oppure su iniziativa del Garante sulla base dell'attività ispettiva programmata su base semestrale con propria deliberazione.

Le Ispezioni possono distinguersi secondo le seguenti tipologie:

1. **Ispezioni tramite istruttoria cartolare** nell'ambito delle quali il Garante può richiedere al Titolare e/o Responsabile di fornire ogni informazione necessaria per l'esecuzione dei suoi compiti (art. 58 par. 1 lett. a) GDPR). L'istruttoria cartolare può precedere anche l'ispezione tramite accesso ai locali.
2. **Ispezioni tramite accesso presso i locali del Titolare e/o Responsabile** (Art. 58 par. 1 lett. f) GDPR). L'ispezione presso i locali può avvenire:

- con preavviso tramite una comunicazione via PEC (posta elettronica certificata) o residualmente via raccomandata A/R, anche il giorno prima dell'arrivo dei soggetti preposti all'ispezione;
- senza preavviso.

Il perimetro dell'Ispezione è individuato all'interno del documento che viene notificato dall'Autorità tramite PEC, in caso di istruttoria cartolare, o al momento dell'accesso nei locali della Giunta, in caso di Ispezione presso i locali.

La supervisione semestrale del piano ispettivo dell'Autorità, finalizzata alla conoscenza degli argomenti sui quali il Garante programma la propria attività ispettiva e la sua divulgazione a tutte

le strutture regionali, è demandata alla Direzione Regionale competente in materia di protezione dei dati personali per il tramite del Direttore *pro tempore* nella qualità di soggetto designato.
Di seguito sono descritte le modalità di gestione delle Ispezioni.

5.2 Indicazioni di carattere generale relative alle Ispezioni in loco

Ai fini del buon esito delle Ispezioni, la Giunta opera per mezzo del Team di cui al precedente par. 4; il SDC competente nelle materie e nei trattamenti oggetto dell'ispezione, per tutta la durata dell'Ispezione stessa coordina le attività e costituisce il punto di riferimento per le strutture regionali coinvolte e per gli ispettori.
Durante l'attività ispettiva il SDC può farsi assistere da consulenti di propria fiducia e riservarsi di produrre la documentazione non immediatamente reperibile entro un termine congruo.
Gli Ispettori raccolgono presso il SDC tutta la documentazione relativa al perimetro ispettivo stabilito, nonché l'ulteriore documentazione utile ai fini della dimostrazione della *compliance* alla normativa in materia di protezione dati personali da parte dello stesso.
In particolare, il personale ispettivo può:

- richiedere informazioni o spiegazioni;
- accedere alle banche dati e agli archivi;
- controllare, estrarre ed acquisire copia dei documenti, anche in formato elettronico.

Per una più dettagliata identificazione della documentazione che può essere richiesta e sottoposta a controllo durante l'Ispezione si rinvia al paragrafo 7 della presente Policy.
Della veridicità delle dichiarazioni rese dal Titolare del trattamento, e dal suo personale autorizzato, nel corso dell'istruttoria, si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice Privacy.
Al termine di ciascuna giornata di ispezione, il SDC si assicura di far registrare nel verbale di ispezione dell'Autorità le proprie considerazioni o dichiarazioni in particolare se in contrasto con le valutazioni emerse durante l'attività ispettiva da parte del Garante.
Il SDP redige un report interno per documentare le attività svolte e ove possibile quelle programmate per la giornata successiva, allegando copia del verbale delle Autorità. Il report ha lo scopo di tenere traccia degli uffici visitati, dei dipendenti interrogati e dei documenti consegnati durante l'ispezione, in modo da poter ricostruire accuratamente i dettagli delle Ispezioni.

5.3 **Il ruolo del DPO nella gestione della Ispezioni**

Tra i compiti del DPO, ai sensi dell'art. 39 del GDPR, vi è quello di "cooperare con l'autorità di controllo" e "fungere da punto di contatto con l'autorità ". Inoltre, l'articolo 38 del GDPR prevede che "*il Titolare del trattamento e il responsabile del trattamento assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*".

Il DPO assiste il Titolare durante le ispezioni. In particolare, ne presidia tutte le fasi e funge da punto di contatto per facilitare l'accesso, da parte dell'Autorità Garante, ai documenti e alle informazioni necessarie per l'adempimento dei compiti ad essa attribuiti dall'art. 57, nonché ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all'art. 58 del GDPR.

6. PROCESSO PER LA GESTIONE DELLE ISPEZIONI

L'accesso ai locali della Giunta da parte del personale incaricato dall'Autorità, nonché la comunicazione dell'Autorità della visita ispettiva in loco o di istruttoria cartolare, sono immediatamente comunicate al SDP, il quale procede ad informare il DPO e a convocare il Team come sopra costituito.

6.1 Processo

6.1.1 Analisi della richiesta e coinvolgimento dei soggetti competenti

R	A	C	I
SDP	SDP	TEAM	TEAM

R=Esecutore A=Responsabile C=Coinvolto I=Informato

Sia in caso di istruttoria cartolare che in caso di Ispezione in loco, il SDP, in primo luogo provvede a informare il DPO il quale si occuperà di presidiare ogni fase del processo di Ispezione. In seguito, l'SDP prende visione del provvedimento ricevuto, ne esamina attentamente il contenuto e attiva tempestivamente il Team coinvolto nella gestione dell'Ispezione. Qualora le materie oggetto di Ispezione riguardino le competenze di più Soggetti Designati, il DG nomina il SDC di riferimento. Il SDP, ove le verifiche riguardino i sistemi informativi, coinvolge il Responsabile del trattamento, il quale con l'atto di nomina si è impegnato ad adottare tutte le misure tecniche indicate dall'art. 32 del RGPD.

6.1.2 Predisposizione contributi per rispondere alla richiesta

R	A	C	I
SDC	SDC	SDP/AR	DPO/DG

R=Esecutore A=Responsabile C=Coinvolto I=Informato

Una volta attivato il Team, l'SDC raccoglie tutta la documentazione e le informazioni utili alla predisposizione dei riscontri al Garante.
Ai fini del riscontro nei termini stabiliti dall'Autorità, nelle ispezioni in loco, nonché nelle istruttorie cartolari il SDC predispone la documentazione richiesta; qualora ciò implichi di fornire l'accesso a documenti cartacei ed elettronici il SDC è supportato in particolare dal SDP e dall'AR.

6.1.3 Predisposizione e formalizzazione della risposta

R	A	C	I
SDC	SDC	SDP/AR/DPO	DG

R=Esecutore A=Responsabile C=Coinvolto I=Informato

Nell'istruttoria cartolare, il SDC, con il supporto del DPO, del SDP e dell'AR, informato il DG, formalizza la risposta e provvede all'invio nei termini stabiliti dall'Autorità.
Nell'Ispezione in loco, il SDC revisiona la lista dei documenti forniti, le minute, i commenti e le osservazioni sollevate durante l'attività ispettiva e nell'ipotesi di istruttorie particolarmente complesse o richieste di documentazione articolate o di particolare rilevanza può valutare,

coadiuvato dal DPO e dall'AR e dal SDP, la richiesta di un differimento dei termini all'Autorità, verificando all'occorrenza con gli stessi eventuali punti ancora da chiarire.

7. DOCUMENTAZIONE RILEVANTE

La tabella che segue evidenzia una serie di documenti utili a dimostrare la *compliance* con la normativa in materia di protezione dei dati personali, generalmente oggetto di richiesta da parte del Garante in caso di ispezione, nonché il rispetto del principio di *accountability*.

In considerazione del fatto che il GDPR prevede in tema di protezione e trattamento dei dati personali che le attività poste in essere siano adeguatamente documentate, la documentazione relativa a eventuali *Assessment* svolti in materia, deve essere conservata al fine di renderla disponibile per dimostrare la conformità delle attività di trattamento ai principi normativi vigenti in materia.

La conservazione, compatibilmente con le dotazioni in essere presso la Giunta, deve essere effettuata in un apposito *repository*.

Elenco documenti
Accordi sindacali e/o autorizzazioni della DTL (direzione territoriale del lavoro)
Regolamento Regionale CAPO V "*Trattamento dei dati personali e banche dati*" nell'ultima versione disponibile
Autorizzazione al trattamento del soggetto incaricato ai sensi dell'art. 29 del Regolamento 2016/679/UE e dell'art. 2 quaterdecies del D. lgs. 196/03 e istruzioni operative
Designazione di amministratore di sistema ai sensi del provvedimento del Garante per la protezione dei dati personali (G.U. n. 300 del 24/12/2008)
Nomina del DPO
Evidenze relative all'attività di formazione per i dipendenti
Designazione Responsabili del trattamento (DPA)
Documentazione di *assessment* Privacy (es. *checklist* GDPR)
Documentazione sui sistemi informatici utilizzati (verifiche/*assessment*)
Documentazione Videosorveglianza (es. accordo sindacale)
Valutazione del rischio delle attività di trattamento
DPIA svolte, complete, ove esistenti degli aggiornamenti
Elenco Amministratori di Sistema e relative nomine
Elenco eventuali contitolari e relativi accordi di contitolarità
Elenco responsabili/sub-responsabili del trattamento
Informative e modulistica standard
Misure di sicurezza adottate

Elenco documenti
Procedure specifiche in materia di protezione e trattamento dei dati personali (es. per esercizio diritti interessati)
Registro attività di trattamento tenuti in qualità di Titolare e/o Responsabile del trattamento
Data breach policy
Registro *data breach*
Repository di segnalazioni e reclami avvenuti
Lista delle richieste di esercizio dei diritti pervenute
Checklist di controllo e esiti audit sulle attività dei Responsabili

Con particolare riferimento alle Ispezioni in loco, il Team, secondo le competenze sopra individuate si assicura di:

- rilasciare sempre informazioni veritiere e corrette;
- non rilasciare mai documentazione in originale ma solo in copia;
- prendere nota, nel report giornaliero di cui al paragrafo 4.2, di tutti i documenti (inclusi anche banche dati, archivi, software) visionati dagli ispettori e delle informazioni richieste e fornite;
- farsi rilasciare copia del verbale di ispezione dell'Autorità.

Qualora il riscontro alle richieste degli Ispettori costituisca attività di particolare complessità, sia in ordine all'istruttoria, sia in ordine al reperimento della documentazione richiesta, il SDC, informati il DPO e il DG, potrebbe valutare la richiesta di differimento dei termini al Garante.

8. CONSEGUENZE DELLE ISPEZIONI

R	A	C	I
SDC	SDC	DPO/AR	DG/DPO/SDP

R=Esecutore A=Responsabile C=Coinvolto I=Informato

Alla luce delle risultanze ispettive, il Garante, valutata la sussistenza di eventi di particolare rilevanza, può irrogare le sanzioni pecuniarie di cui all'art. 83 GDPR e/o i provvedimenti correttivi di cui all'art. 58 paragrafo 2 del GDPR.
Entro trenta giorni dalla comunicazione il SDC, coadiuvato dal DPO e dall'Avvocatura Regionale, informato il DG, può esercitare il proprio diritto di difesa inviando scritti difensivi e deduzioni scritte e può chiedere, con specifica istanza debitamente motivata una breve proroga, di norma concessa per un termine non superiore a quindici giorni, anche tenendo conto delle caratteristiche operativo/dimensionali del Titolare.

8.1 Ricorso giustizia ordinaria avverso il provvedimento del garante

R	A	C	I
SDC	SDC	AR	DPO/DG/SDP

R=Esecutore A=Responsabile C=Coinvolto I=Informato

Ai sensi del combinato disposto degli artt. 78 del Regolamento e 152 del d.lgs 196/2003 è prevista la possibilità di presentare ricorso avverso le decisioni dell'Autorità Garante davanti al Giudice ordinario, il quale può rideterminare le sanzioni irrogate dalla stessa Autorità Garante.

