

# Documento di valutazione di impatto sul trattamento dei dati personali Checklist

*N.B. Sta nelle facoltà dei compilatori responsabili mettere a disposizione di altri soggetti questo documento, per raccogliere proposte migliorative o commenti.*

## Sommario

<b>INFORMAZIONI GENERALI</b>	<b>2</b>
<b>PRINCIPI GENERALI DI PROTEZIONE DEI DATI</b>	<b>3</b>
TRATTAMENTO CONFORME ALL'ART. 5 DEL REGOLAMENTO – INFORMATIVA E RACCOLTA CONSENSO	3
LEGITTIMITÀ E MODALITÀ DI TRATTAMENTO	3
CORRETTEZZA ED ACCURATEZZA DEL TRATTAMENTO	4
PERIODO DI CONSERVAZIONE DEI DATI	5
ESERCIZIO DEL DIRITTO DI ACCESSO	6
<b>SICUREZZA DEL TRATTAMENTO E DEI DATI</b>	<b>8</b>
POLITICHE DI SICUREZZA	8
PROCEDURE DI EMERGENZA E CONTINGENCY PLANNING	9
TRASFERIMENTO ALL'ESTERO DI DATI PERSONALI	9
LA SCELTA DELL'INCARICATO DEL TRATTAMENTO	10
LA SCELTA DEL RESPONSABILE DELLA PROTEZIONE DEI DATI - DPO	10
<b>CONCLUSIONI</b>	<b>11</b>

# INFORMAZIONI GENERALI

<i>Tema</i>	<i>Spazio per la compilazione</i>	<i>Commenti e chiarimenti</i>
Azienda od ente che elabora il documento	FONDAZIONE LIMPE PER IL PARKINSON ONLUS	Nulla da segnalare - nds
Titolo del progetto cui si riferisce la valutazione di impatto	GDPR	L'identificazione del progetto non deve lasciar spazio a dubbi
Altri elementi identificativi del progetto	nds	nds
Eventuale aggiornamento od estensione di progetto già in corso, che non richiedeva valutazione di impatto	nds	È possibile che ci si trovi davanti alla situazione indicata, quando un progetto già in corso non richiedeva una valutazione di impatto- in questo caso, descrivere le modifiche che richiedono la elaborazione della valutazione
Eventuale aggiornamento od estensione di valutazione di impatto afferente a progetto già in corso	nds	
Breve descrizione delle ragioni per cui si ritiene di dovere compilare una valutazione di impatto	Compliance al Reg UE 67-2016	Si legga attentamente il regolamento e si citino i punti rilevanti
Responsabili della compilazione del documento e ruolo nel progetto	PITINGOLO MARIO (LR) PATUSSO ANDREA (PM) _____ _____	Devono apparire i nomi e cognomi e, se è coinvolta una persona giuridica (ad esempio con il ruolo di incaricato del trattamento), i nomi dei legali rappresentanti; non dimenticarsi dei corresponsabili
Contatti con i responsabili – telefono, fax, posta elettronica, altro	comitatoeventilimpe@pec.it	nds

# PRINCIPI GENERALI DI PROTEZIONE DEI DATI

## *Trattamento conforme all'art. 5 del regolamento – informativa e raccolta consenso*

<i>Tema</i>	<i>Spazio per la compilazione</i>	<i>Commenti e chiarimenti</i>
Descrivere tutte le categorie di dati personali che vengono trattate	Personali identificativi (anagrafici)	Si presti attenzione ad elencare specificamente eventuali dati sensibili
I dati sensibili sono classificati separatamente rispetto agli altri dati?	Si (sono conservati in archivi separati e protetti)	Dare chiarimenti, sia in caso di risposta affermativa, sia negativa
Sono state individuate le finalità della raccolta e del trattamento?	Si - nelle informative	Dare chiarimenti, sia in caso di risposta affermativa, sia negativa; se le finalità sono diverse, per diverse categorie di dati, dare chiarimenti
Sono state adeguatamente motivate le finalità della raccolta e del trattamento?	Si - nelle informative	Dare chiarimenti, sia in caso di risposta affermativa, sia negativa; se le motivazioni sono diverse, per diverse categorie di dati, dare chiarimenti
Come è stata offerta l'informativa e raccolto il consenso dell'interessato?	In forma scritta	Offrire esempi della modulistica o della informativa via internet, ad esempio, nonché delle modalità di raccolta del consenso
Le modalità di offerta di informativa e raccolta del consenso sono differenziate, in funzione del fatto che ci si trovi davanti a dati sensibili?	Si	I dati sensibili pongono requisiti specifici e più stringenti, ad esempio un consenso esplicito e scritto

