CONSIGLIO NAZIONALE
DEGLI INGEGNERI

SISTEMA DI GESTIONE DELLA PROTEZIONE DEI DATI PERSONALI

1. PREMESSA

Il presente documento sintetizza l'approccio del Consiglio Nazionale degli Ingegneri riguardo alla protezione dei dati personali, illustrando i principi, i ruoli e le responsabilità, i processi di valutazione del rischio e le attività di monitoraggio che costituiscono un "Sistema di Gestione della protezione dei dati".
Il sistema di gestione della protezione dati si inspira ad un "Plan-Do-Check-Act" con l'obiettivo del miglioramento continuo del livello di protezione dei dati personali e della conformità dell'ente alla normativa applicabile.

2. CONTESTO E PRINCIPI DI RIFERIMENTO

2.1 Il Contesto del titolare

Il Consiglio Nazionale degli Ingegneri (CNI) è un ente di diritto pubblico vigilato dal Ministero della Giustizia che svolge rappresentanza istituzionale degli interessi rilevanti della categoria professionale degli ingegneri. L'ente è disciplinato nell'ordinamento giuridico italiano dalla Legge 1395/1923, dal Regio Decreto 2537/1925, dal Decreto Luogotenenziale 382/1944 e dal DPR 169/2005.
I compiti istituzionali del CNI prevedono, tra gli altri: il ruolo di magistratura di secondo grado nei ricorsi e reclami degli iscritti avverso le decisioni dei Consigli dell'Ordine; l'espressione di pareri, su richiesta del Ministero della Giustizia, in merito a proposte di legge e regolamenti riguardanti la professione; la funzione di referente del Governo in materia professionale.
Il CNI svolge un ruolo di primaria importanza nel promuovere, sviluppare e potenziare il ruolo dell'ingegnere al fine di accrescere la sua incidenza nella società in cui opera ed è impegnato nel perseguire obiettivi di crescita della professione a servizio della collettività e di un sempre maggiore riconoscimento, da parte delle forze politiche e sociali, del ruolo motore dell'ingegnere nei processi di evoluzione e cambiamento.
Il CNI è governato da 15 Consiglieri, tra i quali vengono scelti il Presidente e il Consigliere Segretario.
Per il suo funzionamento l'ente si avvale di dipendenti e collaboratori, ripartititi in settori:

- Settore Giuridico e Banca Dati
- Settore Segreteria ed Affari Generali
- Settore Amministrazione e Personale

L'ente si avvale inoltre di un ufficio di Direzione Tecnica che ha il compito di governare l'infrastruttura IT, avvalendosi anche di fornitori esterni, e di fornire consulenza all'ente su tematiche di ICT e sicurezza informatica.
Il Consiglio riconosce i principi indicati dal Regolamento UE 679/2016 - GDPR e nei relativi considerando, ed in particolare:

- Art.5: *Liceità, correttezza e trasparenza:* i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
- Art.5: *Limitazione della finalità:* i dati vengono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.
- Art.5: *Minimizzazione dei dati:* adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
- Art.5: *Esattezza:* esatti e, se necessario, aggiornati. a tal proposito sono state adottate misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

- Art.5: *Limitazione della conservazione:* conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.
- Art.5: *Integrità e riservatezza:* trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.
- *Considerando 1:* Che i dati riferibili a persone fisiche sono oggetto di tutela da parte dell'Unione Europea e tramite la protezione di dati personali si tutelano le persone fisiche ai quali i dati sono riferiti.
- Art. 24: *Responsabilità del titolare del trattamento:* nell'attuare una protezione efficace dei dati personali, il titolare è chiamato ad effettuare una gestione dei rischi che incombono sui diritti e sulle libertà delle persone fisiche.
- Art. 24: *Responsabilità del titolare del trattamento:* il titolare è chiamato a mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.
- Art. 25: *Privacy by design:* i rischi e le misure di gestione del rischio, devono essere periodicamente rivalutate alla luce dei cambiamenti nell' organizzazione dell'ente, del contesto normativo e della tecnologia.
- Art. 25: *Privacy by Default:* la protezione dei dati personali deve essere garantita per impostazione predefinita.

2.2 Scopo e campo di applicazione

Il sistema di gestione della protezione dei dati personali (SGPD) si applica a tutti i trattamenti di dati riferibili a persone fisiche, effettuati in forma automatizzata o cartacea dal Consiglio Nazionale Ingegneri.

3. RIFERIMENTI NORMATIVI

Il contesto normativo di riferimento è dato dal Regolamento del Parlamento Europeo e del Consiglio numero 679 del 27 aprile 2016 "Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" (*General Data Protection Regulation*, o GDPR). Per le parti di competenza dell'ordinamento italiano, si applica il Decreto Legislativo 196/2003 (cd. "codice privacy"), come modificato dal Decreto Legislativo 101/2018.