Nel caso di emissione della sanzione da parte dell'Autorità, spetta al SDC coadiuvato dall'AR e informati il DG e il DPO, la facoltà di proporre ricorso avverso il provvedimento sanzionatorio emesso dall'Autorità Garante innanzi alle Autorità giurisdizionali competenti, ai sensi dell'art. 78 del GDPR.

Tali controversie sono regolate dal rito del lavoro e vengono decise dal Tribunale ordinario in composizione monocratica, con sentenza non appellabile ma ricorribile unicamente tramite ricorso per Cassazione.

Il ricorso avverso i provvedimenti dell'Autorità, ivi compresi quelli emessi a seguito di un reclamo dell'interessato, è proposto, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Il Regolamento ha previsto rilevanti sanzioni di natura amministrativa in caso di violazioni della normativa sulla protezione dei dati personali. L'art. 83 del Regolamento distingue due gruppi di sanzioni amministrative.

Nel primo gruppo rientrano le violazioni cosiddette di minore gravità, per le quali sono previste le sanzioni amministrative pecuniarie di importi fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, e comprendono, tra l'altro anche le violazioni degli obblighi imposti al Titolare e al Responsabile del trattamento (artt. 8, 11, da 25 a 39, 42 e 43 del GDPR).

Nel secondo gruppo rientrano le violazioni di maggiore gravità per le quali sono previste sanzioni pecuniarie fino all'ammontare di 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, e riguardano nello specifico le seguenti violazioni:

- dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9 del Regolamento;
- dei diritti degli interessati a norma degli articoli da 12 a 22 del Regolamento;
- delle norme relative ai trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli artt. da 44 a 49 del Regolamento;
- di qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX del GDPR;
- nonché l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'Autorità Garante ai sensi dell'art. 58, par. 2 del

Regolamento, o il negato accesso nella Società/Ente in violazione dell'art. 58, par. 1 del Regolamento.

Le sanzioni irrogate dall'Autorità devono essere effettive, proporzionate e dissuasive (art. 83, par. 1 del Regolamento) e devono tenere conto delle circostanze di cui all'art. 83, par. 2 del Regolamento, che contemplano anche il grado di cooperazione con l'Autorità al fine di porre rimedio alle rilevate violazioni; la modalità con cui il Titolare risponde alle richieste dell'Autorità durante le ispezioni, può costituire elemento di valutazione del grado di cooperazione con l'Autorità.

8.2 Azioni successive

All'esito del procedimento ispettivo, il SDC è tenuto a mettere in atto tutte le azioni correttive richieste dal provvedimento dell'Autorità, nonché ad adeguare la documentazione alle risultanze ispettive intervenendo sul sistema di protezione dati per apportare gli opportuni miglioramenti.
Tutta la documentazione relativa all'Ispezione, comprensiva del verbale di ispezione, dei report interni di cui al paragrafo 4.2 nonché degli interventi di adeguamento documentati sul sistema di protezione dati deve essere adeguatamente conservata, compatibilmente con le dotazioni in essere presso la Giunta, anche in un apposito *repository*.".

ALLEGATO SS (art. 28-ter)

Sistema di Contrasto al Riciclaggio ed al finanziamento del Terrorismo (SiCoRiTe)

Sommario

Introduzione 41
1. Ambito di applicazione, oggetto e finalità 43
2. Definizioni 44
3. Soggetti coinvolti 45
4. Attività 45
5. Supporti tecnologici 51
6. Banche-dati 52
7. Indicatori di anomalia 52
A. Indicatori di anomalia connessi con l'identità o il comportamento del soggetto cui è riferita l'operazione 53
B. Indicatori di anomalia connessi con le modalità (di richiesta o esecuzione) delle operazioni. 55
C. Indicatori specifici per settore di attività 56
1. Settore appalti e contratti pubblici 56
2) Settore finanziamenti pubblici 58
3) Settore immobili e commercio 58

Introduzione

In materia di contrasto ai fenomeni di riciclaggio e di finanziamento del terrorismo, gli *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, elaborati dal Gruppo d'Azione Finanziaria Internazionale (GAFI), specifico organismo intergovernativo istituito dal G7 alla fine degli anni '80, rappresentano i principi fondamentali che i Paesi aderenti sono chiamati a recepire nel contesto dei rispettivi ordinamenti. Sul piano comunitario la normativa europea recepisce l'evoluzione dei principi internazionali, in particolare, la Direttiva UE/2018/843 e la Direttiva UE/2015/849 definiscono il sistema di prevenzione degli Stati membri in coerenza con le linee tracciate dal GAFI, valorizzando l'approccio *risk-based* per la gradazione delle misure di prevenzione e controllo, confermando il ruolo centrale delle Financial

Intelligence Unit (FIU) con l'introduzione di obblighi specifici di "scambio automatico" *cross-border* di segnalazioni riguardanti operazioni[6]sospette di riciclaggio[7] o di finanziamento del terrorismo[8].

Il 24 aprile 2024 il Parlamento europeo ha adottato in via definitiva un pacchetto di leggi (c.d. "*AML Package*") pubblicato sulla Gazzetta Ufficiale dell'Unione europea del 19 giugno 2024, e che rafforza ed integra gli strumenti a disposizione dell'UE per combattere il riciclaggio di denaro e il finanziamento del terrorismo. Nell'ambito del pacchetto di norme, il 30 maggio 2024, il Consiglio europeo ha adottato un regolamento che istituisce una nuova Autorità per la lotta al riciclaggio (AMLA) al fine di migliorare la vigilanza in materia di AML/CFT nell'UE e sostenere la cooperazione tra le FIU. L'AMLA avrà sede a Francoforte e sarà operativa a partire dalla metà del 2025. Poiché il riciclaggio è un reato finanziario transfrontaliero, l'AMLA rafforzerà il quadro dell'UE in materia di AML/CFT creando un meccanismo integrato con supervisori nazionali negli Stati membri al fine di garantire che i soggetti obbligati rispettino i loro obblighi[9].

Il decreto legislativo 21 novembre 2007, n. 231 – come modificato dal decreto legislativo 25 maggio 2017, n. 90 e da ultimo dal decreto legislativo 4 ottobre 2019, n. 125 – costituisce la principale fonte normativa nazionale in materia di antiriciclaggio. Le disposizioni nazionali in materia di finanziamento del terrorismo trovano organica sistemazione nel decreto legislativo 22 giugno 2007, n. 109.

In linea generale, le disposizioni normative prevedono che una serie di operatori del settore finanziario e di settori correlati (intermediari bancari e finanziari, altri operatori finanziari, professionisti nell'esercizio della professione in forma individuale, associata o societaria, altri operatori non finanziari, prestatori di servizi di gioco, società di gestione accentrata di strumenti finanziari e di gestione dei mercati regolamentati di strumenti finanziari) altrimenti definiti, "soggetti obbligati", inviano all'Unità di informazione Finanziaria per l'Italia (UIF) una segnalazione di operazione sospetta quando *"sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa"*.

Per quanto concerne gli obblighi specifici per le Pubbliche Amministrazioni, l'articolo 10 del decreto legislativo 21 novembre 2007, n. 231 stabilisce che al fine di consentire lo svolgimento di analisi finanziarie mirate a far emergere fenomeni di riciclaggio e di finanziamento del terrorismo, le Pubbliche Amministrazioni comunicano alla UIF dati e informazioni concernenti le operazioni sospette di cui vengano a conoscenza nell'esercizio della propria attività istituzionale.

---

[6] Il decreto legislativo 21 novembre 2007, n. 231 intende per "operazione" l'attività consistente nella movimentazione, nel trasferimento o nella trasmissione di mezzi di pagamento o nel compimento di atti negoziali a contenuto patrimoniale; costituisce operazione anche la stipulazione di un atto negoziale, a contenuto patrimoniale, rientrante nell'esercizio dell'attività professionale o commerciale.

[7] Il decreto legislativo 21 novembre 2007, n. 231 intende per riciclaggio: a) la conversione o il trasferimento di beni, effettuati essendo a conoscenza che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni; b) l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; c) l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; d) la partecipazione ad uno degli atti di cui alle lettere a), b) e c) l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolarne l'esecuzione."

[8] Il decreto legislativo 21 novembre 2007, n. 231 intende per finanziamento del terrorismo qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione, in qualunque modo realizzate, di fondi e risorse economiche, direttamente o indirettamente, in tutto o in parte, utilizzabili per il compimento di una o più condotte, con finalità di terrorismo secondo quanto previsto dalle leggi penali ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette.

9 Nel dettaglio, l'AML package si compone in tre blocchi:

1) la VI direttiva antiriciclaggio (direttiva Ue 2024/1640 che entra in vigore ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale dell'Unione europea), che disciplina i meccanismi che gli Stati membri devono istituire per prevenire l'uso del sistema finanziario a fini di riciclaggio e finanziamento del terrorismo (modifica la direttiva Ue 2019/1937 e ridefinisce la direttiva Ue 2015/849). Tale norma contiene disposizioni, da recepire nel diritto nazionale, sulla vigilanza e sulle Unità di Informazione finanziaria negli Stati membri, nonché sull'accesso delle autorità competenti a informazioni necessarie e affidabili, come ad esempio registri dei titolari effettivi e beni custoditi nelle zone franche. In via generale, gli Stati membri mettono in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi a tale direttiva entro il 10 luglio 2027 con alcune eccezioni come, ad esempio, le modifiche attinenti al registro dei titolari effettivi da recepire e rendere operative entro il 10 luglio 2026; all'accesso unico alle informazioni sui beni immobili da recepire e rendere operative entro il 10 luglio 2029.
2) il regolamento "single rulebook" (regolamento Ue 2024/1624), contenente norme direttamente applicabili in materia di due diligence sui clienti, trasparenza dei titolari effettivi e utilizzo di strumenti anonimi, come i cripto-asset, nonché su nuove entità, come le piattaforme di crowdfunding. Questo regolamento si applica a decorrere dal 10 luglio 2027, salvo per quanto riguarda gli agenti calcistici e le società calcistiche professionistiche, ai quali si applicherà a decorrere dal 10 luglio 2029.
3) il regolamento Ue 2024/1620, che istituisce una nuova autorità dell'Unione europea (l'AMLA) con poteri di vigilanza e indagine per garantire la compliance in materia di antiriciclaggio e di finanziamento al terrorismo che si applicherà a decorrere dal 1° luglio 2025. La nuova Autorità sarà istituita a Francoforte e avrà il compito di supervisionare direttamente le entità finanziarie più rischiose, di intervenire in caso di carenze nella vigilanza, di fungere da centro di smistamento per le autorità di vigilanza e di mediare le controversie tra di esse, nonché di controllare l'attuazione delle sanzioni finanziarie mirate.

