**DOCUMENTO SULLE ATTIVITA’ DI TRATTAMENTO DEI DATI PERSONALI**

**PER LE ATTIVITA’ DI RICERCA**

**(ai sensi del GDPR 2016/679)**

Titolare[[1]](#endnote-1)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(specificare se ci sono contitolari)* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Responsabile del trattamento dati[[2]](#endnote-2) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Responsabile della protezione dei dati[[3]](#endnote-3)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Responsabile del progetto[[4]](#endnote-4)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Titolo Progetto e descrizione dell’attività

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Data inizio trattamento \_\_\_ /\_\_\_ /\_\_\_\_\_

Data fine trattamento\_\_\_ /\_\_\_ /\_\_\_\_\_

Finalità del trattamento[[5]](#endnote-5):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Incaricati del trattamento[[6]](#endnote-6):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Destinatari a cui i dati saranno comunicati[[7]](#endnote-7):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Modalità di trattamento:

* informatizzato
* manuale

Natura dei dati personali trattati:

* dati personali[[8]](#endnote-8)

*(specificare la tipologia dei dati trattati)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

* dati particolari *(selezionare le voci riportate di seguito)*[[9]](#endnote-9):
* dati che rivelano la posizione geografica
* dati genetici[[10]](#endnote-10)
* dati biometrici[[11]](#endnote-11)
* dati volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo
* altri tipi di dati: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Categorie di Interessati a cui si riferiscono i dati[[12]](#endnote-12):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Indicazione del luogo di conservazione dei dati

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E’ stata effettuata la valutazione d’impatto?[[13]](#endnote-13)

* Si, perché è probabile che il trattamento comporti un rischio elevato per l’Interessato.
* No, perché non è probabile che il trattamento comporti un rischio elevato per l’Interessato.
* No, perché le operazioni di trattamento sono state controllate da un'autorità di vigilanza.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Descrizione delle misure di sicurezza adeguate al caso specifico[[14]](#endnote-14)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Trasferimenti di dati personali verso paesi terzi (se presenti) e la loro identificazione:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Conservazione del documento:**

Il presente documento è archiviato presso la struttura e costituisce parte integrante della documentazione inerente al progetto.

|  |  |
| --- | --- |
| Data | Firma del Responsabile del progetto |

***Note esplicative:***

1. Titolare del trattamento: “la persona fisica giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri (contitolari), determina le finalità e i mezzi del trattamento di dati personali” (art. 4, c. 7 GDPR). [↑](#endnote-ref-1)
2. 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” (art. 4, c. 8 GDPR); per il CNR i responsabili del trattamento sono i direttori delle strutture. [↑](#endnote-ref-2)
3. Il contatto del Responsabile della protezione dei dati del CNR è il seguente: [rpd@cnr.it](mailto:rpd@cnr.it). [↑](#endnote-ref-3)
4. Indicare il responsabile dell’attività di progetto e il laboratorio di afferenza. [↑](#endnote-ref-4)
5. Specificare dettagliatamente le finalità del trattamento dati.

   IMPORTANTE: il trattamento deve avvenire in conformità ai principi stabiliti nell’art. 5 del GDPR:

   *Liceità, correttezza, trasparenza e finalità del trattamento;*

   *limitazione delle finalità;*

   *esattezza e adeguatezza;*

   *minimizzazione;*

   *limitazione della conservazione;*

   *integrità e riservatezza.* [↑](#endnote-ref-5)
6. Incaricato del trattamento: “persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile”. (si evince dall’art. 4 c. 10 del GDPR).

   art. 32 p. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri (art. 32, GDPR).

   IMPORTANTE: è necessario indicare i nominativi degli incaricati del trattamento. Inoltre, nel caso in cui l’incarico venga affidato a persone esterne è necessaria la lettera di incarico firmata dal Direttore. [↑](#endnote-ref-6)
7. 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 L. 119/33 Gazzetta ufficiale dell'Unione europea IT 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”. [↑](#endnote-ref-7)
8. 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 ” (art. 4 GDPR c. 1). [↑](#endnote-ref-8)
9. Il GDPR non parla di dati sensibili, ma di dati “particolari”. Tra i dati particolari rientrano i dati che rivelano “l’origine razziale, etnica, le opinioni religiose, politiche, sindacali, le convinzioni personali, lo stato di salute, l’orientamento sessuale” (art. 9 GDPR).

   Nei dati personali relativi alla salute dovrebbero rientrare (…) i dati riguardanti lo stato di salute dell’interessato che rivelino informazioni connesse alla salute fisica o mentale passata, presente o futura dell’interessato, comprese le informazioni sulle richieste di prestazione di servizi sanitari (…), un numero, simbolo o elemento specifico attribuito per identificare l’interessato in modo univoco a fini sanitari, (…) le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; (…) qualsiasi informazione riguardante, ad esempio, una malattia, l’invalidità, il rischio di malattie, l’anamnesi medica, i trattamenti clinici o l’effettivo stato fisiologico o biomedico dell’interessato, indipendentemente dalla fonte, ad esempio un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro (art. 35 dei “Considerando” GDPR). [↑](#endnote-ref-9)
10. Dati genetici “tutti i dati personali riguardanti le caratteristiche genetiche di una persona fisica che siano ereditarie o acquisite (…) che forniscono informazioni uniche sulla fisionomia o sulla salute dell’individuo considerato, ottenuti in particolare dall’analisi di un campione biologico della persona in questione (art. 4, c. 13 GDPR). [↑](#endnote-ref-10)
11. Dati biometrici: “i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona che ne consentono o confermano l’identificazione univoca, quali l’immagine facciale o i rilievi dattiloscopici” (art. 4, c. 14 GDPR). Es: impronte digitali, immagine del volto, immagine dell’iride. [↑](#endnote-ref-11)
12. Riguardo alle “categorie di interessati”, specificare se si tratta di minori, anziani, persone con particolari patologie ecc…. [↑](#endnote-ref-12)
13. Il Garante ha pubblicato il [provvedimento N. 9058979](https://www.garanteprivacy.it/en/home/docweb/-/docweb-display/docweb/9058979) contenente l’elenco, non esaustivo, delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto, emanato ai sensi dell’art. 35 del GDPR e delle Linee Guida art. 29 WP 248, rev. 01. Nei casi in cui non sia chiaro se sia necessaria una DPIA, il WP29 raccomanda di eseguirla comunque, essendo la valutazione d’impatto uno strumento utile per aiutare i titolari a rispettare la legge sulla protezione dei dati. [↑](#endnote-ref-13)
14. “Sicurezza del trattamento”: 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.

    2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

    3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. [↑](#endnote-ref-14)