## *Legittimità e modalità di trattamento*

<i>Tema</i>	<i>Spazio per la compilazione</i>	<i>Commenti e chiarimenti</i>
Il trattamento è giustificato da disposizioni legislative od amministrative?	Si	Se sì, indicare gli estremi dei documenti di supporto
Il trattamento è conforme ai dettati dello statuto dei lavoratori?	Si	Se no, dare chiarimenti in merito a come il trattamento può esser ricondotto nei ranghi
I dati soggetti a trattamento sono custoditi e controllati dagli addetti al trattamento nel rispetto di regole di riservatezza?	Si	Attenzione: custodire e controllare sono due diverse attività!
Descrivere le istruzioni impartite e gli strumenti a supporto di tali istruzioni, anche in relazione alla distruzione e cancellazione	Formazione - Software di sicurezza - Archivi ad accesso controllato	Ad esempio, formazione in aula oppure on-line, manuali, chiavi USB protette, applicativi crittografici, ecc.

Descrivere le procedure attuate per verificare il rispetto delle istruzioni impartite	Audit semestrale	Ad esempio, auditors, interventi del data protection officer, ecc.
Gli interessati sanno come prender contatto con il responsabile del trattamento?	Si - via mail _____	Illustrare le procedure disponibili e come gli interessati possono conoscerle
Gli interessati sanno come revocare il consenso già espresso, in tutto od in parte?	Si - con richiesta scritta a mezzo e-mail (v. sopra)	Illustrare le procedure disponibili e come gli interessati possono utilizzarle
Nell'ambito di questo progetto, il responsabile del trattamento riceve dati da altri soggetti?	n/a	Descrivere i dati ed i responsabili terzi coinvolti
Nell'ambito di questo progetto, gli interessati sono al corrente che alcuni loro dati possono provenire da altro soggetto?	n/a	Descrivere le modalità di informativa
Nell'ambito di questo progetto, gli interessati sono al corrente delle modalità con cui possono esercitare i loro diritti anche su questi dati?	n/a	Descrivere le modalità di esercizio dei diritti

### ***Correttezza ed accuratezza del trattamento***

<i>Tema</i>	<i>Spazio per la compilazione</i>	<i>Commenti e chiarimenti</i>
Sono in essere delle procedure che permettono di tracciare le modalità di trattamento di tutti i dati personali acquisiti?	Si	Il dato va seguito dall'inizio alla fine, per individuare possibili punti deboli del trattamento
Con che frequenza queste procedure vengono verificate?	Annuale	Occorre trovare un punto di equilibrio tra frequenze troppo diradate, poco credibili, e frequenze troppo ravvicinate, assai penalizzanti
Queste procedure si applicano e sono verificate anche presso soggetti terzi coinvolti nel trattamento, ad esempio incaricati od addetti al trattamento terzi?	Si	
Il progetto in esame prevede il trattamento di dati già acquisiti per nuove finalità?	n/a	
Se sì, come viene informato l'interessato ed eventuali altri soggetti coinvolti, inclusa la autorità nazionale Garante?	n/a	
Quali verifiche sono state condotte, per accertare che le nuove finalità siano compatibili con le finalità originarie?	n/a	

La comunicazione di dati personali a soggetti terzi, ed anche all'interno della azienda, è governata da regole restrittive ed è consentita solo previa verifiche di legittimità?	n/a	Need to know
Come vengono comunicate queste regole ai soggetti coinvolti?	n/a	
Con che frequenza queste regole vengono verificate?	n/a	
Offrire un esempio di come viene determinata la congruità tra i dati acquisiti e le finalità dichiarate	Esame tra prassi interne e informative acquisite	
Con che frequenza tale congruità viene verificata?	Annuale	
Offrire un esempio di come viene valutato il rischio legato all'utilizzo di dati non aggiornati/accurati, e le eventuali conseguenze sull'interessato e/o sul responsabile del trattamento	In base alle modalità di circolazione e diffusione del dato	
Con che frequenza viene verificato l'aggiornamento e l'accuratezza dei dati trattati?	Annuale	
Esiste una registrazione afferente alle sorgenti dei dati ?	n/a	Ad es. l'interessato, altro responsabile, archivi pubblici, ecc.
Qualsiasi segnalazione avanzata dall'interessato, relativa al fatto che i dati non siano aggiornati/accurati, viene esaminata e risolta?	Si	
Viene sempre comunicato all'interessato l'esito della segnalazione?	Si	

### ***Periodo di conservazione dei dati***

<i>Tema</i>	<i>Spazio per la compilazione</i>	<i>Commenti e chiarimenti</i>
In base a quale criterio viene determinata la durata di conservazione dei dati?	Prescrizione fiscale e previdenziale	
Con che frequenza tale criterio viene rivisto?	Annuale	
Il progetto prevede periodi di conservazione differenziati, in funzione della categoria di dati? Se sì, illustrare le ragioni	No	
Il progetto rispetta eventuali disposizioni di legge o di regolamenti, in tema di durata del periodo di conservazione dei dati raccolti?	Sì - le norme fiscali e previdenziali	In caso, riportare i riferimenti appropriati

