Allegato 1

NOTA ESPLICATIVA AI FINI DELLA COMPILAZIONE DEI DATI RICHIESTI PER LA PREDISPOSIZIONE DEL REGISTRO DEL TITOLARE E DEL RESPONSABILE

Premessa

Nella compilazione occorre far riferimento sempre alle norme del RGPD e alle istruzioni delle Autorità di controllo europee e nazionali. Le presenti indicazioni costituiscono uno mero strumento di supporto.

Intestazione

In fase di compilazione è necessario distinguere se il Registro viene compilato in qualità di **Titolare** del trattamento (art. 30 par. 1 RGPD) oppure di **Responsabile** per conto di altro Titolare (art. 30 par. 2 RGPD). Sono allegati due distinti file excel.

Si ricorda che il Titolare del trattamento è "*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*" (art. 4. par. 1, n. 7 RGPD).

Il Responsabile del trattamento è invece "*la persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento*" (art. 4, par. 1, n. 8 RGPD). Si tratta di un soggetto giuridico, distinto dal Titolare, che svolge su base contrattuale un trattamento per conto del Titolare e nei termini contrattualmente precisati. (art.28 RGPD) Nel caso di trattamenti tra "contitolari" ai sensi dell'art. 26 l'informazione è annotata nella colonna n.8 (si veda avanti).

Ogni Responsabile interno del CNR compila i Registri per i trattamenti svolti, secondo i formati allegati alla presente circolare. Nella compilazione occorre attenersi scrupolosamente a quanto richiesto dall'articolo 30 del RGPD, ad ogni eventuale ulteriore istruzione e linea guida anche delle Autorità di controllo (si veda il sito del Garante per la protezione dei dati personali all'indirizzo www.garanteprivacy.it).

Le indicazioni di compilazione qui fornite rappresentano meri suggerimenti per tendere alla chiarezza e alla uniformità di interpretazione, ferme restando libere le determinazioni dei responsabili interni. Il Responsabile interno è il dirigente, il responsabile dell'ufficio o dell'unità, i cui compiti e funzioni in materia, nel quadro attuale, non sono delegabili.

Per le strutture articolate in più sedi di lavoro, i diversi trattamenti dovranno confluire all'interno dei due registri, evidenziando nell'opportuno campo la sede di lavoro dove

avviene il trattamento.

I Registri, già comunicati a far data dal 25 maggio 2018 e resi disponibili alle attuali strutture per consultazione nella piattaforma informatica, dovranno essere compilati e implementati, rivedendo l'intestazione come sopra descritta, aggiungendo i campi nuovi evidenziati in rosso, eliminando il campo "descrizione del trattamento" (dopo il punto 13) e apportando le circoscritte modificazioni alle denominazioni dei campi.

SUGGERIMENTI PER LA COMPILAZIONE DEL REGISTRO DEL TITOLARE
(foglio Excel all. 2)

1. Sede

Indicare la sede fisica dove è svolto il trattamento nel CNR.

2. Nome banca dati/trattamento

Nel campo indicare la banca dati, l'archivio o una denominazione del trattamento che consenta di individuarlo, es. "gestione delle presenze" (inteso come gestione dei permessi, malattie, ecc.), "gestione del rapporto di lavoro" (inteso come presa di servizio, gestione contratto, ecc.) oppure, ove presente, "titolo/denominazione del progetto".

Nel caso in cui il trattamento censito sia parte di un procedimento complesso, la Struttura deve indicare sia il trattamento gestito in qualità di soggetto erogatore del servizio per tutte le unità dell'Ente, sia il trattamento gestito in qualità di soggetto fruitore del servizio medesimo.

Esempio: gestione dei fornitori attraverso il servizio centralizzato "SIGLA". Nel caso in cui l'ufficio Bilancio effettui acquisti per il proprio funzionamento, l'ufficio stesso dovrà descrivere in un record il trattamento per il pagamento di suoi specifici fornitori (struttura fruitore del servizio centralizzato) e, in un secondo record, il trattamento dei dati SIGLA per la parte di servizio "gestione fornitori" erogato per tutte le strutture dell'Ente (struttura erogatore del servizio centralizzato).

3. Identificativo del progetto e del sotto-progetto (nuovo campo)

Riportare, ove necessario, gli elementi utili a ricondurre i trattamenti alle attività programmate a rilevanza esterna (attività su fondi esterni), quali: il codice identificativo del progetto e del sotto-progetto, acquisibile dall'anagrafica presente nella sezione "Gestione Progetti" (GePro) della Intranet.