Il Provvedimento UIF del 23 aprile 2018 recante “Istruzioni sulle comunicazioni di dati e informazioni concernenti le operazioni sospette da parte degli uffici delle Pubbliche Amministrazioni” costituisce il principale supporto operativo per le attività di comunicazione delle operazioni sospette cui sono obbligate le Pubbliche Amministrazioni. Secondo il Provvedimento UIF del 23 aprile 2018:

- il sospetto di riciclaggio o di finanziamento del terrorismo deve essere basato su una compiuta valutazione degli elementi oggettivi e soggettivi acquisiti nell’ambito dell’attività istituzionale svolta, anche alla luce degli indicatori di anomalia;
- la comunicazione alla UIF di dati e informazioni concernenti le operazioni sospette è un atto distinto dalla denuncia di fatti penalmente rilevanti[10];
- le Pubbliche Amministrazioni assicurano la massima riservatezza dell’identità delle persone che effettuano la comunicazione e del contenuto della medesima;
- la comunicazione è inviata alla UIF a prescindere dalla rilevanza e dall’importo dell’operazione sospetta;
- la comunicazione è inviata alla UIF anche quando le Pubbliche Amministrazioni dispongono di dati e informazioni inerenti operazioni rifiutate o interrotte ovvero eseguite in tutto o in parte presso altri destinatari di autonomi obblighi di segnalazione;
- il sospetto di operazioni riconducibili al finanziamento del terrorismo si desume anzitutto dal riscontro di un nominativo e dei relativi dati anagrafici nelle liste pubbliche consultabili sul sito internet della UIF[11];

1. Ambito di applicazione, oggetto e finalità

Il Sistema di Contrasto al Riciclaggio ed al finanziamento del Terrorismo (SiCoRiTe) disciplina le procedure interne volte ad assicurare il riconoscimento, da parte delle Strutture regionali, di operazioni c.d. sospette, favorendone l’efficace rilevazione e, allo stesso tempo, a garantire la tempestività della comunicazione alla U.I.F. e la massima riservatezza dei soggetti coinvolti nell’effettuazione della comunicazione stessa.
A tal fine, il presente documento definisce le modalità con cui i soggetti coinvolti trasmettono le informazioni rilevanti ai fini della valutazione delle operazioni sospette al soggetto “Gestore”, deputato a valutare e trasmettere le comunicazioni alla U.I.F.

Il SiCoRiTe e le relative disposizioni si applicano alle strutture organizzative della Giunta regionale del Lazio che svolgono compiti di amministrazione attiva o di controllo, nell'ambito di:

a) procedimenti finalizzati all'adozione di provvedimenti di autorizzazione o concessione;
b) procedure di scelta del contraente per l'affidamento di lavori, forniture e servizi secondo le disposizioni di cui al “Codice dei contratti pubblici”;
c) procedimenti di concessione ed erogazione di sovvenzioni, contributi, sussidi, ausili finanziari, nonché attribuzioni di vantaggi economici di qualunque genere a persone fisiche ed enti pubblici e privati;
d) ulteriori procedimenti specificatamente individuati dal Comitato di Sicurezza Finanziaria[12] che saranno oggetto di specifica integrazione delle disposizioni di cui al presente atto.

Fino all’emanazione delle specifiche indicazioni previste dall’art. 10 comma 2 del D.lgs. 21 novembre 2007, n. 231, le disposizioni finalizzate all’antiriciclaggio ed al contrasto del finanziamento del terrorismo previste dal SiCoRiTe della Giunta regionale del Lazio si applicano alle procedure ed ai procedimenti sopra indicati alle lettere a), b, e c).

[10] La comunicazione alla UIF non esclude l’obbligo di denuncia di reato all’Autorità giudiziaria al quale sono soggetti i pubblici ufficiali e gli incaricati di pubblico servizio in base all’art. 331 del Codice di procedura penale.
[11] https://uif.bancaditalia.it
[12] Il Comitato di Sicurezza Finanziaria (CDF) è istituito presso il Ministero dell’Economia e delle Finanze (MEF) per monitorare il funzionamento del sistema di prevenzione e contrasto del finanziamento del terrorismo e del riciclaggio, delle attività di Paesi che minacciano la pace e la sicurezza internazionale, del finanziamento della proliferazione delle armi di distruzioni di massa, nonché attuare le misure di congelamento disposte dalle Nazioni Unite, dall'Unione europea e a livello nazionale.

Fino all'emanazione a delle specifiche linee guida previste dall'art. 10 comma 3 del D.lgs. 21 novembre 2007, n. 231, i contenuti di cui al SiCoRiTe della Giunta regionale del Lazio costituiscono idonee misure finalizzate a mappare, valutare e mitigare i rischi di riciclaggio e finanziamento del terrorismo in relazione alle dimensioni organizzative delle strutture della Giunta regionale del Lazio.

2. Definizioni

Ai fini del presente Sistema si intende per:

a) Riciclaggio:
a) "la conversione o il trasferimento di beni, effettuati essendo a conoscenza che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni;
b) l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività;
c) l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività;
d) la partecipazione ad una delle azioni di cui alle lettere a), b) e c), l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolarne l'esecuzione" (cfr. art. 2 del D.lgs. 231/2007);

b) Finanziamento del terrorismo: "qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione, in qualunque modo realizzate, di fondi e risorse economiche, direttamente o indirettamente, in tutto o in parte, utilizzabili per il compimento di una o più condotte, con finalità di terrorismo secondo quanto previsto dalle leggi penali ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette"(cfr. art. 2 del D.lgs. 231/2007);

c) U.I.F: "l'Unità di informazione finanziaria per l'Italia, cioè la struttura nazionale incaricata di ricevere dai soggetti obbligati le segnalazioni in merito alle c.d. operazioni sospette, nonché di richiedere, ai medesimi, di analizzare e di comunicare alle autorità competenti le informazioni che riguardano ipotesi di riciclaggio o di finanziamento del terrorismo" (cfr. art. 1 del D.M. Interno del 25/09/2015);

d) Operazione: "l'attività consistente nella movimentazione, nel trasferimento o nella trasmissione di mezzi di pagamento o nel compimento di atti negoziali a contenuto patrimoniale; costituisce operazione anche la stipulazione di un atto negoziale, a contenuto patrimoniale, rientrante nell'esercizio dell'attività professionale o commerciale" (cfr. art. 1 del D.lgs. 231/2007);

e) Operazione sospetta: "operazione che per caratteristiche, entità, natura, collegamento o frazionamento o per qualsivoglia altra circostanza conosciuta in ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, in base agli elementi a disposizione, acquisiti nell'ambito dell'attività svolta, induce a sapere, a sospettare o ad avere motivo ragionevole per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che, comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa" (cfr. art. 35 del D.lgs. 231/2007);

f) Operazioni collegate: "operazioni tra loro connesse per il perseguimento di un unico obiettivo di carattere giuridico patrimoniale" (cfr. art. 1 del D.lgs. 231/2007);

g) Soggetto "gestore": autorità competente a ricevere dalle Strutture regionali le comunicazioni in merito alle c.d. operazioni sospette, a valutare ed a trasmettere le segnalazioni alla U.I.F. (cfr. art. 11 del Provvedimento della U.I.F. del 23 aprile 2018). Con il soggetto gestore si rapportano i soggetti coinvolti, competenti per le procedure ed i procedimenti, di cui all'art. 3 del presente documento;

h) Comunicazione di dati e informazioni concernenti operazioni sospette: trasmissione alla UIF da parte della Pubblica Amministrazione (soggetto "gestore") dei dati e delle informazioni concernenti le operazioni sospette di cui vengano a conoscenza nell'esercizio della propria attività istituzionale ex art. 10, co. 4 del D.lgs. 231/2007. Propedeutica alla "comunicazione" alla UIF è la 'segnalazione di operazione sospetta' effettuata da parte dei Direttori regionali al Gestore, recante i dati e le informazioni necessari all'identificazione dell'operazione sospetta;

i) Paesi o territori a rischio: i Paesi o i territori non annoverati in quelli a regime antiriciclaggio equivalente a quello nazionale di cui al relativo decreto del Ministero dell'economia e delle finanze e, in ogni caso, quelli indicati da organismi internazionali competenti (ad es. GAFI, OCSE) come esposti a rischio di riciclaggio o di finanziamento del terrorismo ovvero non cooperativi nello scambio di informazioni anche in materia fiscale (cfr. artt. 9 e 64 della Direttiva (UE) 2015/849 e Regolamento Delegato (UE) 2023/1219 del 17 maggio 2023);
j) Titolare effettivo: la persona fisica o le persone fisiche, diverse dall'operatore economico/beneficiario/richiedente (corrispondente al "cliente" di cui al D.lgs. 231/2007), nell'interesse della quale o delle quali, in ultima istanza, sono eseguiti compiti di amministrazione attiva o di controllo, nell'ambito dei procedimenti e delle procedure di cui al presente Sistema (cfr. art. 1 del D.lgs. 231/2007);
k) Persone politicamente esposte: "le persone fisiche che occupano o hanno cessato di occupare da meno di un anno importanti cariche pubbliche, nonché i loro familiari e coloro che con i predetti soggetti intrattengono notoriamente stretti legami" (cfr. art. 1 del D.lgs. 231/2007);
l) Indicatori di anomalia: "indicatori volti a ridurre – nell'ambito di eventuali profili di sospetto di riciclaggio o di finanziamento del terrorismo – i margini di incertezza connessi con valutazioni soggettive o con comportamenti discrezionali, contribuendo al contenimento degli oneri e al corretto e omogeneo adempimento degli obblighi di segnalazione di operazioni sospette" (art. 6, comma 4, lett. e, dal d.lgs. 231/2007).
m) Schemi e comportamenti anomali: strumenti di ausilio che integrano gli indicatori di anomalia per l'individuazione delle operazioni sospette da parte dei segnalanti, elaborati e diffusi dalla UIF in base all'art. 6, comma 7, lett. b), del d.lgs. 231/2007, che esemplificano prassi e comportamenti anomali ricorrenti e diffusi relativi a determinati settori di operatività o a specifici fenomeni riferibili a possibili attività di riciclaggio o di finanziamento del terrorismo, mettendo in correlazione particolari sequenze logico-temporali di fatti e comportamenti che l'esperienza porta a ricondurre a determinati fenomeni criminali.

3. Soggetti coinvolti

Il SiCoRiTe della Giunta regionale del Lazio coinvolge i seguenti soggetti:

- Responsabili dei Procedimenti e/o delle Procedure di cui al paragrafo 1 "Ambito di applicazione, oggetto e finalità", lettere a), b), c);
- Dirigenti di Aree, Uffici e strutture regionali equiparate;
- Direttori di Direzioni e strutture regionali equiparate;
- Il Soggetto Gestore preposto alla valutazione ed alla effettuazione delle comunicazioni concernenti operazioni sospette di riciclaggio e di finanziamento del terrorismo alla UIF;
- La Giunta regionale.

4. Attività

Le attività di contrasto ai fenomeni di riciclaggio e di finanziamento del terrorismo previste dal SiCoRiTe della Giunta regionale del Lazio si svolgono mediante l'attuazione ciclica dei seguenti processi:

- Avvio;
- Esecuzione;
- Aggiornamento.

Il processo di "Avvio" è attuato ciclicamente con frequenza, di norma, triennale. Il processo di "Avvio" ha infatti inizio con la fase di nomina del Soggetto Gestore, compiuta mediante deliberazione di Giunta regionale, almeno una volta ogni tre anni. Alla fase di nomina del Soggetto Gestore segue la fase di registrazione dello stesso al portale INFOSTAT-UIF secondo le indicazioni tecniche riportate nel medesimo portale. La terza fase del processo di "Avvio" prevede infine la trasmissione all'UIF dei riferimenti del Soggetto Gestore e la

contestuale richiesta di abilitazione alle comunicazioni di operazioni sospette, sempre in linea con le indicazioni tecniche di INFOSTAT-UIF. In Figura 1 sono sintetizzate le singole fasi del processo di "Avvio". In Tabella 1 sono dettagliate le singole fasi del processo di "Avvio" con l'indicazione, per ciascuna fase, del responsabile, delle modalità di attuazione, della tempistica di realizzazione e del risultato da ottenere al termine di ciascuna fase.