4. TERMINI E DEFINIZIONI

Estratto dell'art. 4 - Definizioni del Regolamento UE 679/2016:

1) *«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;
2) *«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;

6) *«archivio»:* qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
7) *«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;
8) *«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;
9) *«destinatario»:* la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
10) *«terzo»:* la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
11) *«consenso dell'interessato»:* qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
12) *«violazione dei dati personali»:* 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;
13) *«dati genetici»:* i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
14) *«dati biometrici»:* i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
15) *«dati relativi alla salute»:* i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
21) *«autorità di controllo»:* l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

Estratto del D. Lgs. 101/2018:
Capo IV (Disposizioni relative al titolare del trattamento e al responsabile del trattamento)
Art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati): il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del

proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

5. RUOLI E RESPONSABILITÀ

5.1 Titolare del trattamento

CONSIGLIO NAZIONALE DEGLI INGEGNERI
Via XX Settembre n. 5
00187 Roma
Cod. Fisc.: 80057570584
Telefono: +39.06.6976701
Fax: +39.06.69767048
Email: *segreteria@cni-online.it*
PEC: *segreteria@ingpec.eu*

In materia di protezione dati, l'organo di governo del CNI approva:
- il presente sistema di gestione per la protezione dei dati personali;
- il registro dei trattamenti svolti in qualità di titolare del trattamento;
- i criteri di assegnazione di ruoli e responsabilità;
- la nomina del Responsabile della Protezione Dati (RDP/DPO);
- l'istituzione e la nomina di un Referente Privacy interno;
- l'istituzione e la nomina di figure di controllo interno (delegati alla protezione);
- le deleghe operative per la gestione e la verifica di vari adempimenti.

5.2 Delegati alla protezione

All'interno della propria organizzazione, il titolare del trattamento istituisce la figura dei "delegati alla protezione", ai quali è demandata parte dei compiti di controllo e supervisione delle attività di trattamento.
I delegati alla protezione sono soggetti interni, dotati di un livello di autonomia che permette loro di:
- verificare il costante rispetto della normativa in materia di protezione dei dati personali;
- verificare il rispetto del sistema di gestione per la protezione dei dati personali;
- collaborare alla definizione e vigilare sul rispetto delle misure tecniche ed organizzative adottate dal titolare del trattamento;
- fornire istruzioni agli autorizzati al trattamento;
- verificare l'operato dei Responsabili del trattamento.

Sono individuati e nominati come "delegati alla protezione" le seguenti figure:
- *Consigliere Segretario:* delegato alla protezione per i trattamenti individuati come di competenza del Consiglio;
- *Responsabile del Settore Amministrazione e personale:* per i trattamenti individuati come di competenza dell'area;
- *Responsabile del Settore Segreteria e affari generali:* per i trattamenti individuati come di competenza dell'area;

- *Responsabile del Settore Giuridico e banca dati:* per i trattamenti individuati come di competenza dell'area.

Le nomine dei delegati alla protezione avvengono tramite designazione personale, con esplicito atto di nomina del Presidente o del Consigliere Segretario. In ragione di esigenza organizzative, tra il personale dell'ente possono essere individuati e nominati ulteriori delegati alla protezione, secondo le modalità indicate.

I delegati alla protezione non sono individuati quali responsabili del trattamento ai sensi dell'art. 28 del Regolamento UE 679/2016.

6. REFERENTE PRIVACY

All'interno della propria organizzazione, il titolare del trattamento designa un referente privacy, con il compito di:

- coordinare e gestire il processo di adeguamento alla normativa applicabile in materia di protezione dati;
- verificare e monitorare lo stato degli adempimenti;
- ricevere le richieste di esercizio dei diritti da parte degli interessati.

7. RESPONSABILE DEL TRATTAMENTO

Sono individuati e nominati come "responsabili del trattamento" soggetto esterni, distinti dal CNI, che effettuino trattamenti di dati personali "per conto" del Consiglio Nazionale degli Ingegneri. Affinché un soggetto esterno diventi responsabile del trattamento sono necessarie due condizioni:

- una decisione del Consiglio, del Presidente o del Consigliere Segretario, di affidare ad un soggetto terzo lo svolgimento di un'attività che comporti il trattamento di dati personali;
- l'esistenza di un'evidenza documentale, atto di nomina, sottoscrizione di un contratto o altro atto giuridico conforme al diritto dello Stato o dell'Unione Europea, che individui la materia disciplinata, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento, come indicato nell' art. 28 del GDPR.

8. AUTORIZZATI AL TRATTAMENTO SOTTO LA DIRETTA AUTORITÀ DEL TITOLARE

Sono nominati "autorizzati al trattamento sotto la diretta autorità del titolare" secondo l'art. 29 del Regolamento UE 679/2016 le seguenti categorie:

- dipendenti dell'ente;
- membri del Consiglio;
- collaboratori e consulenti dell'ente che svolgono attività per l'ente in forma non organizzata.

