

Descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del Regolamento¹.

1.1. Ai sensi dell'art. 2, co. 3, del dPCS 38/2020: *“Per i trattamenti dei dati effettuati mediante il sistema informativo della Giustizia Amministrativa, le cui caratteristiche tecniche, strumentali e operative, ivi compreso il profilo della sicurezza, sono stabilite dal Servizio per l'informatica, nonché per i trattamenti che afferiscono all'attività di gestione del personale di segreteria dell'Ufficio servizi, la titolarità dei trattamenti è attribuita all'Amministrazione Consiglio di Stato-Tribunali amministrativi regionali ai sensi di quanto previsto dall'art. 2, comma 3, del D.P.C.S. n. 1 19 del 28 aprile 2020”.*

Si rinvia, pertanto, con riferimento al trattamento dei dati effettuato mediante il sistema informativo della Giustizia Amministrativa, alle misure tecniche e organizzative, anche concernenti il profilo della sicurezza, riportate nel Registro delle attività di trattamento del plesso unitario Consiglio di Stato - Tribunali amministrativi regionali.

Ferma restando la titolarità dell'Amministrazione Consiglio di Stato - Tribunali amministrativi regionali con riferimento al trattamento dei dati aventi le suindicate caratteristiche, il Consiglio di Presidenza adotta per il trattamento, la comunicazione e la conservazione della documentazione recante dati personali, misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio (conformemente a quanto previsto ex art. 32 GDPR).

In particolare, le misure di sicurezza tecniche e organizzative, volte a prevenire danni fisici, materiali o immateriali, alle persone fisiche derivanti dalla violazione dei dati personali, sono declinate in relazione alla tipologia di dato che rileva nel trattamento e all'avvalimento o meno dell'ausilio di strumenti elettronici.

1.2. Il trattamento, la comunicazione e la conservazione della documentazione recante dati personali sono effettuati con l'ausilio di strumenti elettronici. Le misure approntate per la sicurezza dei sistemi e degli strumenti informatici utilizzati dai componenti del Consiglio di Presidenza, dal Segretario, dai magistrati addetti, nell'ambito delle rispettive competenze, e dal personale di segreteria in servizio presso gli uffici in occasione della trasmissione ai destinatari interessati di atti contenenti dati personali sono contenute nelle prescrizioni in materia di sicurezza informatica e nelle condizioni generali di utilizzo delle dotazioni informatiche e degli apparati di telefonia mobile adottate dal Segretariato generale nei confronti del personale amministrativo e di magistratura, cui si rinvia, che prevedono misure tecniche e organizzative per garantire un'adeguata sicurezza dei dati personali da trattamenti non autorizzati o illeciti e dalla perdita, distruzione o danno accidentali degli stessi.

¹ Ai sensi dell'art. 32, co. 1, del GDPR: *“1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:*

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

1.2.1. Al fine di garantire un livello di sicurezza adeguato al “rischio” del trattamento e di escludere o ridurre al minimo possibili impatti negativi sulle libertà e i diritti degli interessati nella raccolta e trattamento dei dati per lo svolgimento dei compiti istituzionali (ferma restando la previsione di cui all’art. 2, co. 3, del dPCS 38/2020), la prima misura e forma di controllo in atto di gestione della sicurezza degli accessi web riguarda proprio il sistema informativo, che veicola le informazioni esclusivamente su canale *https*.

Una successiva fase di controllo è quella che riguarda le informazioni relative ad ogni singolo accesso al sistema, tracciato in conformità con quanto previsto dalla normativa vigente. La documentazione, inserita per l’istruttoria e l’archiviazione in apposite cartelle, ad uso interno e in rete sul NAS, suddivise per argomenti e per commissioni, è costantemente aggiornata dal personale. L’utenza di dominio è rilasciata a ciascun interessato dal Servizio per l’informatica e le credenziali di accesso fornite, configurate con scadenza temporale periodica, sono cambiate dagli utenti in fase di primo accesso. È altresì impostato il blocco di un utente al ripetuto tentativo errato di autenticazione. Una terza fase consiste nella definizione dei livelli di accesso alle cartelle informatiche. All’esito di una valutazione svolta ai sensi dell’art. 5 del GDPR, è definita *ex ante*, in ragione dei compiti attribuiti al personale in servizio presso la segreteria, un’alberatura degli accessi alle cartelle e sottocartelle informatiche in base alla quale specifiche abilitazioni di accesso sono attribuite esclusivamente alle unità assegnate alla segreteria delle Commissioni secondo la competenza per materia, ovvero assegnate con apposito ordine di servizio per il trattamento dei dati che rilevano nei procedimenti disciplinari, di incompatibilità ambientale e di sospensione cautelare dal servizio di magistrati. In tali casi, per l’attribuzione del nome della cartella informatica contenente i dati dell’interessato è utilizzato uno pseudonimo, in modo da non rendere identificabile in via diretta a personale non autorizzato l’identità del magistrato soggetto a procedimento.

La trasmissione di atti, a mezzo di posta elettronica certificata ovvero tramite posta elettronica ordinaria, ai componenti dell’Organo di autogoverno e agli uffici che intervengono nel procedimento di definizione degli affari in trattazione avviene mediante l’adozione di misure di cautela adeguate al tipo di dato personale trattato.