Figura 1. Sintesi del processo di "Avvio"

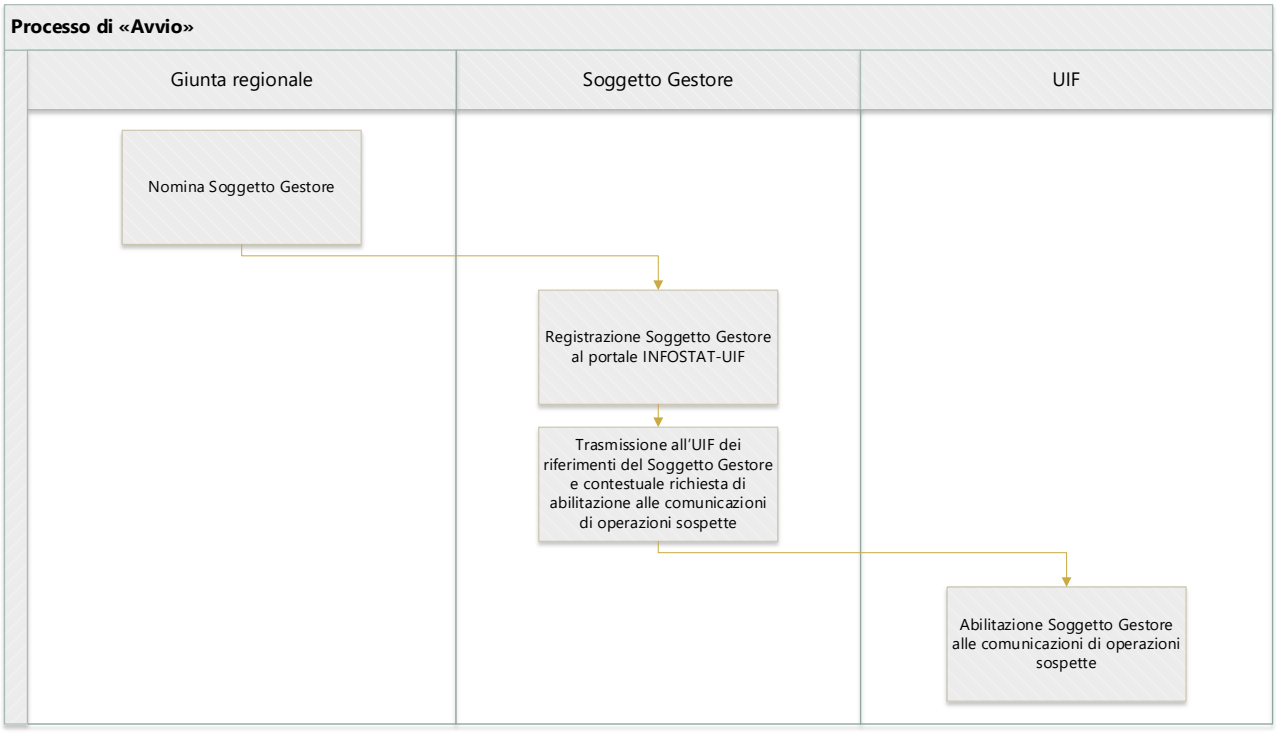

Tabella 1. Descrizione del processo di "Avvio"

Fase	Responsabile	Tempistica	Modalità	Risultato
Nomina Soggetto Gestore	Giunta regionale	Almeno una volta ogni tre anni	Deliberazione di Giunta	Soggetto Gestore nominato
Registrazione Soggetto Gestore al portale INFOSTAT-UIF	Soggetto Gestore	Senza ritardo, a valle dell'approvazione della Deliberazione di Giunta regionale di nomina del Soggetto Gestore	Via Web, come da indicazioni riportate nel portale INFOSTAT-UIF	Soggetto Gestore registrato ed in possesso delle credenziali di accesso al portale INFOSTAT-UIF
Trasmissione all'UIF dei riferimenti del Soggetto Gestore e contestuale richiesta di abilitazione alle comunicazioni di operazioni sospette	Soggetto Gestore	Senza ritardo, a valle della ricezione delle credenziali di accesso al portale INFOSTAT-UIF da parte del Soggetto Gestore	Via PEC, come da indicazioni riportate nel portale INFOSTAT-UIF	Riferimenti del Soggetto Gestore e contestuale richiesta di abilitazione alle comunicazioni di operazioni sospette trasmessi all'UIF
Abilitazione Soggetto Gestore alle comunicazioni di operazioni sospette	UIF	Senza ritardo, a valle della ricezione della PEC con i riferimenti del Soggetto Gestore e la contestuale richiesta di abilitazione alle	Via e-mail, come da indicazioni riportate nel portale INFOSTAT-UIF	Soggetto Gestore abilitato alle comunicazioni di operazioni sospette

		comunicazioni di operazioni sospette		

Il processo di “Esecuzione” è attuato ciclicamente in via continuativa. Il processo di “Esecuzione” è avviato con la fase di monitoraggio di procedimenti e/o procedure operata, in via continuativa, dal Responsabile del Procedimento e/o della Procedura di cui al paragrafo 1 “Ambito di applicazione, oggetto e finalità”, lettere a), b), c) che, nell’ambito dell’attività ordinaria, opera un continuo raffronto del contesto soggettivo e/o oggettivo del procedimento e/o della procedura con gli indicatori di anomalia. Segue la fase di rilevazione anomalie posta in essere sempre a cura dello stesso Responsabile del Procedimento e/o della Procedura di cui al paragrafo 1 “Ambito di applicazione, oggetto e finalità”, lettere a), b), c) che, al presentarsi delle anomalie nel corso del procedimento e/o della procedura, senza ritardo, trasmette una comunicazione riservata, via e-mail al Dirigente sovraordinato, utilizzando il modulo A allegato al presente documento, con annessa descrizione delle anomalie emerse nel contesto soggettivo e/o oggettivo del procedimento e/o della procedura. La successiva fase di analisi delle anomalie è svolta dal Dirigente sovraordinato che, a valle della ricezione della comunicazione, senza ritardo, opera il raffronto delle anomalie emerse nel contesto soggettivo e/o oggettivo del procedimento e/o della procedura con il Provvedimento UIF 23 aprile 2018 e trasmette una comunicazione riservata, via e-mail al Direttore sovraordinato, utilizzando il modulo B allegato al presente documento, con annessa descrizione delle anomalie emerse nel contesto soggettivo e/o oggettivo del procedimento e/o della procedura ed annessa proposta di interruzione o prosecuzione dell’iter di comunicazione dell’operazione sospetta. La fase successiva prevede la formalizzazione dell’operazione sospetta a cura del Direttore sovraordinato che, senza ritardo, a valle della ricezione della comunicazione riservata via e-mail con la proposta di prosecuzione dell’iter di comunicazione dell’operazione sospetta, provvede ad una descrizione dettagliata degli elementi oggettivi e soggettivi che caratterizzano l’operazione sospetta acquisiti nell’ambito dell’attività istituzionale, anche alla luce degli indicatori di anomalia di cui al Provvedimento UIF 23 aprile 2018 e di tutte le altre informazioni disponibili, e trasmette in modalità riservata, via protocollo al Soggetto Gestore, la formale comunicazione di operazione sospetta, utilizzando il modulo C allegato al presente documento. La fase successiva prevede la valutazione dell’operazione sospetta a cura del Soggetto Gestore che, senza ritardo, a valle della ricezione della formale comunicazione di operazione sospetta, opera una compiuta valutazione degli elementi oggettivi e soggettivi che caratterizzano l’operazione sospetta acquisiti nell’ambito dell’attività istituzionale, anche alla luce degli indicatori di anomalia di cui al Provvedimento UIF 23 aprile 2018 e di tutte le di tutte le altre informazioni disponibili. L’ultima fase del processo di “Esecuzione” prevede la comunicazione dell’operazione sospetta operata dal Soggetto Gestore – senza ritardo a valle della compiuta valutazione dell’operazione segnalata con esplicito riferimento alla prosecuzione dell’iter di comunicazione dell’operazione sospetta – in via telematica, attraverso la rete internet, tramite il portale INFOSTAT-UIF della Banca d’Italia, con modalità, contenuti, dati, elementi informativi ed allegati di cui al Provvedimento UIF 23 aprile 2018. In Figura 2 sono sintetizzate le singole fasi del processo di “Esecuzione”. In Tabella 2 sono dettagliate le singole fasi processo di “Esecuzione” con l’indicazione, per ciascuna fase, del responsabile, delle modalità di attuazione, della tempistica di realizzazione e del risultato da ottenere al termine di ciascuna fase.

Figura 2. Sintesi del processo di "Esecuzione"

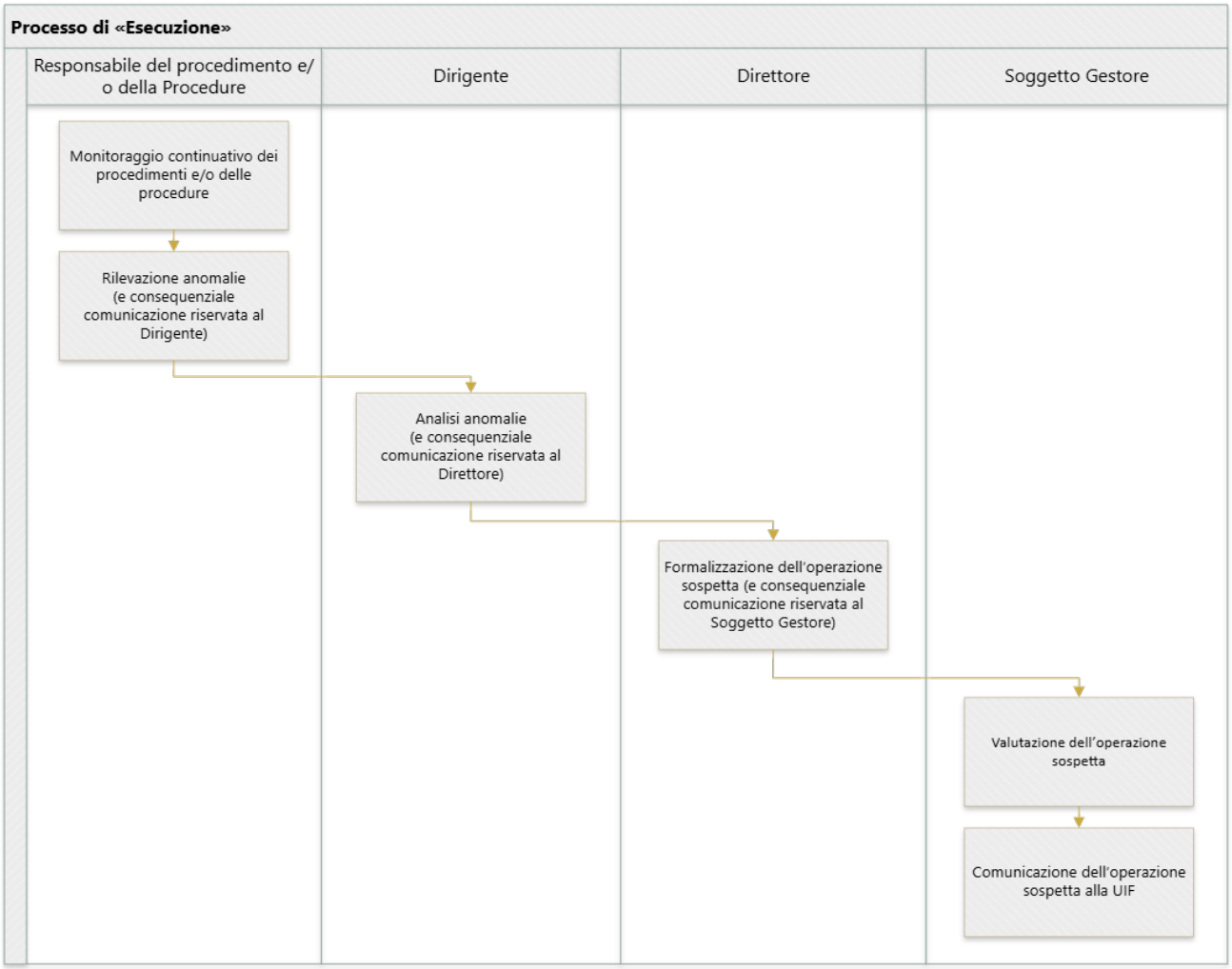

Tabella 2. Descrizione del processo di "Esecuzione"

