

Allegato 6 BIS**PRIVACY E ANAGRAFE DELLE/I DELEGATE/I
E DEI GRUPPI DIRIGENTI**

FAC SIMILE

Autorizzazione al trattamento dei dati personali e sensibili degli iscritti CGIL (gestione anagrafe degli iscritti) ai sensi dell'art. 29 del Regolamento UE 2016/679 (Regolamento Privacy)

(Luogo e data) _____

Il/la sottoscritto/a, in qualità di segretario generale della CGIL _____ (es.: territoriale, regionale o categoria nazionale) per il trattamento dei dati delle/gli iscritte/i alla Confederazione, con la presente, ai sensi dell'art. 29 del Reg. UE 2016/679, autorizza il Presidente dell'Assemblea

- _____
- _____
- _____
- _____
- _____
- _____

a compiere le operazioni di trattamento dei dati personali, anche relativi all'iscrizione al sindacato (gestione anagrafe degli iscritti), di titolarità della CGIL, finalizzando esclusivamente tale incarico ad espletare gli adempimenti necessari per lo svolgimento dei Congressi CGIL, in relazione a quanto è previsto dal Regolamento congressuale e dalle nostre finalità statutarie.

Nell'espletamento dell'incarico conferito, e con riferimento alle disposizioni previste dal Regolamento UE, il Presidente dell'Assemblea dovrà:

- 1) procedere al trattamento attenendosi alle vigenti disposizioni in materia;
- 2) garantire la corretta custodia e la riservatezza dei dati stessi, anche al fine di evitare l'accesso da parte dei soggetti non autorizzati;
- 3) non utilizzare in alcun modo e non cedere a terzi e/o diffondere l'anagrafe degli iscritti alla CGIL che, si precisa, non potrà in alcun modo essere utilizzata per fini diversi da quelli sopra indicati;
- 4) tenere riservate tutte le informazioni relative ai dati di cui verrà a conoscenza durante il trattamento;
- 5) porre in essere, seguendo le istruzioni che verranno di volta in volta impartite dal referente privacy, tutto quanto è necessario al fine di consentire all'organizzazione sindacale di assolvere tempestivamente alle richieste formulate dagli interessati in base a quanto è previsto dal Capo III del Regolamento;
- 6) applicare quanto disposto dal referente privacy, o comunque adottare tutte le più idonee misure di sicurezza, al fine di evitare i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito;
- 7) eseguire gli ordini del Garante per la protezione dei dati personali, dell'Autorità Giudiziaria o del DPO della CGIL, salvo che il referente privacy della CGIL non abbia provveduto a comunicare per iscritto al Presidente dell'Assemblea la propria volontà di promuovere opposizione nelle forme e nei termini di rito.

In aggiunta a quanto sopra, il Presidente dell'Assemblea dovrà provvedere ad avvisare immediatamente lo scrivente o il DPO (contattabile all'indirizzo mail privacy@cgil.it) di ogni richiesta, ordine ovvero attività di controllo da parte del Garante per la protezione dei dati personali o dell'Autorità Giudiziaria ai sensi del sopracitato Regolamento UE in relazione ai dati (anagrafe degli iscritti) di titolarità della CGIL.

I dati (anagrafe degli iscritti) dovranno altresì essere cancellati o resi anonimi o riconsegnati all'organizzazione sindacale quando gli scopi per i quali sono stati raccolti si sono esauriti, cioè subito dopo lo svolgimento dei Congressi di competenza della Commissione.

In ogni caso il Presidente dell'Assemblea sopra autorizzato è tenuto al rispetto delle istruzioni in allegato.

Il Segretario Generale

Per ricevuta e per espressa accettazione dell'incarico di cui sopra in data _____

Firma _____

ISTRUZIONI PER IL TRATTAMENTO DEI DATI PERSONALI

1. Dato personale.

Per *dato personale* si intende qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. Sono definiti, in particolare, *dati particolari*, quelle informazioni idonee a rilevare l'origine razziale ed etnica, le convinzioni religiose (es. la scelta dell'8‰), filosofiche (es. la scelta del 5‰), le opinioni politiche (es. la scelta del 2‰), l'adesione a partiti e sindacati, nonché i dati personali idonei a rilevare lo stato di salute (es. referti o prescrizioni mediche), la vita e l'orientamento sessuale, i dati giudiziari e i dati biometrici.

2. Trattamento di dati personali.

Per trattamento si intende qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati. In ogni caso l'elenco non è tassativo.

3. Informativa e consenso dell'interessato.

Lei è tenuto a rendere all'interessato l'informativa al trattamento procedendo alla stampa e alla messa a disposizione della relativa modulistica presente nel *software* gestionale, sottoscrivendo la quale l'interessato presta anche il consenso al trattamento dei suoi dati personali.