9. RESPONSABILE DELLA PROTEZIONE DATI

Il titolare del trattamento, riconoscendo di trovarsi nelle condizioni di cui all'art. 37 par.1 del GDPR ha provveduto all'individuazione e alla nomina di un "Responsabile della protezione dei dati personali" (DPO). Rientrano tra i compiti del DPO:

- verificare l'attuazione e l'applicazione della normativa applicabile in materia di protezione dati;
- assistere il Titolare nello svolgimento della valutazione di impatto;
- rappresentare il punto di contatto per l'Autorità Garante per la Protezione dei Dati Personali;
- collaborare alla gestione di una violazione dei dati personali (cd. *data breach*);
- collaborare allo svolgimento di audit, verifiche o ispezioni sull' operato dei Responsabili del trattamento;
- collaborare alla formazione in materia di protezione dati degli autorizzati al trattamento e dei delegati alla protezione in materia di protezione dati.

10. DOCUMENTI DEL SISTEMA DI GESTIONE

Per documentare lo stato della protezione dati il titolare del trattamento adotta le seguenti evidenze documentali

10.1 Registri

Ogni registro ha associato:

- Autore: soggetto o ufficio che cura la redazione e l'aggiornamento;
- Verificatore: soggetto o ufficio che cura la verifica;
- Frequenza di verifica periodica.

Ogni modifica è registrata non appena ne venga a conoscenza l'autore del registro.

Codice documento	Titolo
SGDP-RG-01	Registro delle attività di trattamento (art. 30 par. 1)
SGDP-RG-02	Registro delle attività di trattamento svolte in qualità di responsabile del trattamento (art. 30 par. 2)
SGDP-RG-03	Registro dei responsabili del trattamento
SGDP-RG-04	Registro dei delegati alla protezione
SGDP-RG-05	Registro valutazioni di impatto (art.35)
SGDO-RG-06	Registro delle attività formative
SGDP-RG-07	Registro dei data breach
SGDP-RG-08	Registro degli amministratori di sistema

10.2 Regolamento Interno in materia di protezione dati

Il titolare del trattamento demanda al referente privacy, al DPO, alla direzione tecnica e ad eventuali terzi la stesura e l'aggiornamento di un Regolamento Interno da portare a conoscenza del personale dell'ente.

10.3 Nomine dei delegati alla protezione

I delegati alla protezione sono nominati tramite atto interno del Consiglio Nazionale degli Ingegneri. Ogni singola nomina è conservata a cura del referente privacy.

10.4 Nomine dei responsabili del trattamento

I responsabili del trattamento sono nominati tramite contratto o altro atto giuridico conforme all'ordinamento vigente. Ogni singola nomina è conservata a cura del referente privacy.

10.5 Informative

Il titolare del trattamento demanda al referente privacy, al DPO, alla direzione tecnica e ad eventuali fornitori terzi, la predisposizione delle informative relative alle modalità di trattamento.
I documenti predisposti sono portati a conoscenza degli interessati; una copia è conservata a cura del referente privacy

10.6 Valutazione dei rischi

Il titolare del trattamento demanda al referente privacy, al DPO e alla direzione tecnica la valutazione dei rischi che incombono sui dati personali trattati.
I seguenti documenti certificano l'esecuzione della valutazione dei rischi:

Codice documento	Titolo
SGPD-RM-01	Mappatura dei sistemi di trattamento
SGPD-RM-02	Valutazione dei rischi e contromisure
SGDP-RM-03	Valutazioni di impatto sulla protezione dei dati (art. 35)

11. FORMAZIONE

Il titolare del trattamento demanda al referente privacy, al DPO e alla direzione tecnica la pianificazione di interventi formativi per il personale dell'ente sulla normativa applicabile in materia di protezione dei dati personali e sulle misure tecniche ed organizzative di sicurezza adottate.
Gli eventi formativi e gli argomenti trattati sono riportati nell'apposito registro, richiamato nel precedente punto 10.1, di codice documento SGDP-RG-06.

12. MONITORAGGIO E VERIFICA

Il titolare del trattamento delega al referente privacy, al DPO e alla direzione tecnica il monitoraggio e la verifica periodica dello stato di attuazione del presente modello organizzativo.
E' compito dei soggetti individuati la formulazione di relazioni di sintesi per riportare al titolare del trattamento le criticità, i rischi e le opportunità.

13. RIESAME

Con cadenza annuale, il titolare del trattamento effettua una verifica dei risultati raggiunti e degli indicatori di sintesi individuati dal piano di monitoraggio e verifica.
I soggetti individuati nel presente manuale possono produrre ulteriori evidenze, registri, valutazioni utili a dimostrare la conformità dell'ente, il Consiglio si riserva di valutare l'utilità di quanto proposto.