Fase	Responsabile	Tempistica	Modalità	Risultato
Monitoraggio procedimenti e/o procedure	Responsabile del Procedimento e/o della Procedure di cui al paragrafo 1 "Ambito di applicazione" lettere a), b), c)	In via continuativa	Raffronto del contesto soggettivo e/o oggettivo del procedimento e/o della procedura con gli indicatori di anomalia	Procedimenti e/o procedure monitorate
Rilevazione anomalie	Responsabile del Procedimento e/o della Procedure di cui al paragrafo 1 "Ambito di	Senza ritardo, al presentarsi delle anomalie nel corso del	Rilevazione delle anomalie nel contesto soggettivo e/o oggettivo	Comunicazione riservata via e-mail utilizzando il modulo A al Dirigente

	applicazione" lettere a), b), c)	procedimento e/o della procedura	del procedimento e/o della procedura	sovraordinato con annessa descrizione delle anomalie emerse nel contesto soggettivo e/o oggettivo del procedimento e/o della procedura
Analisi anomalie	Dirigenti di Aree, Uffici e strutture regionali equiparate	Senza ritardo, a valle della ricezione della comunicazione riservata via-e-mail con la descrizione dell'anomalia nel contesto soggettivo e/o oggettivo del procedimento e/o della procedura	Raffronto delle anomalie emerse nel contesto soggettivo e/o oggettivo del procedimento e/o della procedura con il Provvedimento UIF 23 aprile 2018	Comunicazione riservata via e-mail al Direttore sovraordinato utilizzando il modulo B con annessa descrizione delle anomalie emerse nel contesto soggettivo e/o oggettivo del procedimento e/o della procedura ed annessa proposta di interruzione o prosecuzione dell'iter di comunicazione dell'operazione sospetta
Formalizzazione dell'operazione sospetta	Direttori di Direzioni e strutture regionali equiparate	Senza ritardo, a valle della ricezione della comunicazione riservata via e-mail con la proposta di prosecuzione dell'iter di comunicazione dell'operazione sospetta	Descrizione dettagliata degli elementi oggettivi e soggettivi che caratterizzano l'operazione sospetta acquisiti nell'ambito dell'attività istituzionale, anche alla luce degli indicatori di anomalia di cui al Provvedimento UIF 23 aprile 2018 e di tutte le altre informazioni disponibili	Formale comunicazione di operazione sospetta inviata, in modalità riservata, via protocollo al Soggetto Gestore utilizzando il modulo C
Valutazione dell'operazione sospetta	Soggetto Gestore	Senza ritardo, a valle della ricezione della formale comunicazione di operazione sospetta inviata, in modalità riservata, via protocollo al Soggetto Gestore	Formale, compiuta valutazione degli elementi oggettivi e soggettivi che caratterizzano l'operazione sospetta acquisiti nell'ambito dell'attività istituzionale, anche alla luce degli indicatori di anomalia di cui al Provvedimento UIF 23 aprile 2018 e di tutte le di tutte le altre informazioni disponibili	Compiuta valutazione dell'operazione sospetta, con esplicito riferimento all'interruzione o alla prosecuzione dell'iter di comunicazione dell'operazione sospetta
Comunicazione dell'operazione sospetta	Soggetto Gestore	Senza ritardo, a valle della compiuta valutazione dell'operazione sospetta, con esplicito riferimento alla prosecuzione	In via telematica, attraverso la rete internet, tramite il portale INFOSTAT-UIF della Banca d'Italia, con modalità, contenuti, dati,	Comunicazione dell'operazione sospetta inviata all'UIF

		dell'iter di comunicazione dell'operazione sospetta	elementi informativi ed allegati di cui al Provvedimento UIF 23 aprile 2018	

Il processo di "Aggiornamento" è attuato ciclicamente con frequenza, di norma, annuale. Il processo di "Aggiornamento" è avviato con la fase di predisposizione di percorsi formativi in materia di contrasto al riciclaggio ed al finanziamento del terrorismo, a cura del Direttore regionale competente in materia di personale che, almeno una volta ogni anno, mette a disposizione del personale in servizio presso le strutture della Giunta Regionale percorsi formativi in materia di contrasto al riciclaggio ed al finanziamento del terrorismo erogati mediante formazione a distanza, asincrona, in linea con le previsioni contenutistiche di cui all'art. 10, comma 5, D.lgs 21 novembre 2007, n. 231. La successiva fase di partecipazione ai percorsi formativi in materia di contrasto al riciclaggio ed al finanziamento del terrorismo chiama in causa tutto il personale in servizio presso le strutture della Giunta Regionale invitato, senza ritardo, a fruirne via Web, come da indicazioni del Direttore regionale competente in materia di personale, onde acquisire le conoscenze necessarie a riconoscere fattispecie meritevoli di comunicazioni di operazioni sospette. La fase di monitoraggio relativa alle novità normative/ regolamentari/operative in materia di contrasto al riciclaggio ed al finanziamento del terrorismo è attuata, in via continuativa, dal Soggetto Gestore che, tramite specifiche attività di formazione, informazione, comunicazione in materia di contrasto al riciclaggio ed al finanziamento del terrorismo, rileva predette novità. Segue la fase di proposta di aggiornamento formale del SiCoRiTe, a cura del Soggetto Gestore che, senza ritardo, a valle della rilevazione di predette novità, propone formalmente alla Giunta regionale la relativa Deliberazione di aggiornamento. L'ultima fase del processo di "Aggiornamento" comprende l'adeguamento formale del SiCoRiTe che la Giunta regionale pone in essere approvando la relativa proposta di Deliberazione avanzata dal Soggetto Gestore.

Figura 3. Sintesi del processo di "Aggiornamento"

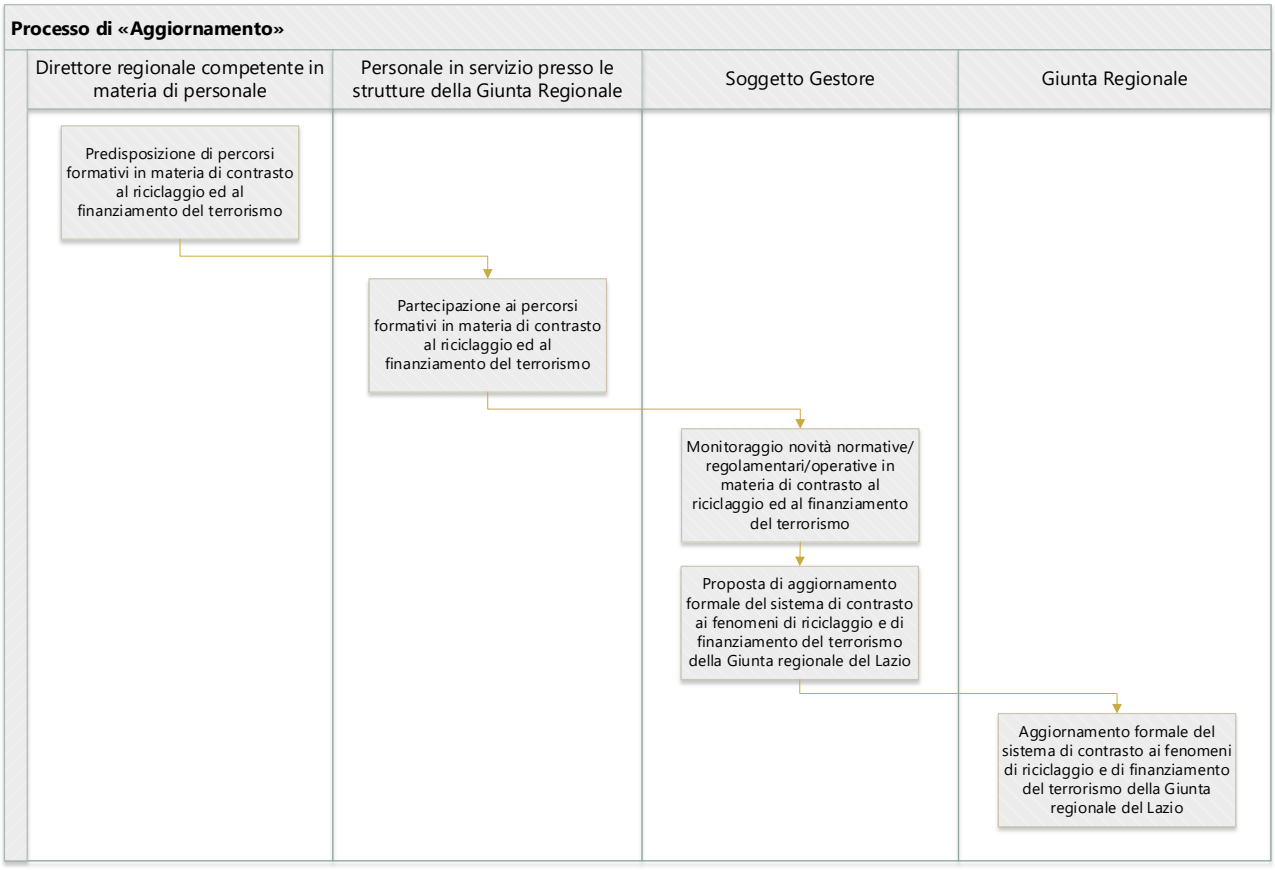

Tabella 3. Descrizione del processo di "Aggiornamento"

Fase	Responsabile	Tempistica	Modalità	Risultato
Predisposizione di percorsi formativi in materia di contrasto al riciclaggio ed al finanziamento del terrorismo	Direttore regionale competente in materia di personale	Almeno una volta ogni anno	Formazione a distanza, asincrona, in linea con le previsioni contenutistiche di cui all'art. 10, comma 5, D.lgs 21 novembre 2007, n. 231	Percorsi formativi in materia di contrasto al riciclaggio ed al finanziamento del terrorismo a disposizione del personale in servizio presso le strutture della Giunta Regionale
Partecipazione ai percorsi formativi in materia di contrasto al riciclaggio ed al finanziamento del terrorismo	Personale in servizio presso le strutture della Giunta Regionale	Senza ritardo, a valle della disponibilità dei percorsi formativi in materia di contrasto al riciclaggio ed al finanziamento del terrorismo	Via Web, come da indicazioni del Direttore regionale competente in materia di personale	Personale in servizio presso le strutture della Giunta Regionale formato per riconoscere fattispecie meritevoli di comunicazioni di operazioni sospette
Monitoraggio novità normative/ regolamentari/operative in materia di contrasto al riciclaggio ed al finanziamento del terrorismo	Soggetto Gestore	In via continuativa	Tramite specifiche attività di formazione, informazione, comunicazione in materia di contrasto al riciclaggio ed al finanziamento del terrorismo	Novità normative/ regolamentari/operative in materia di contrasto al riciclaggio ed al finanziamento del terrorismo rilevate dal Soggetto Gestore
Proposta di aggiornamento formale del SiCoRiTe	Soggetto Gestore	Senza ritardo, a valle della rilevazione di novità normative/ regolamentari/operative in materia di contrasto al riciclaggio ed al finanziamento del terrorismo	Proposta di Deliberazione di Giunta regionale	Proposta di aggiornamento formale del SiCoRiTe
Aggiornamento formale del SiCoRiTe	Giunta regionale	A valle della ricezione della proposta di Deliberazione di Giunta regionale di aggiornamento formale del SiCoRiTe	Deliberazione di Giunta regionale	Sistema di contrasto ai fenomeni di riciclaggio e di finanziamento del terrorismo della Giunta regionale del Lazio aggiornato

5. Supporti tecnologici

Al fine di agevolare l'attività di contrasto ai fenomeni di riciclaggio e di finanziamento del terrorismo:

- il Soggetto Gestore provvede alla pubblicazione aggiornata di norme, atti, provvedimenti e modelli standardizzati resi disponibili al personale in servizio presso le strutture della Giunta regionale del Lazio anche tramite una specifica sezione del portale Intranet;
- il Direttore competente in materia di innovazione tecnologica, sentiti il Direttore competente in materia di ragioneria ed il Soggetto Gestore, provvede all'eventuale sviluppo tecnologico dei sistemi informatici in uso presso le strutture della Giunta regionale, anche tramite l'implementazione di sistemi per il riconoscimento automatizzato di eventuali corrispondenze tra dati in trattazione da parte delle strutture della Giunta regionale e dati presenti nelle liste pubblicate sul portale UIF per le medesime finalità di contrasto ai fenomeni di riciclaggio e di finanziamento del terrorismo.

