



ATTO DI NOMINA DEI SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Il sottoscritto **Leonardi Alan** nato a Modena il 12 maggio 1977 C.F. LNRLNA77E12F257X, in qualità di legale rappresentante della Associazione **P.A. CROCE BLU SOLIERA** con sede legale in SOLIERA C.F. 01886480365 Titolare del trattamento dei dati, ai sensi dell'art. 28 del Regolamento Europeo sulla protezione dei dati personali (2016/679).

Premesso che

- connessa al ruolo stesso di volontario/dipendente del Titolare, quale soggetto che tratta dati personali e/o sensibili dei dipendenti/volontari ai sensi dell'art. 4 Regolamento Europeo sulla Protezione dei dati 2016/679, è la qualifica di Incaricato del Trattamento dei dati Personalni quale persona fisica autorizzata al trattamento dei dati personali/sensibili sotto l'autorità diretta del titolare o del responsabile;
- la formalizzazione della suddetta qualifica di Incaricato è indispensabile in quanto legittima il trattamento delle informazioni personali/sensibili nell'ambito delle attività associative; essa è altresì necessaria al fine di evitare ai volontari/dipendenti l'irrogazione di sanzioni civili, amministrative e penali (salvo il caso di dolo o colpa) che, viceversa, potrebbero scaturire nell'ipotesi di trattamento di dati effettuate da soggetti non designati INCARICATI, come previsto dal suddetto art. 30;

Nomina

Cognome e nome	Luogo di nascita	Data di nascita	Cod. Fiscale

quale Incaricato al trattamento dei dati personali/sensibili ex art. 4 Regolamento Europeo sulla Protezione dei Dati (2016/679).

Tale nomina è in relazione alle operazioni di trattamento di dati ai quali ha accesso nell'ambito delle attività che effettivamente svolge nell'Organizzazione.

L'ambito del trattamento consentito è quello relativo alla sua funzione associativa e può essere di volta in volta modificato secondo quanto previsto dall'organizzazione dell'ufficio. Le tipologie di trattamento possono essere Raccolta, Registrazione, Organizzazione, Conservazione, Consultazione, Comunicazione, Elaborazione, Modificazione, Selezione, Estrazione, Raffronto, Utilizzo, Interconnessione. Le categorie di dati personali a cui lei avrà accesso saranno quelle relative alla funzione svolta per il Titolare.

In ottemperanza al Regolamento Privacy UE 2016/679, che regola il trattamento dei dati personali, laddove costituisce trattamento "qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati", ed in relazione al presente atto di nomina, Lei è incaricato¹ al trattamento dei dati personali (tutti quei dati idonei a identificare direttamente o indirettamente una persona fisica) ed eventualmente dei dati appartenenti a categorie particolari (i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale) la cui conoscenza ed il cui trattamento siano strettamente necessari per adempiere ai compiti assegnati.

¹ Incaricati del trattamento: chi "tratta" i dati non può che essere un incaricato. Data la nozione amplissima di "trattamento" (art. 4 comma 1), non c'è dubbio che tutti i dipendenti/collaboratori aziendali che trattano dati personali debbano firmare per presa visione la formale nomina ad incaricati del trattamento, in quanto questa è la precondizione per poter svolgere il

lavoro che contrattualmente sono tenuti a svolgere. Rifiutare la nomina equivale a: non poter "trattare" alcun dato e quindi a non poter svolgere il lavoro per cui si è assunti. Il rifiuto potrebbe pertanto portare: comunque ad una sanzione disciplinare e al limite, alla risoluzione del rapporto di impiego.

Nel trattamento dei dati l'incaricato deve scrupolosamente attenersi alle seguenti istruzioni:

- ✓ trattare i dati in modo lecito e secondo correttezza;
- ✓ raccogliere i dati e registrarli per gli scopi inerenti l'attività svolta;
- ✓ verificare, ove possibile, che i dati siano esatti e, se necessario, aggiornarli;
- ✓ verificare che i dati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Responsabile del trattamento;
- ✓ mantenere la massima riservatezza sui dati di cui si effettua il trattamento;
- ✓ non utilizzare, comunicare o diffondere alcuno dei dati predetti se non previamente autorizzato dal Titolare del trattamento o dal Responsabile;
- ✓ adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato;
- ✓ in caso di allontanamento, anche temporaneo, dal posto di lavoro, l'incaricato dovrà verificare che non vi sia possibilità, da parte di terzi, di accedere a dati personali per i quali sia in corso un qualunque tipo di trattamento, sia cartaceo che informatizzato.
- ✓ In particolare, per quanto concerne l'utilizzo degli strumenti informatici, dovranno essere scrupolosamente osservate le seguenti disposizioni:

• Costruzione delle parole chiave:

Devono avere una lunghezza minima di 8 caratteri alfanumerici, se il sistema consente raggiungere questa lunghezza

Non devono essere basate su informazioni personali, come nomi di membri della famiglia e simili

Sono inoltre da scartare parole o sequenze numeriche del tipo aaaaaaaa, bbbb, 121212, 123456, eccetera.
Sono da scartare parole come sopra, digitate alla rovescia

E' da scartare una qualsiasi delle parole chiave precedentemente indicata preceduta o seguita da una cifra come ad esempio giovanni1, oppure 1giovanni.