I dati sono dotati di indicatori, che possano evidenziare fattori afferenti alla durata di conservazione ed eventuale avvio della procedura di cancellazione?	n/a	
Esiste una procedura per gestire un periodo di conservazione più lungo di quello predeterminato?	n/a	Ad esempio, quando i dati debbono esser conservati su indicazione dell'autorità investigativa o giudiziaria
Esiste una procedura dettagliata che illustra le modalità di cancellazione dei dati, su qualsiasi supporto registrati, al termine del periodo di conservazione ed ovunque essi si trovino?	Si - v. misure idonee di sicurezza	Rammentare la norma europea EN15713 – <i>secure destruction of confidential material</i> – Code of Practice
Tale procedura differenzia il livello di distruzione/cancellazione, in funzione della sensibilità del dato?	No	

### ***Esercizio del diritto di accesso***

<i>Tema</i>	<i>Spazio per la compilazione</i>	<i>Commenti e chiarimenti</i>
Esiste una procedura dettagliata che illustra le modalità con le quali un interessato può esercitare il diritto di accesso?	Si – v. informativa	
Esiste una procedura dettagliata che illustra le modalità con le quali è possibile esser ragionevolmente certi di avere recuperato tutti dati di un interessato?	n/a	
Esiste una procedura dettagliata che illustra le modalità con le quali è possibile esser ragionevolmente certi che i dati forniti all'interessato siano decodificati e comprensibili?	n/a	
Esiste una procedura dettagliata che illustra le modalità con le quali vengono eventualmente gestiti e separati i dati riferibili ad interessati terzi?	n/a	
Esistono circostanze nelle quali viene negato ad un interessato l'accesso ad alcuni suoi dati personali? Se sì, con quali motivazioni?	No	
Esiste una procedura che gestisce i trattamenti che potrebbero causare danni fisici e psichici ad un interessato?	n/a	

È stata presa in considerazione la possibilità che tali trattamenti possano esporre l'azienda a richieste di danni?	Si	
Esiste una procedura che consente ad un interessato di negare l'utilizzo dei suoi dati per finalità di marketing diretto?	Si – v. informativa	
Sono in vigore trattamenti automatizzati che possono coinvolgere gli interessati?	No	
Se sì, come vengono informati gli interessati dell'esistenza e delle funzionalità di tali trattamenti automatizzati?	n/a	
Esistono procedure in grado di rispondere a richieste giudiziarie afferenti a: <ul style="list-style-type: none"> <li>● rettifica di dati</li> <li>● blocco di dati</li> <li>● cancellazione di dati</li> <li>● distruzione di dati?</li> </ul>	Si – v. misure idonee	

# SICUREZZA DEL TRATTAMENTO E DEI DATI

## Politiche di sicurezza

<i>Tema</i>	<i>Spazio per la compilazione</i>	<i>Commenti e chiarimenti</i>
Il responsabile del trattamento, di concerto con l'incaricato e con l'assistenza del responsabile della protezione dei dati, ha elaborato una politica di sicurezza dei dati?	No – tali figure non sono presenti, ma la <i>policy</i> è stata delineata nell'adottare le misure idonee	
Se sì, quale è il settore dell'organizzazione aziendale incaricato di attuare tale politica?	n/a	
Quali sono le procedure che tengono sotto controllo il rispetto di tale politica di sicurezza dei dati?	n/a	
La politica di sicurezza ha preso in considerazione l'evoluzione delle tecniche di attacco e difesa ed ha inquadrato tale evoluzione in un contesto economico sostenibile?	Si	
La politica di sicurezza adottata è conforme a norme nazionali od internazionali, applicabili al settore?	n/a	Ad es. EN 27000
La politica di sicurezza adottata è inquadrata in un sistema di certificazione, gestito da un ente di certificazione accreditato per il settore specifico?	n/a	
Quali sono le misure di sicurezza in essere, atte a prevenire un trattamento non autorizzato o non conforme alle finalità della raccolta, per dati residenti: <ul style="list-style-type: none"> <li>• in archivi automatizzati (ad esempio gli archivi delle parole chiave)</li> <li>• in archivi cartacei (ad esempio in classificatori metallici)</li> <li>• in altri archivi e su altri tipi di supporti (ad es. CD, smartphones, BYOD o chiavi USB)?</li> </ul>	Username e password - archivi fisici ad accesso controllato - BYOD con accesso controllato ( <i>username e password</i> )	
I dati sensibili sono protetti con misure di sicurezza di più elevato livello, rispetto a quelle adottate per altri dati?	Si	
Descrivere le procedure che permettono di rilevare violazioni delle misure di sicurezza, sia di tipo fisico, sia di tipo logico, sia a distanza	Firewall - log di sistema - Impianto di allarme anti-intrusione -	