6. Banche-dati

Le anomalie eventualmente rilevate nel corso dell'attività istruttoria devono formare oggetto di ulteriore verifica anche tramite accesso a banche-dati nella disponibilità dell'Amministrazione regionale o di altri Enti pubblici o privati.

Ai fini delle verifiche in oggetto potranno essere utilizzate, in relazione a ciascun ambito di competenza ed alla relativa disponibilità/accessibilità, le seguenti banche-dati:

- Agenzia Entrate – SIATEL Punto Fisco;
- Agenzia Entrate e Riscossione;
- Anagrafe Catasto Nazionale – SISTER;
- Casellario Informatico dei contratti pubblici di lavori, servizi e forniture (c.d. "Casellario Informatico ANAC") – annotazioni riservate sugli operatori economici;
- Elenco dei fornitori, prestatori di servizi ed esecutori non soggetti a tentativo di infiltrazione mafiosa (c.d. "White List") istituito presso le Prefetture;
- Motorizzazione civile – MTC;
- ACI – PRA;
- TELEMACO – Registro Imprese - Banca dati Camere di Commercio;
- ARACHNE – Strumento di valutazione del rischio della Commissione Europea;
- Sistema Informativo "ReGiS";
- BORIS – *Beneficial Ownership Registers Interconnection System* (c.d. "Sistema di interconnessione dei registri dei titolari effettivi");
- PIAF – Piattaforma Integrata Anti-Frode;
- BDU – Banca dati Unitaria - MEF- RGS - IGRUE;
- BDAP – Banca dati delle pubbliche Amministrazioni;
- BDNCP – Banca Dati Nazionale dei Contratti Pubblici.

Potranno altresì essere consultate le liste dei soggetti designati dal Consiglio di Sicurezza dell'ONU e dall'Unione Europea, nonché le ulteriori liste predisposte da altre istituzioni ed enti coinvolti nel contrasto del terrorismo internazionale, come quella dell'Office of Foreign Asset Control (OFAC) del Dipartimento del Tesoro degli Stati Uniti, la lista dei Paesi ad alto rischio (c.d. *black list*) e la lista dei Paesi con deficienze strategiche nei sistemi AML/CFT sottoposti ad intenso monitoraggio (c.d. *grey list*) pubblicate dal Gruppo di Azione Finanziaria Internazionale (GAFI).

Resta ferma la possibilità di integrare in ogni momento la predetta lista delle banche dati consultabili o fornire chiarimenti in ordine al loro utilizzo, anche sulla base di specifiche indicazioni ricevute da parte dei soggetti Gestori.

7. Indicatori di anomalia

Con riferimento agli indicatori di anomalia, il Provvedimento UIF del 23 aprile 2018 evidenzia quanto segue.

Gli indicatori di anomalia sono volti a ridurre i margini di incertezza delle valutazioni soggettive connesse alle comunicazioni di operazioni sospette e hanno lo scopo di contribuire al contenimento degli oneri e alla correttezza e omogeneità delle comunicazioni medesime.

L'elencazione degli indicatori di anomalia non è esaustiva, anche in considerazione della continua evoluzione delle modalità di svolgimento delle operazioni.

L'impossibilità di ricondurre operazioni o comportamenti a uno o più degli indicatori non è sufficiente a escludere che l'operazione sia sospetta; vanno valutati pertanto con la massima attenzione ulteriori

comportamenti e caratteristiche dell'operazione che, sebbene non descritti negli indicatori, siano egualmente sintomatici di profili di sospetto.

La mera ricorrenza di operazioni o comportamenti descritti in uno o più indicatori di anomalia non è motivo di per sé sufficiente per la qualificazione dell'operazione come sospetta ai fini della comunicazione alla UIF, ma è comunque necessario svolgere una specifica analisi nel concreto e una valutazione complessiva dell'operatività avvalendosi di tutte le altre informazioni disponibili.

Le Pubbliche Amministrazioni applicano gli indicatori rilevanti alla luce dell'attività istituzionale in concreto svolta e si avvalgono degli indicatori di carattere generale unitamente a quelli specifici per tipologia attività.

Ai fini dell'applicazione degli indicatori, per "soggetto cui è riferita l'operazione" si intende il soggetto (persona fisica o entità giuridica) che entra in relazione con le Pubbliche amministrazioni e riguardo al quale emergono elementi di sospetto di riciclaggio, di finanziamento del terrorismo o di provenienza da attività criminosa delle risorse economiche e finanziarie.

Per favorirne la lettura e la comprensione alcuni indicatori sono stati specificati in sub-indici; i sub-indici costituiscono un'esemplificazione dell'indicatore di riferimento e devono essere valutati congiuntamente al contenuto dello stesso. I riferimenti dell'indicatore a circostanze oggettive (quali, ad esempio, la ripetitività dei comportamenti o la rilevanza economica dell'operazione) ovvero soggettive (quali, ad esempio, l'eventuale incoerenza della giustificazione addotta o del profilo economico del soggetto cui è riferita l'operazione), seppure non specificamente richiamati, valgono anche con riguardo ai relativi sub-indici.

Le operazioni e i comportamenti inerenti ad attività economiche svolte nei settori degli appalti e dei finanziamenti pubblici, individuati nella sezione C, devono essere valutati sulla base degli elementi di anomalia indicati per ciascun settore e dei seguenti criteri: incoerenza con l'attività o il profilo economico-patrimoniale del soggetto cui è riferita l'operazione; assenza di giustificazione economica; inusualità, illogicità, elevata complessità dell'attività.

A. Indicatori di anomalia connessi con l'identità o il comportamento del soggetto cui è riferita l'operazione

- Il soggetto cui è riferita l'operazione ha residenza, cittadinanza o sede in Paesi terzi ad alto rischio[13], ovvero opera con controparti situate in tali Paesi, e richiede ovvero effettua operazioni di significativo ammontare con modalità inusuali, in assenza di plausibili ragioni.
- Il soggetto cui è riferita l'operazione ha residenza, cittadinanza o sede in un Paese la cui legislazione non consente l'identificazione dei nominativi che ne detengono la proprietà o il controllo.
- Il soggetto cui è riferita l'operazione risiede in una zona o in un territorio notoriamente considerati a rischio, in ragione tra l'altro dell'elevato grado di infiltrazione criminale, di economia sommersa o di degrado economico-istituzionale.
- Il soggetto cui è riferita l'operazione risiede ovvero opera con controparti situate in aree di conflitto o in Paesi che notoriamente finanziano o sostengono attività terroristiche o nei quali operano organizzazioni terroristiche, ovvero in zone limitrofe o di transito rispetto alle predette aree.
- Il soggetto cui è riferita l'operazione presenta documenti (quali, ad esempio, titoli o certificati), specie se di dubbia autenticità, attestanti l'esistenza di cospicue disponibilità economiche o finanziarie in Paesi terzi ad alto rischio.
- Il soggetto cui è riferita l'operazione presenta garanzie reali o personali rilasciate da soggetti con residenza, cittadinanza o sede in Paesi terzi ad alto rischio ovvero attinenti a beni ubicati nei suddetti Paesi.
- Il soggetto cui è riferita l'operazione fornisce informazioni palesemente inesatte o del tutto incomplete o addirittura false ovvero si mostra riluttante a fornire ovvero rifiuta di fornire informazioni, dati e

[13] Paesi non appartenenti all'Unione europea i cui ordinamenti presentano carenze strategiche nei rispettivi regimi nazionali di prevenzione del riciclaggio e del finanziamento del terrorismo, per come individuati dalla Commissione europea nell'esercizio dei poteri di cui agli articoli 9 e 64 della direttiva (UE) 2015/849.

documenti comunemente acquisiti per l'esecuzione dell'operazione, in assenza di plausibili giustificazioni.

- Il soggetto cui è riferita l'operazione presenta documentazione che appare falsa o contraffatta ovvero contiene elementi del tutto difformi da quelli tratti da fonti affidabili e indipendenti o presenta comunque forti elementi di criticità o di dubbio.
- Il soggetto cui è riferita l'operazione, all'atto di esibire documenti di identità ovvero alla richiesta di fornire documentazione o informazioni inerenti all'operazione, rinuncia a eseguirla.
- Il soggetto cui è riferita l'operazione rifiuta di ovvero è reticente a fornire informazioni o documenti concernenti aspetti molto rilevanti, specie se attinenti all'individuazione dell'effettivo beneficiario dell'operazione.
- Il soggetto cui è riferita l'operazione risulta collegato, direttamente o indirettamente, con soggetti sottoposti a procedimenti penali o a misure di prevenzione patrimoniale ovvero con persone politicamente esposte[14] o con soggetti censiti nelle liste pubbliche delle persone o degli enti coinvolti nel finanziamento del terrorismo, e richiede ovvero effettua operazioni di significativo ammontare con modalità inusuali, in assenza di plausibili ragioni.
- Il soggetto cui è riferita l'operazione è notoriamente contiguo (ad esempio, familiare, convivente, associato) ovvero opera per conto di persone sottoposte a procedimenti penali o a misure di prevenzione patrimoniale o ad altri provvedimenti di sequestro.
- Il soggetto cui è riferita l'operazione è notoriamente contiguo (ad esempio, familiare, convivente, associato) ovvero opera per conto di persone che risultano rivestire importanti cariche pubbliche, anche a livello domestico, nazionale o locale.
- Il soggetto cui è riferita l'operazione è un'impresa che è connessa a vario titolo a una persona con importanti cariche pubbliche a livello domestico e che improvvisamente registra un notevole incremento del fatturato a livello nazionale o del mercato locale.
- Il soggetto cui è riferita l'operazione è notoriamente contiguo (ad esempio, familiare, convivente, associato) ovvero opera per conto di soggetti censiti nelle liste delle persone o degli enti coinvolti nel finanziamento del terrorismo o comunque notoriamente riconducibili ad ambienti del radicalismo o estremismo.
- l soggetto cui è riferita l'operazione è un'impresa, specie se costituita di recente, partecipata da soci ovvero con amministratori di cui è nota la sottoposizione a procedimenti penali o a misure di prevenzione o che sono censiti nelle liste delle persone o degli enti coinvolti nel finanziamento del terrorismo, ovvero notoriamente contigui a questi.
- Il soggetto cui è riferita l'operazione intrattiene rilevanti rapporti finanziari con fondazioni, associazioni, altre organizzazioni non profit ovvero organizzazioni non governative, riconducibili a persone sottoposte a procedimenti penali o a misure di prevenzione patrimoniale o a provvedimenti di sequestro, a persone che risultano rivestire importanti cariche pubbliche, anche a livello domestico, ovvero a soggetti censiti nelle liste delle persone o degli enti coinvolti nel finanziamento del terrorismo.
- Il soggetto cui è riferita l'operazione risulta collegato con organizzazioni non profit ovvero con organizzazioni non governative che presentano tra loro connessioni non giustificate, quali ad esempio la condivisione dell'indirizzo, dei rappresentanti o del personale, ovvero la titolarità di molteplici rapporti riconducibili a nominativi ricorrenti.
- Il soggetto cui è riferita l'operazione risulta caratterizzato da assetti proprietari, manageriali e di controllo artificiosamente complessi od opachi e richiede ovvero effettua operazioni di significativo ammontare con modalità inusuali, in assenza di plausibili ragioni.