• Modifica della parola chiave: la parola chiave attribuita ai singoli incaricati per accedere al proprio computer, deve essere cambiata al primo utilizzo e successivamente almeno sei mesi. Quest'intervallo di tempo deve essere ridotto a tre mesi, se questa parola chiave viene utilizzata per accedere a dati personali sensibili e giudiziari. Si raccomanda comunque vivamente di ridurre al massimo questo intervallo di tempo, perché più esso è breve, minori sono le probabilità che la parola chiave venga in qualche modo compromessa

• Protezione della parola chiave: la parola chiave prescelta non dev'essere condivisa con alcun soggetto, interno o esterno all'Associazione, ivi inclusi i superiori, a qualsiasi livello. Tutte le parole chiavi che sono state generate da un incaricato, devono essere trattate come informazione strettamente riservata. In particolare, ecco un elenco delle cose che non bisogna fare;

Non rivelate una parola chiave attraverso il telefono a chicchessia.

Non scrivete una parola chiave in un messaggio di posta elettronica.

Non rivelate la parola chiave al vostro superiore.

Non parlate di parole chiave di fronte di terzi.

Non date alcuna indicazione in merito al formato ed alla lunghezza della parola chiave, che utilizzate.

Non rivelate la parola chiave a membri della famiglia.

Non rivelate la parola chiave ad un vostro collega di lavoro, mentre voi siete assenti.

Non scrivete la parola chiave su un qualsiasi documento e non nascondetelo in alcuna parte del vostro ufficio.

• Disattivazione del profilo di autenticazione: nel caso l'incaricato non utilizzi il proprio codice identificativo personale e la parola chiave per un periodo superiore a sei mesi, il suo profilo di autenticazione viene automaticamente disattivato. Per riprendere l'operatività, l'incaricato deve prendere contatto con il titolare o responsabile del trattamento di dati personali.

• Accesso agli strumenti elettronici durante una sessione di lavoro: si prescrive di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro qualora l'incaricato debba allontanarsi dagli stessi. Se lo strumento elettronico utilizzato è un personal computer è necessario:

per quanto concerne gli archivi cartacei, l'accesso e consentito solo se preventivamente autorizzato o dal titolare del trattamento e deve riguardare i soli dati personali la cui conoscenza

Quando si utilizza un dispositivo di controllo remoto, si deve accorgersi che il dispositivo di controllo sia sempre copiato su un hard disk, adatto a contenere dati sensibili.

Si faccia sempre attenzione a non dimenetrare i supporti rimovibili all'interno del computer, quando si tratta della copia, si spenga il computer e ci si allontana.

I supporti rimovibili contenenti dati sensibili e guidiziari non devono essere esposti ad estremi temperature e di umidità; in particolare, esso non deve essere lasciato esposto al sole e qualsiasi temperatura ambiente caldo ad uno freddo, o viceversa, con possibile sbalzo di temperatura. I supporti rimovibili contenenti dati sensibili e guidiziari non devono essere esposti ad estremi temperature e di umidità; in particolare, esso non deve essere esposto all'ambiente caldo ad uno freddo, o viceversa, con possibile sbalzo di temperatura. I supporti rimovibili contenenti dati sensibili e guidiziari non devono essere esposti ad estremi temperature e di umidità; in particolare, esso non deve essere esposto all'ambiente caldo ad uno freddo, o viceversa, con possibile sbalzo di temperatura.

Poiché i supporti rimovibili in genere sono particolarmente sensibili ai campi magnetici, per evitare cancellazione o danneggiamento anche accidentalmente dei dati, non devono mai essere avvicinati a campo magnetico, come quello di un altoparlante, oppure lasciato abbandonato nelle vicinanze di trasformatore, come quelli utilizzati nelle lampade da tavolo, in quanto i campi dispersi potrebbero danneggiare il contenuto.

I supporti rimovibili contenenti dati sensibili e guidiziari devono essere sempre direttamente personalmente custoditi dall'incaricato che ha realizzato la copia.

Per evitare l'alterazione dei dati in questione, dopo la copia su supporto, si attivi la protezione dei possibili nuove scitture, che potrebbero alterare i dati stessi. Per evitare la perdita dei dati in questione, dopo la copia su supporto, si attivi la protezione dei possibili nuove scitture, che potrebbero alterare i dati stessi. I supporti rimovibili devono essere contrassegnati da un'etichetta, con una indicazione in chiaro e codice, tale da permettere all'incaricato di riconoscere immediatamente il loro contenuto ed evitare errori. I supporti confondibili con altri supporti probabilmente in suo possesso ebbi possa confondere con altri supporti probabilmente in suo possesso.

chiave durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati multus) e trattamenti non consentiti in particolare, assi devono essere considerati in cassetti chiavi di utente debitamente formattate prima di altri file, che potrebbero essere infettati da un altro, e sempre bene provvedere alla formattazione ex novo, prima di registrare dati.

- Supporti rimovibili (chiavette usb, memorie esterne), contenenti dati personali

