DISCIPLINARE PER LA CONDUZIONE DELLE INFRASTRUTTURE E L'EROGAZIONE DEI SERVIZI INFORMATICI DEL DIPARTIMENTO DELLA RAGIONERIA GENERALE DELLO STATO

ALLEGATO E

ATTRIBUZIONE ALLA SOGEI – SOCIETÀ GENERALE D'INFORMATICA S.P.A , DEL RUOLO E DEGLI OBBLIGHI DI CUI ALL'ART. 28 DEL REGOLAMENTO UE 2016/679

1. DEFINIZIONI

Nel presente documento si intende per

- "*Amministrazione*", il Dipartimento della Ragioneria Generale dello Stato destinataria dei servizi erogati dalla Sogei, che riveste il ruolo di *Titolare del Trattamento* e per cui Sogei riveste la qualifica di *Responsabile del trattamento*;
- "*Dati Personali*" qualsiasi informazione relativa a una persona fisica identificata o identificabile (interessato) - ivi inclusi i dati di cui agli artt. 9 e 10 del Regolamento - trattata dal Responsabile del trattamento per conto del Titolare;
- "*Disciplinare*" si intende il Contratto, così citato nel resto del presente documento, comprensivo di tutta la documentazione allo stesso afferente, tra Ministero dell'Economia e delle Finanze - Dipartimento della Ragioneria Generale dello Stato (RGS) e Sogei S.p.A. per la conduzione delle infrastrutture e l'erogazione dei servizi informatici del Dipartimento della Ragioneria Generale dello Stato;
- "*Norme in materia di protezione dei dati personali*" il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento nell'ordinamento nazionale al Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali di cui al D.lgs. 30 giugno 2003 n. 196, come modificato e integrato dal D.lgs. n. 101/2018;
- "*Misure di Sicurezza*" le misure di sicurezza tecniche e organizzative adeguate garantire un livello di sicurezza adeguato al rischio di cui all'art. 32 del Regolamento;
- "*Persone autorizzate al trattamento*" persone che in qualità di dipendenti, collaboratori, amministratori di sistema o consulenti del Responsabile del trattamento e/o del Sub-Responsabile del trattamento sono stati da questi autorizzati al trattamento dei dati personali sotto la loro diretta autorità;
- "*Registro delle attività di trattamento*" o "*Registro*", il registro tenuto dal Responsabile del trattamento di tutte le categorie di attività relative al trattamento svolte per conto del Titolare del trattamento, di cui all'art. 30 del GDPR;

- "*Regolamento*" o "*GDPR*" il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27.04.2016, relativo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
- "*Responsabile iniziale del trattamento*" o "*Responsabile del trattamento*" o "*Responsabile*" ai sensi dell'art. 4, n. 8 del Regolamento, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento individuato per i trattamenti dati di seguito specificati per conto del Titolare o dell'eventuale Contitolare del trattamento, individuato in relazione al Contratto nella società Sogei S.p.A.;
- "*Sub-Responsabile del trattamento*" o "*Sub-Responsabile*" il fornitore o i suoi subappaltatori e subfornitori, individuati con procedura a evidenza pubblica, di cui Sogei S.p.A. si avvale per effettuare eventuali trattamenti di dati personali per conto del Titolare;
- *Titolare del trattamento*" o "*Titolare*" ai sensi dell'art. 4, n. 7 del Regolamento, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali nell'*Amministrazione Cliente*;
- "*Trattamento*" qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma messa a disposizione, il raffronto o l'interconnessione, la limitazione, allineamento o combinazione, la cancellazione o la distruzione;
- "*Violazione dei dati personali (data breach)*" la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