La condivisione della documentazione contenente dati soggetti a regime “speciale” avviene, nei confronti dell’Organo di autogoverno, nelle forme e modalità previste al seguente punto 1.2.2; nei confronti degli uffici della G.A., con le forme e modalità previste al punto 1.3.1.

Ulteriori misure di sicurezza sono, inoltre, adottate in accordo con il Servizio per l’informatica e sono costituite dall’aggiornamento delle dotazioni informatiche e dal collegamento diretto e quotidiano garantito dallo SPI per la soluzione immediata di eventuali problematiche che dovessero interessare la disponibilità e l’accesso informatico ai dati raccolti.

1.2.2. L’Ufficio servizi del Consiglio di Presidenza utilizza un sistema telematico di condivisione della documentazione, degli atti delle Commissioni e del *Plenum*, denominato *Sharepoint*, messo a disposizione dal Servizio per l’informatica nell’ottica di

migliorare la qualità di lavoro del Titolare del trattamento dei dati (il CPGA) e di dematerializzare l'attività dell'ufficio.

Attraverso il caricamento dei documenti sul portale *Sharepoint* da parte del personale di segreteria specificamente autorizzato al trattamento dei dati, è assicurato ai componenti del CPGA, al Segretario e ai magistrati addetti nell'ambito delle rispettive competenze, l'accesso alla documentazione riguardante le questioni trattate in seno alle varie commissioni e dal *Plenum*. All'ufficio del Segretariato generale è garantito l'accesso alla documentazione riguardante le questioni trattate nell'ambito del *Plenum*. Per impostazione predefinita, i dati personali inseriti sul portale *Sharepoint* sono resi accessibili ai soli aventi diritto sopra richiamati e non sono divulgabili a terzi se non con l'intervento volontario della persona fisica che ne ha la disponibilità.

Ferme restando le responsabilità personali di diversa natura connesse alla divulgazione a terzi dei dati conosciuti e acquisiti nell'esercizio delle funzioni, la divulgazione volontaria a terzi dei dati conosciuti e acquisiti dai singoli componenti del CPGA nell'esercizio della funzione non costituisce violazione del trattamento dei dati ai sensi del GDPR e non dà luogo a responsabilità del titolare e dei designati al trattamento per il danno cagionato al terzo. I soggetti che nell'ambito del trattamento vengono a conoscenza di una presunta violazione della normativa sul trattamento dei dati, sono tenuti ad informare tempestivamente il titolare del trattamento, dal quale attenderà le opportune istruzioni ai fini degli adempimenti di cui all'art. 33, comma 2, del GDPR.

Le misure tecniche e organizzative adottate sono riesaminate e aggiornate sulla base degli indirizzi impartiti dal titolare in attuazione di adeguate politiche in materia di protezione dei dati e ferma restando la previsione di cui all'art. 2, co. 3, del dPCS 38/2020.

1.3. Il trattamento e la conservazione della documentazione recante dati personali, ove effettuati senza l'ausilio di strumenti elettronici, sono soggetti a particolari misure di salvaguardia, quali:

- a) custodia in archivi ad accesso controllato e con serratura;
- b) movimentazione dei fascicoli (compresi quelli contenenti la documentazione necessaria per le riunioni del *Plenum*) sotto la vigilanza di personale dell'ufficio con l'ausilio di appositi contenitori;
- c) ritiro a fine seduta della Commissione o del *Plenum* di tutta la documentazione cartacea non trattenuta dai componenti e distruzione mediante apposito strumento.

1.3.1. La trasmissione, agli uffici interessati, della documentazione contenente i dati di cui agli artt. 9 e 10 del GDPR 679/2016 (quali, a titolo esemplificativo, i dati relativi allo stato di salute dei magistrati o di loro congiunti, quelli che emergono da esposti indirizzati al Consiglio di Presidenza o relativi a procedimenti disciplinari, di trasferimento per incompatibilità ambientale e di sospensione cautelare dal servizio a carico di magistrati) avviene su Folium, secondo le proprietà offerte dal citato sistema. In taluni casi permane la trasmissione in busta chiusa e sigillata sui lembi con annotazione, sulla busta, della dicitura "*contiene dati ex artt. 9 e 10 del GDPR 679/2016*". La conservazione è effettuata secondo modalità che ne precludono la visione, in occasione della consultazione di documenti di altro genere, mediante creazione di sottofascicoli in busta chiusa, con sottoscrizione degli stessi Designati al Trattamento.

1.4. Con riguardo alle misure di sicurezza fisica, il controllo accessi fisici ai locali è regolato dalla direttiva del Segretario delegato per il Consiglio di Stato in data 29 aprile 2013, prot. n. 7953, la quale prevede che *"il personale addetto alla reception provvederà a filtrare gli accessi agli uffici, che saranno liberi per magistrati, dirigenti, dipendenti e altri componenti del Consiglio di Presidenza della Giustizia amministrativa ..., mentre per tutti gli altri ospiti dovrà procedersi a registrazione dell'accesso, facendosi consegnare in entrata il documento di identità ed annunciandoli ai dipendenti presso cui si recano (check - in) e successivamente riconsegnando il documento ed annotando l'uscita (check - out)"*.