CRUSO
STUDIO LEGALE

Avv. Davide Richetta

Avv. Donatella Roviello

daviderichetta
claradealexandris
andreapanero
marcomazzù
yleniaserra
riccardocorleone
angelafigone
donatellaroviello
irenedisanto
lauraolivero

FONDAZIONE ACCORSI-OMETTO

SISTEMA DI GESTIONE DELLA PRIVACY EX REG. UE 679/16 (GDPR) e D.lgs 196/03 (così come modificato dal D.lgs 101/18)

MANUALE INFORMATIVO SULLE LINEE GUIDA PER IL TRATTAMENTO DEI DATI PERSONALI DELLE PERSONE FISICHE

c.so re umberto 56
10128 torino
tel 011.191.171.24
tel 011.192.138.90
fax 011.192.138.93

daviderichettavvocato@gmail.com
info@donatellaroviello.it

Fondazione Accorsi - Ometto
TORINO
Museo di Arti Decorative

MANUALE INFORMATIVO SULLE LINEE GUIDA PER IL TRATTAMENTO DEI DATI PERSONALI DELLE PERSONE FISICHE

1. PREMESSA E SCOPO DEL MANUALE

Seppur non prescritto dall'attuale normativa di riferimento, si ritiene utile la redazione del presente manuale volto a esporre le linee guida per il trattamento dei dati personali delle persone fisiche da parte della Fondazione ACCORSI-OMETTO.

2. NORMATIVA DI RIFERIMENTO

Il presente Manuale è predisposto alla luce della vigente normativa di riferimento in materia di protezione dei dati personali, ovvero il Regolamento Europeo 2016/679 – di seguito GDPR - recante disposizioni per la protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione degli stessi, nonché la normativa di adeguamento nazionale (d.lgs 196/03 così come modificato dal d.lgs 101/18).
Le revisioni periodiche del sistema saranno occasione, fra l'altro, per l'ulteriore adeguamento ad eventuali previsioni legislative nazionali future.

3. DEFINIZIONI

Di seguito le principali definizioni contenute nell'art. 4 del GDPR:
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;
3) **«limitazione di trattamento»**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
4) **«profilazione»**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una

persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) **«pseudonimizzazione»**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

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 4.5.2016 IT Gazzetta ufficiale dell'Unione europea L 119/33 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;

16) **dati particolari:** i dati particolari, anche detti sensibili, sono quelli che, ai sensi dell'art. 9 GDPR, rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, i dati biometrici intesi ad identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona; il trattamento di tali dati è vietato se non derivante da obblighi di legge, dagli specifici casi previsti dall'art. 9 GDPR ovvero se l'interessato non ha prestato il proprio consenso esplicito.

4. PRINCIPI GENERALI SUL TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali secondo le modalità stabilite dal GDPR e seguite nel presente manuale si ispira ai seguenti principi e criteri:

a. Principi di liceità e correttezza del trattamento nei confronti dell'interessato.

Il trattamento è lecito soltanto quando:

i. l'interessato ha prestato un consenso informato;
ii. quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte;
iii. quando il trattamento è necessario per adempiere un obbligo legale a cui è soggetto il titolare del trattamento;
iv. quando lo stesso è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
v. quando è necessario per l'esecuzione di un compito di interesse pubblico o per il perseguimento del legittimo interesse del titolare del trattamento.

b. Principio di trasparenza

Il GDPR richiede che i dati siano facilmente accessibili e che le comunicazioni relative al trattamento siano comprensibili. La trasparenza, peraltro, è anche un diritto dell'interessato.

c. Principio di limitazione delle finalità dei dati

Il GDPR prescrive che la raccolta dei dati degli utenti dovrà avvenire soltanto per finalità determinate, esplicite e legittime, e che il trattamento conseguente a tale raccolta dovrà essere effettuato con modalità compatibili con tali finalità.

d. Principio di minimizzazione dell'uso dei dati

La richiesta dei dati deve essere adeguata, pertinente e limitata a quanto necessario per il perseguimento delle finalità per cui i dati sono raccolti e trattati.

e. Principio di esattezza dei dati:

I dati raccolti dovranno essere esatti e, se necessario, aggiornati. Di conseguenza la Fondazione ACCORSI-OMETTO adotterà tutte le misure che riterrà opportune per modificare, rettificare e/o cancellare e tempestivamente eventuali dati inesatti rispetto alle finalità per le quali sono trattati.