2. ATTRIBUZIONE DEL RUOLO DI RESPONSABILE

PREMESSO CHE

- il Ministero dell'Economia e delle Finanze - Dipartimento della Ragioneria Generale dello Stato svolge i compiti ad essi demandati dalla Costituzione, dalla legge e dai propri atti regolamentari;
- il Regolamento (UE) n. 679/2016 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (d'ora innanzi "Regolamento"); all'art. 28 prevede che "Qualora un trattamento debba essere effettuato per conto del Titolare quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato";
- la Direttiva del Ministro dell'economia e delle finanze n. 118067 del 3 ottobre 2018 detta specifiche disposizioni in materia di trattamento di dati personali;
- con nota prot. 19505 del 6 febbraio 2019, il Ragioniere Generale dello Stato ha nominato l'Ispettore Generale Capo dell'Ispettorato Generale per l'informatica e l'Innovazione Tecnologica, dott. Carmine di Nuzzo, quale Referente Privacy ai sensi del paragrafo 1, ultimo periodo, della citata direttiva del Ministro dell'economia e delle finanze;
- Sogei riveste il ruolo di società in house al Ministero dell'economia e delle finanze, in ragione delle disposizioni di legge e di Statuto che ne regolano l'attività;
- a tale riguardo è stato stipulato il contratto in relazione al quale è necessario procedere alla sottoscrizione di apposito atto di attribuzione a Sogei S.p.A. del ruolo di Responsabile del trattamento dei dati personali ai sensi del citato art. 28 del Regolamento (cd. designazione);
- Sogei S.p.A. presenta garanzie sufficienti in termini di conoscenza specialistica, affidabilità, esperienza e risorse per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del Regolamento, compreso il profilo relativo alla sicurezza del trattamento;
- le premesse formano parte integrante e sostanziale del presente atto.

Ai sensi dell'art. 28 del Regolamento, il Ragioniere Generale dello Stato per conto del Ministero dell'Economia e delle Finanze - Titolare del trattamento dei dati personali, di seguito rappresentato dall'Ispettore Generale Capo dell'Ispettorato Generale per l'informatica e l'Innovazione Tecnologica, dott. Carmine di Nuzzo, quale Referente Privacy dipartimentale,

ATTRIBUISCE A

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

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

- conferma la sua diretta e approfondita conoscenza degli obblighi che si assume in relazione a quanto disposto dal Regolamento e, più in generale, dalle Norme in materia di protezione dei dati personali;
- si obbliga a procedere al trattamento dei dati – laddove questo sia necessario all'esecuzione delle prestazioni affidate – attenendosi in materia di sicurezza dei dati, oltre che al rispetto della normativa vigente in materia di protezione dei dati personali anche, alle istruzioni di carattere generale nonché a ogni altra istruzione documentata concordate con il Titolare.

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

3. ISTRUZIONI

3.1 Elementi essenziali dei trattamenti

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

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

Il tipo di dati personali trattati sono i seguenti:

- dati che permettono l'identificazione diretta;
- dati che permettono l'identificazione indiretta;
- dati rientranti in particolari categorie (dati c.d. "sensibili");
- dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale (articolo 9 Regolamento UE 2016/679);
- i dati relativi a condanne penali e reati: (articolo 10 Regolamento UE 2016/679);
- dati relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geo-localizzazione.

Le categorie di interessati a cui si riferiscono i dati sono i seguenti:

- personale dipendente RGS e familiari;
- personale dipendente di Enti pubblici/istituzioni nazionali e internazionali;
- fornitori esterni di beni e servizi per la P.A. e Professionisti;
- rappresentanti e dipendenti di enti/istituzioni;
- utenti Pubblica Amministrazione;
- docenti corsi formazione;
- personale ausiliario dell'autorità giudiziaria;
- richiedenti attività di verifica amministrativo contabili e giudiziarie.

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

3.2 Obblighi del Responsabile del trattamento

3.2.1 Limiti e termini del trattamento dei dati personali

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

3.2.2 Istruzioni del Titolare

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

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

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

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

3.2.3 Fornitura dei dati al Titolare

Qualora il *Titolare* o soggetto/funzione da esso incaricato/a abbia necessità, per lo svolgimento dei propri compiti istituzionali, di accedere a dati non disponibili attraverso i servizi applicativi, li richiede per iscritto, esplicitando la

tipologia dei dati, la tempistica e la modalità di fornitura, al *Responsabile* il quale è tenuto a renderli disponibili, secondo linee guida da concordare.

3.2.4 Registro dei trattamenti

Il *Responsabile* tiene un *Registro* di tutte le categorie di attività relative al trattamento (o ai trattamenti) svolti per conto del Titolare. Il Responsabile ed il Titolare devono assicurare la coerenza reciproca dei propri Registri.
Il Responsabile mette a disposizione dell'Autorità di controllo il Registro, ove richiesto, dandone al contempo informazione al *Titolare*.

3.2.5 Autorità di Controllo

Il *Responsabile* è tenuto in ogni caso a cooperare, su richiesta, con l'Autorità di controllo nell'esecuzione dei suoi compiti.
Il *Responsabile* si obbliga a cooperare con il *Titolare* al fine di fornire tutte le informazioni, i dati e la documentazione necessaria affinché il Titolare possa adempiere alle richieste dell'Autorità di controllo ovvero qualora si rendessero necessarie informazioni in caso di precontenzioso o contenzioso.