	Servizio di vigilanza nel sito	
--	-----------------------------------	--

### ***Procedure di emergenza e contingency planning***

<i>Tema</i>	<i>Spazio per la compilazione</i>	<i>Commenti e chiarimenti</i>
Esiste un piano di emergenza in grado di fronteggiare possibili eventi critici, di origine naturale, accidentale o criminosa?	Si	
In particolare, descrivere i piani di emergenza applicabili ai seguenti eventi: <ul style="list-style-type: none"> <li>● errore umano</li> <li>● infezione informatica</li> <li>● caduta di rete informatica</li> <li>● furto</li> <li>● incendio</li> <li>● allagamento</li> <li>● altri scenari catastrofici</li> </ul>	Ripristino dati da <i>backup/mirror</i>	

### ***Trasferimento all'estero di dati personali***

E' previsto il trasferimento all'estero di dati personali, verso paesi non appartenenti alla UE?	Si	Attenzione – compilare una tabella per ogni singolo paese
Se sì, quali?	No	
Quali tipi di dati vengono trasferiti?	Contabili, Commerciali e di Prodotto, Personale ( <i>payroll</i> )	
Vengo trasferiti dati sensibili? Se sì, dare dettagli	No	
È stata sviluppata una analisi di rischio per ogni singolo paese ed ogni singola categoria di dati?	Si	
Sono state attuate adeguate e preventive misure di sicurezza, afferenti alle fasi di trasporto e di trattamento di tali dati in paesi terzi?	Si	
L'analisi di rischio viene aggiornata ad intervalli appropriati ed ogniqualvolta cambia lo scenario di trasferimento e/o trattamento?	Annualmente	
È stato fatto un controllo circa il fatto che il trattamento in tali paesi possa esser autorizzato, perché inseriti nella apposita lista elaborata ed aggiornata	n/a	

dalla UE (decisione di adeguatezza ex art. 41)?		
È stato fatto un controllo circa il fatto che il trattamento in tali paesi possa esser consentito, in presenza di garanzie adeguate, ex art. 42?	n/a	
In alternativa, sono state definite delle binding corporate rules, applicabili al trattamento e debitamente sottoscritte dalle parti in causa, ex art. 43?	n/a	
Se il trasferimento avviene verso gli USA, è stato verificato il rispetto delle condizioni stipulate nel EU-USA privacy shield?	n/a	
E' stata verificata la applicabilità dell'art. 43 bis -Trasferimento o divulgazione non autorizzati dal diritto dell'Unione?	n/a	

### ***La scelta dell'incaricato del trattamento***

Quali criteri di selezione sono stati adottati, in fase di selezione dell'incaricato del trattamento?	Competenza specifica - <i>Job description</i>	Competenza specifica, segnalazione da altro responsabile, fattori economici, certificazione, altro
Quali criteri di valutazione sono stati adottati, in fase di verifica dell'attività di trattamento svolta dall'incaricato del trattamento?	Il rispetto dei <i>task</i> assegnati	
Quali tecniche di controllo sono in essere, circa l'attività di trattamento svolta dall'incaricato del trattamento?	Audit annuale	
Esiste una procedura per la gestione di possibili anomalie, rilevate in fase di controllo dell'attività?	Si - assegnazione ad altro incaricato	Penali, trasferimento ad altro incaricato, ecc.

### ***La scelta del responsabile della protezione dei dati - DPO***

Quali criteri di selezione sono stati adottati, in fase di selezione del DPO?	n/a	Competenza specifica, segnalazione da altro responsabile, fattori economici, certificazione, altro
Il contratto prevede termini di durata temporale minima della collaborazione del DPO?	n/a	Verificare dettati del regolamento
Quali criteri di valutazione sono stati adottati, in fase di verifica dell'attività svolta dal DPO?	n/a	

Il rapporto triangolare tra Data controller, Data processor e DPO è formalizzato in un apposito documento?	n/a	
Esiste una procedura per la gestione di possibili anomalie e di recepimento di indicazioni, fornite dal DPO?	n/a	Penali, trasferimento ad altro incaricato, ecc.

## CONCLUSIONI


Esporre in termini discorsivi la sintesi degli elaborati precedenti e le conclusioni cui il responsabile del trattamento è giunto. Questa sintesi può prender in considerazione eventuali interventi migliorativi, da attuare in prosieguo di tempo, con la indicazione di una ragionevole scaletta temporale.

Data e firma del responsabile del trattamento dei dati - data controller

Data e firma dell'incaricato del trattamento dei dati - data processor

Data e firma per presa visione del responsabile della protezione dei dati - DPO

28/04/2023

 RAPSODOO ITALIA SRL