4. Eventuali modifiche ed eventi relativi al trattamento specifico

Nel campo devono essere annotate eventuali violazioni e/o altri eventi anche relativi alle modifiche che possono intervenire in un trattamento tenendo conto che lo storico degli aggiornamenti deve essere mantenuto agli atti (sia al centro che a livello periferico). In questo campo andrà annotato: lo stato del trattamento (in essere/sospeso/terminato); se si tratta di un trattamento modificato; se si tratta di un trattamento che è passato da un Responsabile interno ad un altro (es. nuove competenze e funzioni a seguito di riorganizzazione, trasferimento del progetto ecc.); ogni altra vicenda ritenuta utile ai fini del censimento nel Registro.

5. Descrizione delle categorie di dati personali/natura dei dati

Indicare, prima di tutto, se il trattamento include categorie particolari di cui agli artt. 9 e 10 (ex sensibili e giudiziari) o altri dati personali (c.d. comuni).

Specificare inoltre a quali categorie ci si riferisce. Per i dati particolari, ad esempio, indicare se si tratta di dati relativi alla salute, piuttosto che dati biometrici, oppure dati che rivelino opinioni politiche, dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione ecc.

Allo stesso modo, per i dati personali comuni, indicare le categorie, ad esempio precisare se si tratta di dati anagrafici (cognome, nome, sesso, data di nascita, luogo di nascita, codice fiscale), piuttosto che di dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile) oppure dati di pagamento (numero di conto corrente e/o coordinate bancarie e/o dati della carta di credito), dati di profilazione o di localizzazione, ecc.

6. Finalità del trattamento/base normativa

Nel campo "Finalità del trattamento" oltre alla precipua indicazione della stessa, distinta per tipologie di trattamento (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini), sarebbe opportuno indicare anche la base giuridica del trattamento (artt. 6, 2, 9 se applicabile del RGPD). Poiché le amministrazioni pubbliche trattano i dati nell'ambito delle funzioni istituzionali, ai sensi dell'articolo 6, par. 1 lettera e), si dovrebbe indicare anche la legge o il regolamento (se previsto dalla legge) su cui si fonda il trattamento. A titolo esemplificativo, è possibile fare riferimento all'art.2 del d.lgs. 127/2003, agli art.2 e 17 dello Statuto del CNR, ovvero ad altra fonte normativa di riferimento.

Si ricorda che il trattamento è lecito quando ricorre almeno una base giuridica, per cui possono essere indicate ulteriori basi giuridiche tra quelle previste dall'articolo 6. In particolare, per i trattamenti di dati appartenenti alle categorie particolari, occorre rilevare una delle condizioni di cui all'art. 9, par. 2 del RGPD.

7. Descrizione delle categorie di interessati

L'interessato è la persona fisica cui si riferiscono i dati personali. Nel campo vanno specificate le categorie di interessati, ad esempio si deve indicare se si trattano dati relativi a dipendenti/consulenti, minori, persone vulnerabili (vittime di violenza o abusi, rifugiati, richiedenti asilo), cittadini, pazienti, ecc.

8. Categorie di destinatari a cui i dati possono essere comunicati compresi i destinatari di Paesi terzi o Organizzazioni internazionali

In tale campo dovranno essere indicati i soggetti ai quali vengono comunicati i dati personali trattati al fine di specificare il flusso di informazioni.

Ai sensi e per gli effetti dell'art. 4 punto 9) del Regolamento UE 2016/679, per destinatario si intende 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. I destinatari dei dati, quindi, sono i soggetti, siano essi interni o esterni, ai quali i dati personali possono essere comunicati da parte del Titolare del trattamento.

I destinatari possono essere indicati anche semplicemente per categoria di appartenenza (es. enti previdenziali per la trasmissione dei dati dei dipendenti per adempiere agli obblighi contributivi), soggetti ai quali – in qualità di responsabili e sub-responsabili del trattamento– siano trasmessi i dati da parte del Titolare (es. soggetto esterno cui siano affidate in tutto o in parte le attività di trattamento). Occorre altresì indicare eventuali ulteriori responsabili interni al CNR, quando il trattamento è parzialmente svolto da altro Responsabile (es. gestione contabile sistema SIGLA).

In tale campo indicare esplicitamente la presenza di eventuali "Contitolari" e, ove nominati, dei responsabili della protezione dei dati.