3.2.6 Comunicazione e diffusione di dati

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

3.2.7 Ricorso a Sub-Responsabili del trattamento

Il *Sub-Responsabile* del trattamento dovrà rispettare gli obblighi in materia di protezione dei dati personali imposti al *Responsabile* dalla normativa in materia di protezione dei dati personali e dal *Titolare* con il presente atto e le eventuali ulteriori istruzioni documentate che lo stesso dovesse impartire.
A tal fine il *Responsabile* è autorizzato dal Titolare a designare ai sensi dell'art. 28 del *Regolamento* i fornitori quali *Sub-Responsabili*.
Ai *Sub-Responsabili* verranno imposti, con l'atto di attribuzione del ruolo stesso di Sub-Responsabile ai sensi dell'art. 28 del *Regolamento*- che può essere anche contenuto, ove possibile, nella documentazione della procedura ad evidenza pubblica - i medesimi obblighi e le medesime istruzioni ricevute dal *Titolare*, salvo che la particolare natura del servizio acquisito richieda necessariamente, per la fruizione dello stesso da parte del *Titolare*, l'adesione a condizioni generali inerenti la protezione dei dati personali stabilite dal fornitore.

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

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

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

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

3.2.8 Riservatezza e formazione delle persone autorizzate al trattamento

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

3.2.9 Obblighi del Responsabile nell'ambito dei diritti esercitati dagli Interessati

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

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

3.2.10 Misure di sicurezza

Il *Responsabile*, sulla base delle indicazioni del *Titolare*, adotta le misure richieste dall'art. 32 del Regolamento.

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

Fatto salvo quanto previsto al par. 3.2.7, quarto paragrafo, il Responsabile dovrà operare, rendendo disponibile al *Titolare* ogni utile informazione per il corretto adempimento degli obblighi di cui agli articoli 25, 32 e 35 del *Regolamento*.

Il *Responsabile* adotta e rispetta le misure di sicurezza indicate e predisposte dal *Titolare* e individua, sottoponendole al *Titolare*, misure di sicurezza ulteriori a quelle già in uso, che dovesse ritenere necessarie per garantire un adeguato livello di protezione dei dati personali in relazione all'analisi dei rischi e alla PIA.

3.2.11 Cancellazione e distruzione dei dati

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

3.2.12 Ispezioni e revisione

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

3.2.13 Codici di condotta

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

3.2.14 Violazioni dei dati

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

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

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

3.2.15 Valutazione di impatto

Per svolgere la valutazione d'impatto sulla protezione dei dati personali il *Titolare* può consultarsi con il proprio *Responsabile* della protezione dei dati, ai sensi dell'art. 35, comma 2, del Regolamento.
Il *Responsabile* del trattamento si impegna ad assistere il *Titolare*, a livello tecnico e organizzativo, nello svolgimento della valutazione d'impatto, così come disciplinata dall'art. 35 citato, in tutte le ipotesi in cui il trattamento preveda o necessiti della preliminare valutazione di impatto sulla protezione dei dati personali o del suo aggiornamento, fatto salvo quanto previsto al par. 2.7, quarto paragrafo.
Il *Responsabile* dovrà operare attenendosi alle istruzioni che verranno impartite dal Titolare rendendo disponibile al Titolare ogni utile informazione per il corretto adempimento degli obblighi di cui all'articolo 35 del *Regolamento*.
Il *Responsabile* del trattamento si impegna altresì ad assistere il *Titolare* nell'attività di consultazione preventiva dell'Autorità di controllo prevista dall'articolo 36 del Regolamento.

3.2.16 Modifiche normative

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

3.3 Rinvio

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

L'ispettore Generale Capo dell'IGIT *l'Amministratore Delegato di Sogei*

4. APPENDICE

FLUSSO DI NOTIFICA DI DATA BREACH ALL'AUTORITÀ DI CONTROLLO

Qui di seguito si riporta una descrizione del flusso di notifica delle violazioni dei dati personali che presentino un rischio per i diritti e le libertà delle persone fisiche (*Data Breach*) in conformità a quanto previsto dal *Regolamento*.