[14] Le persone fisiche che occupano o hanno cessato di occupare da meno di un anno importanti cariche pubbliche, nonché i loro familiari e coloro che con i predetti soggetti intrattengono notoriamente stretti legami, come elencate dall'art. 1, comma 2, lettera dd), del decreto legislativo 21 novembre 2007, n. 231.

- Il soggetto cui è riferita l'operazione è caratterizzato da strutture societarie opache (desumibili, ad esempio, da visure nei registri camerali) ovvero si avvale artificiosamente di società caratterizzate da catene partecipative complesse nelle quali sono presenti, a titolo esemplificativo, *trust*, fiduciarie, fondazioni, *international business company*.
- Il soggetto cui è riferita l'operazione è caratterizzato da ripetute e/o improvvise modifiche nell'assetto proprietario, manageriale (ivi compreso il "direttore tecnico") o di controllo dell'impresa.
- Il soggetto cui è riferita l'operazione è di recente costituzione, effettua una intensa operatività finanziaria, cessa improvvisamente l'attività e viene posto in liquidazione.
- Il soggetto cui è riferita l'operazione è un'impresa, specie se costituita di recente, controllata o amministrata da soggetti che appaiono come meri prestanome.
- Il soggetto che effettua ripetute richieste di operazioni mantiene invariati gli assetti gestionali e/o la propria operatività, nonostante sia un'azienda sistematicamente in perdita o comunque in difficoltà finanziaria.
- Il soggetto cui è riferita l'operazione mostra di avere scarsa conoscenza della natura, dell'oggetto, dell'ammontare o dello scopo dell'operazione, ovvero è accompagnato da altri soggetti che si mostrano interessati all'operazione, generando il sospetto di agire non per conto proprio ma di terzi.

B. Indicatori di anomalia connessi con le modalità (di richiesta o esecuzione) delle operazioni.

Richiesta ovvero esecuzione di operazioni con oggetto o scopo del tutto incoerente con l'attività o con il complessivo profilo economico-patrimoniale del soggetto cui è riferita l'operazione o dell'eventuale gruppo di appartenenza, desumibile dalle informazioni in possesso o comunque rilevabili da fonti aperte, in assenza di plausibili giustificazioni.

- Acquisto di beni o servizi non coerente con l'attività del soggetto cui è riferita l'operazione, specie se seguito da successivo trasferimento del bene o servizio in favore di società appartenenti allo stesso gruppo, in mancanza di corrispettivo.
- Impiego di disponibilità che appaiono del tutto sproporzionate rispetto al profilo economico-patrimoniale del soggetto (ad esempio, operazioni richieste o eseguite da soggetti con "basso profilo fiscale" o che hanno omesso di adempiere agli obblighi tributari).
- Operazioni richieste o effettuate da organizzazioni *non profit* ovvero da organizzazioni non governative che, per le loro caratteristiche (ad esempio tipologie di imprese beneficiarie o aree geografiche di destinazione dei fondi), risultano riconducibili a scopi di finanziamento del terrorismo ovvero manifestamente incoerenti con le finalità dichiarate o comunque proprie dell'ente in base alla documentazione prodotta, specie se tali organizzazioni risultano riconducibili a soggetti che esercitano analoga attività a fini di lucro.
- Operazioni richieste o effettuate da più soggetti recanti lo stesso indirizzo ovvero la medesima domiciliazione fiscale, specie se tale indirizzo appartiene anche a una società commerciale e ciò appare incoerente rispetto all'attività dichiarata dagli stessi.
- Richiesta di regolare i pagamenti mediante strumenti incoerenti rispetto alle ordinarie prassi di mercato, in assenza di ragionevoli motivi legati al tipo di attività esercitata o a particolari condizioni adeguatamente documentate.
- Offerta di polizze di assicurazione relative ad attività sanitaria da parte di agenti o *brokers* operanti in nome e/o per conto di società estere, anche senza succursali in Italia, a prezzi sensibilmente inferiori rispetto a quelli praticati nel mercato.

Richiesta ovvero esecuzione di operazioni prive di giustificazione commerciale con modalità inusuali rispetto al normale svolgimento della professione o dell'attività, soprattutto se caratterizzate da elevata complessità o da significativo ammontare, qualora non siano rappresentate specifiche esigenze.

- Frequente e inconsueto rilascio di deleghe o procure al fine di evitare contatti diretti ovvero utilizzo di indirizzi, anche postali, diversi dal domicilio, dalla residenza o dalla sede, o comunque ricorso ad altre forme di domiciliazione di comodo.

- Frequente richiesta di operazioni per conto di uno o più soggetti terzi, in assenza di ragionevoli motivi legati al tipo di attività esercitata o al rapporto tra le parti o a particolari condizioni adeguatamente documentate.
- Estinzione anticipata e inaspettata, in misura totale o parziale, dell'obbligazione da parte del soggetto cui è riferita l'operazione.
- Richiesta di estinzione di un'obbligazione effettuata da un terzo estraneo al rapporto negoziale, in assenza di ragionevoli motivi o di collegamenti con il soggetto cui è riferita l'operazione.
- Improvviso e ingiustificato intervento di un terzo a copertura dell'esposizione del soggetto cui è riferita l'operazione, specie laddove il pagamento sia effettuato in un'unica soluzione ovvero sia stato concordato in origine un pagamento rateizzato.
- Presentazione di garanzie personali rilasciate da parte di soggetti che sembrano operare in via professionale senza essere autorizzati allo svolgimento dell'attività di prestazione di garanzie.

Richiesta ovvero esecuzione di operazioni con configurazione illogica ed economicamente o finanziariamente svantaggiose, specie se sono previste modalità eccessivamente complesse od onerose, in assenza di plausibili giustificazioni.

- Richiesta a una Pubblica amministrazione dislocata in località del tutto estranea all'area di interesse dell'attività del soggetto cui è riferita l'operazione, specie se molto distante dalla residenza, dal domicilio o dalla sede effettiva.
- Richiesta di modifica delle condizioni o delle modalità di svolgimento dell'operazione, specie se tali modifiche comportano ulteriori oneri a carico del soggetto cui è riferita l'operazione.
- Richiesta di esecuzione in tempi particolarmente ristretti a prescindere da qualsiasi valutazione attinente alle condizioni economiche.
- Acquisto o vendita di beni o servizi di valore significativo (ad esempio, beni immobili e mobili registrati; società; contratti; brevetti; partecipazioni) effettuate a prezzi palesemente sproporzionati rispetto ai correnti valori di mercato o al loro prevedibile valore di stima.
- Operazioni ripetute, di importo significativo, effettuate in contropartita con società che risultano costituite di recente e hanno un oggetto sociale generico o incompatibile con l'attività del soggetto che richiede o esegue l'operazione (ad esempio, nel caso di rapporti ripetuti fra appaltatori e subappaltatori "di comodo").
- Richiesta di accredito su rapporti bancari o finanziari sempre diversi.
- Proposta di regolare sistematicamente i pagamenti secondo modalità tali da suscitare il dubbio che si intenda ricorrere a tecniche di frazionamento del valore economico dell'operazione.
- Ripetuto ricorso a contratti a favore di terzo, contratti per persona da nominare o a intestazioni fiduciarie, specie se aventi ad oggetto diritti su beni immobili o partecipazioni societarie.

C. Indicatori specifici per settore di attività

1. Settore appalti e contratti pubblici[15]

- Partecipazione a gara per la realizzazione di lavori pubblici o di pubblica utilità, specie se non programmati, in assenza dei necessari requisiti (soggettivi, economici, tecnico-realizzativi, organizzativi e gestionali) con apporto di rilevanti mezzi finanziari privati, specie se di incerta provenienza o non compatibili con il profilo economico-patrimoniale dell'impresa, ovvero con una forte disponibilità di anticipazioni finanziarie e particolari garanzie di rendimento prive di idonea giustificazione.
- Partecipazione a procedure di affidamento di lavori pubblici, servizi e forniture in assenza di qualsivoglia convenienza economica all'esecuzione del contratto, anche con riferimento alla dimensione aziendale e alla località di svolgimento della prestazione.
- Partecipazione a procedure di affidamento di lavori pubblici, servizi e forniture da parte di un raggruppamento temporaneo di imprese, costituito da un numero di partecipanti del tutto sproporzionato in relazione al valore economico e alle prestazioni oggetto del contratto, specie se il singolo partecipante è a sua volta riunito, raggruppato o consorziato.

[15] Le operazioni e i comportamenti inerenti ad attività economiche svolte nei settori degli appalti e dei finanziamenti pubblici devono essere valutati sulla base degli elementi di anomalia indicati per ciascun settore e dei seguenti criteri: incoerenza con l'attività o il profilo economico-patrimoniale del soggetto cui è riferita l'operazione; assenza di giustificazione economica; inusualità, illogicità, elevata complessità dell'attività.

- Partecipazione a procedure di affidamento di lavori pubblici, servizi e forniture da parte di una rete di imprese il cui programma comune non contempla tale partecipazione tra i propri scopi strategici.
- Partecipazione a procedure di affidamento di lavori pubblici, servizi e forniture mediante ricorso al meccanismo dell'avvalimento plurimo o frazionato, ai fini del raggiungimento della qualificazione richiesta per l'aggiudicazione della gara, qualora il concorrente non dimostri l'effettiva disponibilità dei mezzi facenti capo all'impresa avvalsa, necessari all'esecuzione dell'appalto, ovvero qualora dal contratto di avvalimento o da altri elementi assunti nel corso del procedimento se ne desuma l'eccessiva onerosità ovvero l'irragionevolezza.
- Partecipazione a procedure di affidamento di lavori pubblici, servizi e forniture da parte di soggetti che, nel corso dell'espletamento della gara, ovvero della successiva esecuzione, realizzano operazioni di cessione, affitto di azienda o di un suo ramo ovvero di trasformazione, fusione o scissione della società, prive di giustificazione.
- Presentazione di offerta con un ribasso sull'importo a base di gara particolarmente elevato nei casi in cui sia stabilito un criterio di aggiudicazione al prezzo più basso, ovvero che risulta anormalmente bassa sulla base degli elementi specifici acquisiti dalla stazione appaltante, specie se il contratto è caratterizzato da complessità elevata.
- Presentazione di una sola offerta da parte del medesimo soggetto nell'ambito di procedure di gara che prevedono tempi ristretti di presentazione delle offerte, requisiti di partecipazione particolarmente stringenti e un costo della documentazione di gara sproporzionato rispetto all'importo del contratto, specie se il bando di gara è stato modificato durante il periodo di pubblicazione.
- Ripetuti affidamenti a un medesimo soggetto, non giustificati dalla necessità di evitare soluzioni di continuità di un servizio nelle more della indizione ovvero del completamento della procedura di gara.
- Ripetute aggiudicazioni a un medesimo soggetto, in assenza di giustificazione, specie se in un breve arco temporale, per contratti di importo elevato e mediante affidamenti diretti o con procedura negoziata senza previa pubblicazione del bando di gara, o a seguito di procedura a evidenza pubblica precedentemente revocata.
- Contratto aggiudicato previo frazionamento in lotti non giustificato in relazione alla loro funzionalità, possibilità tecnica o convenienza economica.
- Modifiche delle condizioni contrattuali in fase di esecuzione, consistenti in una variazione delle prestazioni originarie, in un allungamento dei termini di ultimazione dei lavori, servizi o forniture, in rinnovi o proroghe, al di fuori dei casi normativamente previsti, o in un significativo incremento dell'importo contrattuale.
- Esecuzione del contratto caratterizzata da ripetute e non giustificate operazioni di cessione, affitto di azienda o di un suo ramo, ovvero di trasformazione, fusione o scissione della società.
- Ricorso al subappalto oltre la quota parte subappaltabile, in assenza di preventiva indicazione in sede di offerta ovvero senza il necessario deposito del contratto di subappalto presso la stazione appaltante o della documentazione attestante il possesso da parte del subappaltatore dei requisiti di legge.
- Cessioni di crediti derivanti dall'esecuzione del contratto, effettuate nei confronti di soggetti diversi da banche e da intermediari finanziari aventi nell'oggetto sociale l'esercizio dell'attività di acquisto dei crediti ovvero senza l'osservanza delle prescrizioni di forma e di previa notifica della cessione, salva la preventiva accettazione, da parte della stazione appaltante, contestuale alla stipula del contratto.
- Previsione nei contratti di concessione o di finanza di progetto di importo superiore alle soglie comunitarie e di un termine di realizzazione di lunga durata, soprattutto se superiore a 4 anni, a fronte anche delle anticipazioni finanziarie effettuate dal concessionario o promotore.
- Esecuzione delle attività affidate al contraente generale direttamente o per mezzo di soggetti terzi in assenza di adeguata esperienza, qualificazione, capacità organizzativa tecnico-realizzativa e finanziaria.
- Aggiudicazione di sponsorizzazioni tecniche di utilità e/o valore complessivo indeterminato o difficilmente determinabile, con individuazione, da parte dello sponsor, di uno o più soggetti esecutori, soprattutto nel caso in cui questi ultimi coincidano con raggruppamenti costituiti da un elevato numero di partecipanti o i cui singoli partecipanti sono, a loro volta, riuniti, raggruppati o consorziati, specie se privi dei prescritti requisiti di qualificazione per la progettazione e l'esecuzione.
- Esecuzione della prestazione oggetto della sponsorizzazione mediante il ricorso a subappalti oltre i limiti imposti per i contratti pubblici ovvero mediante il ripetuto ricorso a sub affidamenti, specie se