f. Principio della limitazione della conservazione

I dati saranno conservati esclusivamente per il tempo necessario al raggiungimento delle finalità per le quali sono trattati, fatti salvi gli obblighi previsti ex lege.

g. Principio dell'integrità e della riservatezza

I dati dovranno essere sempre trattati in maniera da garantire una sicurezza adeguata, cioè adottare misure di sicurezza tecniche ed organizzative idonee a proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale.

h. Principio di accountability

E' il principio di responsabilizzazione; il GDPR richiede che il Titolare del trattamento adotti misure tecniche e organizzative non solo adeguate a garantire che il trattamento sia conforme alla normativa vigente ma anche idonee a dimostrare tale idoneità nei confronti di tutti gli stakeholders.

A tale principio risponde la scelta della Fondazione di predisporre un apposito sistema di gestione della privacy, racchiuso nel presente Manuale nonché nei documenti ad esso allegati.

5. FINALITA', INFORMATIVA E CONSENSO

Nello svolgimento della propria attività l Fondazione ACCORSI-OMETTO tratta dati personali delle persone fisiche per le seguenti finalità:

- **dati dei dipendenti, collaboratori e consulenti esterni**: per finalità di gestione del rapporto di lavoro e di organizzazione dell'attività della Fondazione;
- **dati di fornitori** (**prestatori di beni o servizi)**: per finalità di gestione del rapporto di prestazione di servizi o di merci e per l'adempimento degli obblighi derivanti dal contratto e per finalità contabili e fiscali;
- **dati dei clienti**: per finalità di adempimento degli obblighi precontrattuali e contrattuali, per finalità amministrative, contabili e fiscali e per finalità di aggiornamento sulle proposte commerciali;

- **dati dei soggetti che si iscrivono alla newsletter sul sito Internet della Fondazione:** per informare il richiedente sulle attività della Fondazione;

Informativa all'interessato: è sufficiente quando i dati dell'interessato vengono trattati per obbligo di legge o per la prestazione del servizio oggetto del contratto.

Consenso dell'interessato: è necessario quando si trattano dati particolari ex art. 9 GDPR ovvero per finalità diverse dalla prestazione oggetto del contratto; Il consenso deve essere prestato **liberamente** e per valutare se il consenso sia stato liberamente prestato si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto (art. 7 par. 4 GDPR).

6. DIRITTI DELL'INTERESSATO

a. L'informativa all'interessato sui suoi diritti

A norma dell'art. 13 del GDPR, l'interessato o la persona presso la quale sono raccolti i dati personali devono essere previamente informati oralmente o per iscritto circa:

- le finalità e le modalità del trattamento cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di conferimento;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- i diritti previsti dal GDPR;
- gli estremi identificativi del titolare.

b. I diritti che possono essere esercitati dall'interessato

I diritti che l'interessato può esercitare si possono suddividere in tre categorie:

- il diritto di conoscere quali dati personali sul proprio conto il titolare possieda;
- il diritto di controllare tali dati;
- il diritto di resistere ed opporsi al trattamento, in tutto o in parte.

In particolare l'interessato può:

- chiedere la conferma del fatto che sia o meno in corso un trattamento di dati personali che lo riguarda e da parte di chi;
- ottenere l'accesso ai suddetti dati e alle informazioni circa le finalità del trattamento, le categorie dei dati personali, i destinatari o le categorie di

destinatari a cui i dati personali sono stati o saranno comunicati, il periodo di conservazione;

- ottenere la rettifica o la cancellazione dei dati, la limitazione del trattamento od opporsi al trattamento stesso;
- il diritto di proporre reclamo al Garante per la Privacy o a qualsiasi altra autorità di controllo competente;
- qualora i dati non siano stati raccolti presso l'interessato, il diritto di ottenere ogni informazione disponibile sulla loro origine;
- ottenere la portabilità dei dati, ossia riceverli da un titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e trasmetterli ad un altro titolare del trattamento senza impedimenti;
- qualora il trattamento sia basato sul consenso al trattamento dei dati prestato dall'interessato, il diritto in qualsiasi momento di revocare il predetto consenso, senza che ciò pregiudichi la liceità del trattamento dei dati trattati prima della revoca stessa;

c. Modalità di esercizio dei diritti da parte dell'interessato

L'interessato può rivolgere senza particolari formalità (ad esempio lettera raccomandata, telefax o posta elettronica) la propria richiesta al Titolare o al Responsabile del Trattamento.
L'interessato deve dimostrare la propria identità, sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibendo il documento di riconoscimento ovvero allegando copia dello stesso se la richiesta è inoltrata via posta o con mezzi analoghi.