Oltre a rispettare eventuali specifiche indicazioni fornite al momento della formazione, Lei è tenuto a procedere alla compilazione della modulistica contenente il consenso dell'interessato chiedendo previamente allo stesso se ritiene di prestare o meno il consenso alle singole condizioni previste dalla modulistica e, solo successivamente, alla stampa della modulistica stessa, sottoponendola alla compilazione dell'interessato e caricandola, scansionata, nel gestionale. In ogni caso anche dopo la relativa compilazione, l'interessato mantiene il diritto di modificare i consensi, nel quale caso Lei è tenuto a stampare il modello corretto e a modificare, a sistema, il relativo *flag*.

In ogni caso non è tenuto a raccogliere un nuovo consenso laddove l'interessato l'abbia già fornito negli anni precedenti. Le si rammenta che l'interessato gode della più assoluta libertà nel prestare il consenso e, quindi, non può in alcun modo coartare la sua volontà.

In ogni caso, se dovessero sorgere contestazioni da parte dell'interessato o in caso di chiarimenti relativi alle modalità di trattamento a Lei non conosciute, dovrebbe rivolgersi solitamente al Suo responsabile, investendolo delle relative problematiche, così come potrà contattare via e-mail il Responsabile della Protezione dei Dati (privacy@cgil.it).

4. Diritti dell'interessato.

Per "diritti dell'interessato" si intende la possibilità da parte dell'utente di richiedere informazioni circa i dati trattati, così come di esercitare qualsivoglia pretesa rispetto ai dati stessi (cancellazione, portabilità, modifica, ecc.).

Nel caso in cui taluno chieda di sapere quali sono i suoi dati trattati, dovrà dargliene notizia oralmente, previa identificazione, oppure, qualora lo richieda, mediante stampa su supporto cartaceo (qualsiasi altra modalità di messa a disposizione -es. invio via mail- dovrà essere concordata con il Suo Responsabile).

Nel caso in cui taluno eserciti diritti differenti o ponga questioni particolari in materia di trattamento di dati personali dovrà darne comunicazione immediata al Suo Responsabile, raccogliendo la relativa richiesta anche mediante annotazione della stessa, specificando all'interessato che riceverà un riscontro al domicilio entro un mese.

5. Misure di sicurezza e organizzative inerenti il trattamento elettronico dei dati.

Nel trattamento automatizzato dei dati è indispensabile osservare le seguenti disposizioni:

- utilizzare, nell'accesso alla rete, ai documenti e ai dati, il codice identificativo personale (CIP) e la parola chiave (PW), mantenendola segreta. Il suo CIP (Codice Identificativo Personale) e la PW (Password) iniziali sono fornite dall'Amministratore Di Sistema (ADS) e Le è fatto obbligo modificare la PW iniziale con una di Sua scelta all'atto del primo accesso; la PW dovrà essere di almeno otto caratteri alfanumerici e non dovrà contenere riferimenti a Lei agevolmente riconducibili (es. iniziali del nome, data di nascita, ecc.). È inoltre fatto obbligo di modificare la PW ogni tre mesi, anche senza richiesta o sollecitazione;
- la PW deve essere mantenuta segreta e memorizzata, senza renderla nota ad alcuno o, comunque senza trascriverla in supporti che ne consentirebbero o agevolerebbero la conoscenza da parte di terzi (es. post-it, trascrizione in supporti presenti sulla Sua scrivania); in caso di conoscenza accidentale da parte di terzi della PW, dovrà provvedere a cambiarla immediatamente o, laddove non sia possibile, dovrà darne immediato avviso al Suo responsabile; le stesse regole appena menzionate valgono anche rispetto a qualsivoglia altro codice di accesso a Sua disposizione (es. PIN per l'accesso al sistema INPS, Agenzia delle Entrate, ecc.)
- in ogni caso di allontanamento dalla postazione di lavoro deve provvedere a spegnere il pc o ad attivare l'apposita funzione di blocco dello schermo anche se è a conoscenza del fatto che, decorso un certo periodo di tempo, tale blocco si attiverà autonomamente;
- non dare alcuna comunicazione a soggetti terzi dei dati trattati, se non su indicazione del Suo Responsabile. Nel caso Lei riceva istanza di accesso proveniente da terzi deve darne immediata comunicazione al responsabile del servizio;
- i supporti di qualsivoglia natura per la registrazione di dati devono essere forniti dall'ADS e, nel caso in cui debbano essere distrutti, dovrà procedervi consegnandoli all'ADS; in ogni caso Le è fatto espresso divieto di salvare dati personali di qualsiasi natura in supporti esterni (es. chiavette USB, pc portabili, ecc.), così come di salvarli in servizi *cloud* e/o di inviarli via e-mail senza l'autorizzazione dell'ADS o del suo Responsabile;
- in caso di trattamento di dati su supporto cartaceo, dovrà provvedere a riporre la documentazione contenente i dati trattati al termine delle operazioni affidate all'interno degli appositi armadi o contenitori messi a disposizione nell'ufficio, chiudendoli a chiave;
- i supporti cartacei contenenti dati personali non possono essere gettati negli ordinari porta rifiuti ma devono essere distrutti attraverso appositi apparecchi trita-documenti o distruggendo i supporti stessi in modo tale che non siano ricostruibili;