in reiterata violazione degli obblighi contrattuali e delle prescrizioni impartite dall'amministrazione in ordine alla progettazione, direzione ed esecuzione del contratto.

2) Settore finanziamenti pubblici[16]

- Richiesta di finanziamento pubblico incompatibile con il profilo economico-patrimoniale del soggetto cui è riferita l'operazione.
- Richiesta di finanziamenti pubblici effettuata anche contestualmente da più società appartenenti allo stesso gruppo, dietro prestazione delle medesime garanzie.
- Utilizzo di finanziamenti pubblici con modalità non compatibili con la natura e lo scopo del finanziamento erogato.
- Costituzione di società finalizzata esclusivamente alla partecipazione a bandi per l'ottenimento di agevolazioni finanziarie, specie se seguita da repentine modifiche statutarie e, in particolare, da cospicui aumenti di capitale, cambiamenti di sede ovvero da trasferimenti d'azienda.
- Richiesta di agevolazioni finanziarie da parte di soggetti giuridici aventi il medesimo rappresentate legale, uno o più amministratori comuni, ovvero riconducibili al medesimo titolare effettivo o a persone collegate (ad esempio, familiare, convivente ovvero associato).
- Richiesta di agevolazioni finanziarie da parte di società costituite in un arco temporale circoscritto, specie se con uno o più soci in comune.
- Richiesta di agevolazioni finanziarie previste da differenti disposizioni di legge da parte di più società facenti parte dello stesso gruppo, in assenza di plausibili giustificazioni.
- Richiesta di agevolazioni finanziarie presentate da professionisti o procuratori che operano o sono domiciliati in località distanti dal territorio in cui sarà realizzata l'attività beneficiaria dell'agevolazione, specie se i predetti soggetti operano come referenti di più società richiedenti interventi pubblici.
- Presentazione di dichiarazioni relative alla dimensione aziendale dell'impresa necessaria per ottenere le agevolazioni pubbliche che appaiono false o carenti di informazioni rilevanti.
- Estinzione anticipata di finanziamento agevolato con utilizzo di ingenti somme che appaiono non compatibili con il profilo economico del soggetto finanziato.

3) Settore immobili e commercio

- Disponibilità di immobili o di altri beni di pregio da parte di nominativi privi delle necessarie disponibilità economiche o patrimoniali, in assenza di plausibili giustificazioni, anche connesse con la residenza del soggetto cui è riferita l'operazione, la sede della sua attività, ovvero in assenza di legami fra il luogo in cui si trovano i beni e il soggetto cui è riferita l'operazione.
  - Acquisto di beni immobili per importi rilevanti da parte di società scarsamente capitalizzate o con notevole deficit patrimoniale.
  - Acquisto e vendita di beni immobili, specie se di pregio, in un ristretto arco di tempo, soprattutto se sia riscontrabile un'ampia differenza tra il prezzo di vendita e di acquisto.
  - Ripetuti acquisti di immobili, specie se di pregio, in un ristretto arco temporale, in assenza di ricorso a mutui immobiliari o ad altre forme di finanziamento.
  - Operazioni di acquisto e vendita di beni o attività tra società riconducibili allo stesso gruppo.
- Svolgimento di attività commerciali soggette a comunicazioni o ad autorizzazioni da parte di nominativi privi delle necessarie disponibilità economiche o patrimoniali, in assenza di plausibili giustificazioni, anche connesse con la residenza del soggetto cui è riferita l'operazione, la sede della sua attività ovvero in assenza di legami con il luogo in cui si svolge l'attività.
  - Acquisto di licenze di commercio per importi rilevanti da parte di società scarsamente capitalizzate o con notevole deficit patrimoniale, in assenza di plausibili giustificazioni connesse con la residenza o la sede dell'attività del soggetto cui è riferita l'operazione.

[16] Le operazioni e i comportamenti inerenti ad attività economiche svolte nei settori degli appalti e dei finanziamenti pubblici devono essere valutati sulla base degli elementi di anomalia indicati per ciascun settore e dei seguenti criteri: incoerenza con l'attività o il profilo economico-patrimoniale del soggetto cui è riferita l'operazione; assenza di giustificazione economica; inusualità, illogicità, elevata complessità dell'attività.

- Richieste di licenze di commercio da parte di società scarsamente capitalizzate o con notevole deficit patrimoniale, in assenza di plausibili giustificazioni connesse con la residenza o la sede dell'attività del soggetto cui è riferita l'operazione.
- Ripetute cessioni di licenze di commercio, in un ristretto arco di tempo, soprattutto se per importi molto differenti.
- Ripetuti subentri in licenze di commercio, in un ristretto arco di tempo ovvero frequente affitto o subaffitto di attività.
- Ripetuto rilascio di licenze commerciali senza avvio dell'attività produttiva.

Al Dirigente _____
_____
_____

(indicare struttura, nome, cognome, indirizzo e-mail istituzionale del dirigente destinatario)

RISERVATA

Oggetto: Rilevazione anomalie ai sensi e per gli effetti del Sistema di Contrasto al Riciclaggio ed al finanziamento del Terrorismo (SiCoRiTe) della Giunta regionale del Lazio.

1. Procedimento/Procedura	*2. (Riportare il procedimento e/o la procedura nell'ambito della quale sono emerse le anomalie oggetto della rilevazione avendo cura di esplicitare tutti i riferimenti utili all'identificazione univoca del procedimento e/o della procedura)* 3.
4. Anomalie rilevate	*5. (Elencare le anomalie emerse nell'ambito del procedimento e/o della procedura avendo cura di utilizzare la terminologia utilizzata nell'ambito della descrizione degli indicatori di anomalia di cui al SiCoRiTe)* 6.
7. **Soggetti coinvolti**	*8. (Elencare persone fisiche e/o giuridiche nei confronti delle quali sono emerse le anomalie oggetto della rilevazione avendo cura di riportare tutti gli elementi utili all'identificazione univoca dei soggetti coinvolti)* 9.

10. Descrizione anomalie rilevate nel contesto oggettivo e/o soggettivo del procedimento	*11. (Descrivere in dettaglio le anomalie rilevate nel contesto oggettivo e/o soggettivo del procedimento avendo cura di riportare ogni informazione utile al raffronto delle stesse con il Provvedimento UIF 23 aprile 2018)* *12.*

Data rilevazione __/__/____

Firma digitale del Responsabile del Procedimento e/o della Procedura

Al Direttore _____

_____

_____

(indicare struttura, nome, cognome, indirizzo e-mail istituzionale del direttore destinatario)

RISERVATA

Oggetto: Analisi anomalie ai sensi e per gli effetti del Sistema di Contrasto al Riciclaggio ed al finanziamento del Terrorismo (SiCoRiTe) della Giunta regionale del Lazio.

13. Procedimento/Procedura	*14. (Riportare il procedimento e/o la procedura nell'ambito della quale sono emerse le anomalie oggetto della rilevazione avendo cura di esplicitare tutti i riferimenti utili all'identificazione univoca del procedimento e/o della procedura)* 15.
16. Anomalie rilevate	*17. (Elencare le anomalie emerse nell'ambito del procedimento e/o della procedura avendo cura di utilizzare la terminologia utilizzata nell'ambito della descrizione degli indicatori di anomalia di cui al SiCoRiTe)* 18.
19. Soggetti coinvolti 20. 21. 22. 23. 24. 25. 26. 27. 28. 29.	*30. (Elencare persone fisiche e/o giuridiche nei confronti delle quali sono emerse le anomalie oggetto della rilevazione avendo cura di riportare tutti gli elementi utili all'identificazione univoca dei soggetti coinvolti)* 31.

32. Descrizione anomalie rilevate nel contesto oggettivo e/o soggettivo del procedimento	*33. (Descrivere in dettaglio l'esito del raffronto delle anomalie emerse nel contesto soggettivo e/o oggettivo del procedimento e/o della procedura con il Provvedimento UIF 23 aprile 2018 avendo cura di evidenziare le motivazioni alla base della proposta di interruzione o di prosecuzione dell'iter di comunicazione dell'operazione sospetta)*
34. Esito analisi anomalie	*35. (Barrare l'esito dell'analisi delle anomalie)* *36.* ☐ 37 38. Proposta interruzione iter comunicazione sospetta ☐ 39 40. ☐ 41 42. Proposta prosecuzione iter comunicazione sospetta *43.*

Data analisi __/__/____

Firma digitale del Dirigente

Al Soggetto Gestore preposto alla valutazione ed alla effettuazione delle comunicazioni concernenti operazioni sospette di riciclaggio e di finanziamento del terrorismo alla UIF

RISERVATA

Oggetto: Formalizzazione operazione sospetta ai sensi e per gli effetti del Sistema di Contrasto al Riciclaggio ed al finanziamento del Terrorismo (SiCoRiTe) della Giunta regionale del Lazio

Procedimento/Procedura	*(Riportare il procedimento e/o la procedura nell'ambito della quale sono emerse le anomalie oggetto della rilevazione avendo cura di esplicitare tutti i riferimenti utili all'identificazione univoca del procedimento e/o della procedura)*
Anomalie rilevate	*(Elencare le anomalie emerse nell'ambito del procedimento e/o della procedura avendo cura di utilizzare la terminologia utilizzata nell'ambito della descrizione degli indicatori di anomalia di cui al SiCoRiTe)*
Soggetti coinvolti	*(Elencare persone fisiche e/o giuridiche nei confronti delle quali sono emerse le anomalie oggetto della rilevazione avendo cura di riportare tutti gli elementi utili all'identificazione univoca dei soggetti coinvolti)*

Descrizione operazione sospetta	*(Descrivere in dettaglio gli elementi oggettivi e soggettivi che caratterizzano l'operazione sospetta acquisiti nell'ambito dell'attività istituzionale, anche alla luce degli indicatori di anomalia di cui al Provvedimento UIF 23 aprile 2018 e di tutte le altre informazioni disponibili avendo cura di evidenziare le motivazioni alla base della formalizzazione dell'operazione sospetta)*

Data formalizzazione __/__/____

Firma digitale del Direttore