d. La risposta all'interessato

Il riscontro alla richiesta, da parte del Titolare, o da soggetto dal medesimo incaricato, deve essere fornito entro il minor tempo possibile.
Nel caso in cui le operazioni necessarie per un integrale riscontro alla richiesta siano di particolare complessità, ovvero ricorra altro giustificato motivo, il Titolare può informare di tali circostanze l'interessato, entro trenta giorni dal ricevimento della richiesta.
La modalità più idonea, per fornire i dati all'interessato consiste nella loro estrazione e nella successiva consegna allo stesso in formato leggibile.
Di norma vanno quindi fornite solo le informazioni, non i documenti di cui queste sono parte, o i supporti in cui esse sono contenute.
L'interessato non può pretendere di ottenere una copia di tutti i documenti in cui vi sono dati personali a lui riferiti a meno che la legge non disponga diversamente.
Il Titolare può chiedere un contributo spese all'interessato, che non sia eccedente i costi effettivamente sopportati per la ricerca nel caso specifico.

7. SOGGETTI COMPITI E RESPONSABILITÀ

Titolare del trattamento è la Fondazione ACCORSI-OMETTO considerata nel suo complesso di ente giuridico. Alla stessa spetta esercitare il potere decisionale sulle finalità e sulle modalità del trattamento dei dati personali.

Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento; Si tratta di soggetti esterni all'organizzazione del Titolare del Trattamento; vengono nominati tramite formale atto giuridico.

Incaricati del trattamento sono coloro che, all'interno dell'organizzazione del Titolare del trattamento, e sotto la sua direzione, trattano materialmente i dati degli interessati; vengono incaricati tramite formale lettera.

Amministratore di sistema è il soggetto a cui è conferito il compito di sovrintendere al sistema di risorse tecnico-informatiche della Fondazione e di consentirne l'utilizzo, la gestione e la manutenzione, con le opportune misure di sicurezza; egli ha altresì il compito di gestire, attribuire e revocare le credenziali di autenticazione per l'accesso al sistema informatico secondo le indicazioni del Titolare.
L'attribuzione della funzione di Amministratore di sistema deve essere preceduta, da parte del Titolare del trattamento, dalla valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, compreso il profilo relativo alla sicurezza.
La nomina avviene con apposita lettera di incarico.

Responsabile della protezione dei dati personali (DPO) – Tale figura è prevista dagli artt. 37-39 del GDPR.
Nei casi previsti dall'art. 37 GDPR (principalmente quando titolare del trattamento è un'autorità pubblica, quando vi è monitoraggio regolare e sistematico degli interessati su larga scala o trattamento, sempre su larga scala, di dati particolari ex art. 9 GDPR), il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati (DPO).
La Fondazione ACCORSIOMETTO, dopo opportuna valutazione, ritiene che per le attività da essa esercitate non sia necessaria la nomina di un DPO.

8. REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

In ossequio all'art. 30 GDPR la Fondazione ACCORSI-OMETTO tiene il registro dei trattamenti il quale contiene le seguenti informazioni

a. il nome e i dati di contatto del titolare del trattamento le finalità del trattamento;
b. una descrizione delle categorie di interessati e delle categorie di dati personali;
c. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi eventuali destinatari di paesi terzi od organizzazioni internazionali;
d. *ove applicabile*, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 GDPR, la documentazione delle garanzie adeguate;
e. *ove possibile*, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
f. *ove possibile*, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 GDPR.

9. MISURE DI PROTEZIONE DEI DATI PERSONALI

9.1. Finalità e tipologia

I dati personali oggetto di trattamento sono custoditi e controllati in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi:

a) di distruzione e/o perdita e/o modifica, anche accidentale, dei dati stessi;
b) di accesso non autorizzato e/o di trattamento non consentito e/o non conforme alle finalità della raccolta.