Sono contitolari del trattamento due o più titolari che determinano congiuntamente le finalità e i mezzi del trattamento. Nel caso in cui siano individuati uno o più contitolari del trattamento, dovranno essere riportati, per esteso, i relativi riferimenti (nome, contatti telefonici, RPD del contitolare) (art. 26 del RGPD).

Si ricorda che per «Organizzazione Internazionale» si intende: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati (art. 4 par..26).

9. Ove previsto il Trasferimento verso Paesi extra UE o Organizzazioni Internazionali, indicare il Paese o l'Organizzazione Internazionale, le condizioni di cui al Capo V del RGPD e per i trasferimenti di cui al secondo comma dell'art. 49, la documentazione delle garanzie previste

Si ricorda che il RGPD (art.44) subordina ad una particolare disciplina qualunque trasferimento di dati personali oggetto di un trattamento, o destinati a essere oggetto di un trattamento, dopo il trasferimento verso un Paese terzo, o verso un'organizzazione internazionale. Tale disciplina è dettata dal Capo V del RGPD (artt.44-49) e ha lo scopo di assoggettare i trasferimenti fuori dall'area in cui è applicabile il RGPD a garanzie equivalenti.

In tale campo, oltre ad indicare la denominazione del paese extra-UE o dell'organizzazione internazionale verso i quali sono trasferiti i dati personali, va indicata la condizione che autorizza il trasferimento di dati personali verso paesi terzi (al di fuori dell'UE) oppure organizzazioni internazionali. Le condizioni che autorizzano il trasferimento all'estero sono:

- Decisioni di adeguatezza:
    - Trasferimento sulla base di una **decisione di adeguatezza** (art. 45 RGPD);

- Condizioni di adeguatezza:
    - Trasferimento soggetto a garanzie adeguate (art. 46 RGPD);
    - Norme vincolanti di impresa (art. 47 RGPD);
- Deroghe (art. 49 RGPD);
    - Consenso dell'interessato al trasferimento;
    - Esecuzione di un contratto tra titolare e interessato;
    - Esecuzione di un contratto tra titolare e soggetto che agisce per conto dell'interessato;
    - Importanti motivi di interesse pubblico;
    - Accertamento, esercizio o difesa di un diritto in sede giudiziaria
    - Tutela degli interessi vitali dell'interessato o di terzi
    - Predisposizione di un registro normato dal diritto dell'UE O degli Stati membri.

Nel caso in cui non ricorrano le condizioni sopra richiamate il trasferimento è possibile alle condizioni indicate dal 2° comma del paragrafo 1 dell'articolo 49 ma è necessario attestare nel Registro la valutazione relativa alla sussistenza delle condizioni e l'adeguatezza delle garanzie. Sul punto si possono consultare le linee guida 2/2018 del Comitato europeo per la protezione dei dati (European Data Protection Board – EDPD).

10. Descrizione generale delle misure di sicurezza tecniche e organizzative per garantire un livello di sicurezza dei dati personali adeguato al rischio cui gli stessi sono esposti (art. 32 par. 1)

Nel campo andranno indicate le misure tecnico-organizzative adottate dal Titolare ai sensi dell'art. 32 del RGDP tenendo presente che l'elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimessa al Titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere.

Tale lista ha di per sé un carattere dinamico (e non più statico come è stato per l'Allegato B del d.lgs. 196/2003) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l'insorgere di nuovi rischi. Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (es. procedure organizzative interne; security policy ecc.).

11. Valutazione d'impatto (nuovo campo)

Inserire un nuovo campo con l'intestazione "Valutazione di impatto" in cui dovrà essere riportato se è stata effettuata o meno la valutazione di impatto richiesta dall'articolo 35 del RGPD nei casi in cui il trattamento presenti un rischio elevato, specificando [SI] o [NO].

12. I termini ultimi previsti per la cancellazione delle diverse categorie di dati

Indicare, ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati. Qualora non fosse noto il periodo di conservazione indicare quanto meno i criteri utilizzati per determinare tale periodo (cfr. art. 13 par. 2 lett. a RGPD).

Ferme restando le disposizioni specifiche per le tipologie di dati/documenti trattati, si segnala che informazioni sui tempi di conservazione della documentazione amministrativa nel CNR sono contenute nel "**Massimario di conservazione e selezione dei documenti d'archivio**", allegato al Manuale di gestione del sistema di protocollo informatico e della gestione documentale, disponibile al seguente link:

https://www.cnr.it/sites/default/files/public/media/amministrazione_trasparente/altri_contenuti/manuale_gestione/allegato8_massimario.pdf

13. Modalità di trattamento

Indicare se cartaceo, informatico o misto. Ove possibile anche i luoghi fisici (es. stanze, archivi) dove sono conservati i dati trattati, gli strumenti informatici (es. server) utilizzati per il trattamento e la loro ubicazione.