- segnalare immediatamente al Suo Responsabile eventi che possano configurare una violazione di sicurezza tale da comportare accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali, conservati o comunque trattati (c.d. Violazione dei Dati Personali quale, a titolo esemplificativo, furti di supporti cartacei o elettronici, smarrimento degli stessi supporti, attacchi *hacker* ai supporti elettronici, ecc.);
- dovrà informarsi sull'identità e sulle qualità personali di chiunque acceda agli archivi e, nel caso in cui l'accedente sia sconosciuto, dovrà informare immediatamente il Suo Responsabile.

6. Misure di sicurezza e organizzative inerenti il trattamento cartaceo, o comunque non automatizzato, dei dati.

Nel trattamento non automatizzato dei dati è indispensabile osservare le seguenti disposizioni e/o prescrizioni:

- i documenti contenenti dati personali (es. i fogli di carta) devono essere custoditi in modo da non essere accessibili a persone non autorizzate. In particolare i documenti contenenti categorie particolari di dati personali devono essere controllati e custoditi in modo che non vi accedano persone prive di autorizzazione (es. custodia in cartelline non trasparenti, faldoni, dossier, armadi o cassetti chiusi a chiave, porte degli uffici chiuse a chiave od assicurate da altri dispositivi di chiusura elettronica, ecc.) e non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative;
- l'archiviazione dei documenti cartacei contenenti categorie particolari di dati personali deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave. Per accedere agli archivi contenenti tali dati fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del proprio Responsabile;
- i documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata. Le copie dei documenti contenenti dati personali che risultino inutilizzate o mal riuscite non devono essere utilizzate come carta da appunti o da riciclo, e devono essere distrutte (non possono essere gettati negli ordinari porta rifiuti ma devono essere distrutti attraverso appositi apparecchi trita-documenti o distruggendo i supporti stessi in modo tale che non siano ricostruibili); in ogni caso le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate ai documenti originali.
- i documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro. In particolare, nell'ipotesi di ricevimento di soggetti o terzi non autorizzati, i documenti eventualmente in utilizzo dovranno essere chiusi e nascosti alla vista dei soggetti non autorizzati, per evitare che questi possano carpire informazioni di soggetti contenuti in tali documenti.
- i fax pervenuti in altro ufficio devono essere ritirati quanto prima; qualora vengano trasmessi via fax categorie particolari di dati personali la persona autorizzata può nel caso in cui lo reputi opportuno, anticipare l'invio chiamando il destinatario della comunicazione al fine di assicurare il ricevimento nelle mani del medesimo, evitando che soggetti o terzi non autorizzati conoscano il contenuto della documentazione inviata.
- è fatto divieto di effettuare copie fotostatiche o di qualsiasi altra natura non autorizzate dal responsabile, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento, se non richiesto ed autorizzato nell'ambito della propria mansione. In tutti i casi in cui vi sia l'autorizzazione, la persona che provvede alla copia avrà cura di assicurarsi che l'originale e la copia vengano prelevate dalla fotocopiatrice e non lasciate in alcun modo incustodite.
- è fatto divieto di sottrarre, cancellare, distruggere senza l'autorizzazione del responsabile, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del Trattamento, se non richiesto dalla propria mansione ed autorizzato nell'ambito della propria mansione.
- nelle comunicazioni telefoniche accertarsi sempre dell'identità del proprio interlocutore al fine di non divulgare dati a soggetti non autorizzati (l'identificazione può avvenire chiedendo all'interlocutore i suoi dati personali di non facile conoscenza quale, a titolo esemplificativo, il codice fiscale o l'indirizzo e-mail dallo stesso precedentemente comunicato).

7. Istruzioni.

Le presenti istruzioni devono essere osservate in ogni fase di lavoro e, comunque, la violazione degli obblighi di riservatezza devono essere rispettati sotto pena di sanzioni penali e di rivalsa civile per ogni danno del quale il titolare e/o il responsabile siano chiamati a rispondere. Lei è tenuto a rispettare le eventuali integrazioni e/o modificazioni comunicatigli in qualsiasi forma, anche verbale o durante eventuali corsi di aggiornamento e/o di formazione tenuti dalla CGIL.

In ogni caso Lei è tenuto a partecipare agli incontri formativi organizzati dalla CGIL, ed è altresì tenuto a prendere visione e leggere con cura:

- il Regolamento sull'utilizzo dei sistemi informatici ed informativi, della posta elettronica e istruzioni al trattamento dei dati;
- la Procedura per la gestione dei casi di violazione dei dati personali.