Ai sensi dell'articolo 4 paragrafo 12 del *Regolamento* per "violazione dei dati personali" si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

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

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

DESCRIZIONE DEL FLUSSO

Il flusso di notifica all'Autorità di controllo da parte del *Titolare* prevede i seguenti passi:

1. Il CERT Sogei, nel corso della gestione di un incidente di sicurezza, rileva una possibile "violazione dei dati personali" (Data Breach). Il CERT Sogei notifica al *Titolare* (competente struttura di sicurezza informatica o struttura equivalente della stessa) e al RPD della stessa che è in corso la valutazione di un incidente di sicurezza, fornendo, altresì, una prima sommaria descrizione dell'incidente ed assegnando un identificativo univoco allo stesso. Nel caso in cui sia il *Titolare* a rilevare un incidente di sicurezza caratterizzato da una possibile "violazione dei dati personali" (*Data Breach*) che necessita dell'intervento di Sogei, la competente struttura di sicurezza informatica (o struttura equivalente) del Dipartimento RGS informa il CERT Sogei e il proprio RPD. Il CERT Sogei avvia la verifica fornendo eventualmente informazioni aggiuntive a quelle ricevute ed assegnando un identificativo unico ad esso.
2. Il CERT Sogei verifica la presenza o meno della "violazione di dati personali".

3. In caso di esito negativo della verifica, il CERT Sogei termina il processo, notificando al *Titolare* (competente struttura di sicurezza informatica o struttura equivalente della stessa) e al relativo RPD la chiusura dell'incidente caratterizzato dall'identificativo precedentemente comunicato e le motivazioni.

4. In caso di esito positivo della verifica (ossia è stata accertata la "violazione dei dati personali", è stata svolta la relativa valutazione di impatto e stabilita la gravità del rischio per i diritti e le libertà delle persone fisiche secondo il modello adottato e proposto all' Amministrazione Titolare), il CERT Sogei informa immediatamente e senza ritardo la propria competente struttura di vertice (Direttore Security, Safety e Industrial Relations). Quest'ultima, senza ingiustificato ritardo e in modo dettagliato, comunica il Data Breach al *Titolare* (competente struttura di sicurezza informatica o struttura equivalente) e, contestualmente, al RPD della stessa e al RPD Sogei, completando le informazioni di propria competenza di cui al successivo paragrafo 2 e trasmettendone la notifica al *Titolare*.

5. Il *Titolare* che ha ricevuto la notifica di "Data Breach", sentito il proprio RPD, valuta il livello di gravità della "violazione dei dati personali" proposto da Sogei avvenuta sui dati personali contenuti nelle banche dati disponibili nella propria titolarità. Nel caso in cui la "violazione dei dati personali" comporta un rischio per i diritti e le libertà delle persone fisiche, provvede a completare la notifica con le informazioni di propria competenza, di cui al successivo paragrafo 2 e ad inviare la stessa all'Autorità di controllo entro 72 ore dalla conoscenza dell'avvenuta compromissione dei dati personali, dandone contestualmente riscontro alla struttura di vertice Sogei (Direttore Security, Safety e Industrial Relations) e al RPD di quest'ultima. Qualora la notifica all'Autorità di Controllo non sia effettuata entro 72 ore, provvede, altresì, a corredarla con le motivazioni del ritardo.
Eventuali richieste di ulteriori informazioni o modifiche alla notifica all'Autorità di controllo necessarie durante le attività di risoluzione dell'evento saranno concordate tra il *Titolare*, la struttura di vertice Sogei (Direttore Security, Safety e Industrial Relations) e i rispettivi RPD.
Il CERT Sogei dovrà mantenere un'accurata documentazione di tutte le "violazioni di dati personali" registrate, comprese le circostanze ad esse relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione sarà integrata con le eventuali azioni intraprese dal *Titolare* e opportunamente comunicate allo stesso.

NOTIFICA ALL'AUTORITA' DI CONTROLLO

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

Il CERT Sogei inserirà nella notifica le seguenti informazioni, che saranno comunicate al *Titolare*:

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

le seguenti informazioni necessarie saranno inserite a cura del *Titolare* nella comunicazione all'Autorità di Controllo:

1. il nome e i dati di contatto del RPD o di altro punto di contatto presso cui ottenere più informazioni;
2. validazione ed eventuale integrazione della descrizione del CERT Sogei di una probabile conseguenza della violazione dei dati personali;
3. eventuale ulteriore integrazione delle misure di sicurezza indicate del CERT Sogei adottate o di cui si propone l'adozione da parte del *Titolare* per porre rimedio alla violazione di dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
4. i dati organizzativi di riferimento e i relativi recapiti del *Titolare*;
5. il livello di gravità della violazione.
6. l'eventuale comunicazione agli interessati e le relative modalità;
7. qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, le motivazioni del ritardo.

Firmatario1

L'Amministratore Delegato di Sogei

L'Ispettore Generale Capo
Dott. Carmine di Nuzzo

Firmato digitalmente