9.2. Valutazione dei rischi

Nel valutare l'adeguato livello di sicurezza la Fondazione ACCORSI-OMETTO ha tenuto conto delle situazioni che possono comportare rischi di distruzione, perdita, modifica, divulgazione non autorizzata, trattamento non consentito o non conforme dei dati personali (Art. 32, co. 2 GDPR).

Per la specifica valutazione dei rischi si rimanda al documento “Valutazione dei rischi”.

9.3 Misure di sicurezza adottate alla Fondazione ACCORSI-OMETTO sulla base della valutazione dei rischi effettuata

Per le specifiche misure di sicurezza adottate dalla Fondazione ACCORSI-OMETTO si rinvia all’apposito documento “Sistema di protezioni informatiche e fisiche”.

10. MISURE CONSEGUENTI AD UNA EVENTUALE VIOLAZIONE DEI DATI PERSONALI

In caso di violazione dei dati personali chiunque ne venga per primo a conoscenza informa il Titolare del trattamento senza ingiustificato ritardo.

Ai sensi dell'art. 33 GDPR il Titolare documenta qualsiasi violazione dei dati personali, comprese le circostanze, le conseguenze e i provvedimenti adottati per porvi rimedio.

A meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, il Titolare comunica la violazione al Garante senza ritardo e ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, indicando altresì le misure adottate per porvi rimedio (art. 33 GDPR).

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica con linguaggio chiaro e comprensibile la violazione all'interessato senza ingiustificato ritardo (Art. 34 GDPR).

11. GESTIONE DEL SITO INTERNET

Il sito internet della Fondazione ACCORSI-OMETTO ha carattere prevalentemente informativo e ospita, in una sezione visibile ad ogni utente, l'esposizione dell'informativa ai sensi dell'art 13 GDPR e dei cookies.

12. VIDEOSORVEGLIANZA

La Fondazione ACCORSI-OMETTO è dotata di impianto di videosorveglianza presso i locali del Museo e della biglietteria a tutela delle opere esposte e degli addetti alla biglietteria stessa.

Tutte le telecamere sono adeguatamente segnalate.

Il sistema di registrazione è gestito dagli addetti alla sicurezza in appositi locali non accessibili al pubblico.

Le Informazioni (immagini registrate) vengono mantenute per **7 giorni e poi cancellate per sovrascrittura**. Il periodo di conservazione è fissato nel tempo massimo di una settimana consentito dal punto 3.4 del provvedimento in materia di videosorveglianza 8 aprile 2010 del garante per la protezione dei dati personali per le ragioni indicate nell'apposita sezione del registro dei Trattamenti.

13. CONSERVAZIONE DEI DATI

Salvo quanto previsto al punto 12, il periodo di conservazione dei dati trattati è limitato al periodo utile al perseguimento della finalità del trattamento, fatti salvi gli obblighi di conservazione previsti dalla legge.

I dati sono distrutti con sistemi meccanici o automatizzati che non ne prevedano in alcun modo il recupero.

I dati possono altresì essere cancellati su richiesta dell'interessato sempre che la loro conservazione non sia necessaria per legge.

14. ILLECITI E SANZIONI

Le violazioni alle regole in materia di privacy da parte degli incaricati circa il trattamento di dati personali potranno essere valutate come illeciti disciplinari ed essere come tali sanzionate.

15. DATA BREACH

“Data Breach” è traducibile in italiano con “violazione dei dati personali”.

E’ Una 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.

Una violazione dei dati personali può compromettere la riservatezza, l’integrità o la disponibilità di dati personali.

Per la procedura da seguire in caso di Data Breach si rimanda al documento a disposizione presso la coordinatrice delle attività relative alla protezione dei dati personali delle persone fisiche

16. VERIFICHE E AGGIORNAMENTI

Il Titolare del trattamento, eventualmente coadiuvato dall’Amministratore di sistema ove necessario, effettua verifiche periodiche del sistema di sicurezza della privacy allo scopo di garantirne l’efficacia e l’aggiornamento.

La verifica deve essere documentata attraverso un rapporto scritto da conservarsi a cura del Titolare del trattamento.

La Fondazione ACCORSI-OMETTO si riserva di effettuare verifiche in qualsiasi momento circa il rispetto del GDPR presso i responsabili del trattamento.

La Fondazione ACCORSI-OMETTO si riserva inoltre di effettuare le necessarie verifiche in materia dei dati personali anche ricorrendo a servizi di auditing da parte di studi legali o di società informatiche specializzate.

Torino, 14.10.2022