14. Tipologia di Finalità

Ricondurre la finalità del trattamento individuata nel campo n.6 alle seguenti tipologie:

- Gestionale-amministrativa – Struttura erogatrice (servizio centralizzato)
- Gestionale-amministrativa – Struttura fruitrice (servizio centralizzato)
- Ricerca scientifica

15. Responsabili esterni e referenti

Indicare la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, che tratta dati personali per conto del CNR ai sensi dell'articolo 28 del RGPD, sulla base di Convenzione/Accordo/Contratto, nonché il RPD ove nominato. Se esiste una figura interna di riferimento è utile annotarla.

SUGGERIMENTI PER LA COMPILAZIONE DEL REGISTRO DEL RESPONSABILE (foglio Excel all. 3)

1. Sede

Indicare la sede fisica dove è svolto il trattamento nel CNR.

2. Dati di contatto del titolare e dei responsabili del trattamento e, ove applicabile, del responsabile della protezione dei dati

Inserire il nome e i dati di contatto del Titolare, del Responsabile o dei Responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il Responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati.

Ove il Titolare o il Responsabile del trattamento risulti essere un soggetto stabilito in un Paese non appartenente all´Unione Europea, indicare il nome e i dati di contatto del rappresentante dagli stessi designato, incaricato a fungere da interlocutore (art. 27 RGPD).

3. Categorie dei trattamenti effettuati per conto del titolare

Far riferimento a quanto contenuto nel contratto di designazione a Responsabile che, ai sensi dell'art. 28 del RGPD, deve individuare, in particolare, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati oggetto del trattamento, nonché la durata di quest'ultimo.

4. Identificativo del progetto e del sotto-progetto (nuovo campo)

Ove presenti, riportare gli elementi utili a ricondurre i trattamenti alle attività programmate quali: il codice identificativo del progetto e del sotto-progetto stesso, acquisibile dall'anagrafica presente nella sezione "Gestione Progetti" (GePro) della Intranet.

5. Ove previsto il Trasferimento verso Paesi extra UE o Organizzazioni Internazionali, indicare il Paese o l'Organizzazione Internazionale, le condizioni di cui al Capo V del RGPD e per i trasferimenti di cui al secondo comma dell'art. 49, la documentazione delle garanzie previste

In tale campo, oltre ad indicare la denominazione del paese extra-UE o dell'organizzazione internazionale verso i quali sono trasferiti i dati personali, va indicata la condizione che autorizza il trasferimento di dati personali verso paesi terzi (al di fuori dell'UE) oppure organizzazioni internazionali.

Le condizioni che autorizzano il trasferimento all'estero sono:

- Trasferimento sulla base di una decisione di adeguatezza (art. 45 del Regolamento)

- Trasferimento soggetto a garanzie adeguate (art. 46 del Regolamento)
- Consenso dell'interessato al trasferimento
- Esecuzione di un contratto tra titolare e interessato
- Esecuzione di un contratto tra titolare e soggetto che agisce per conto dell'interessato
- Interesse pubblico
- Accertamento, esercizio o difesa di un diritto in sede giudiziaria
- Tutela degli interessi vitali dell'interessato o di terzi
- Predisposizione di un registro normato dal diritto dell'UE

Nel caso in cui non ricorrano le condizioni sopra richiamate o nelle deroghe previste dall'articolo 49, paragrafo 1, primo comma del RGPD, è necessario attestare nel Registro le garanzie adeguate ai sensi del comma 2 dello stesso paragrafo 1.

6. Descrizione generale delle misure di sicurezza tecniche e organizzative per garantire un livello di sicurezza dei dati personali adeguato al rischio cui gli stessi sono esposti (art. 32 par.1)

Nel campo andranno indicate le misure tecnico-organizzative adottate dal Titolare ai sensi dell'art. 32 del RGDP, tenendo presente che l'elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimessa al Titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere.

Tale lista ha di per sé un carattere dinamico (non più statico come è stato per l'Allegato B del d.lgs. 196/2003), dovendosi continuamente confrontare con gli sviluppi della tecnologia e l'insorgere di nuovi rischi. Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure, in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (es. procedure organizzative interne; politiche atte a favorire la sicurezza degli impianti, dei software, misure tecniche ed organizzative di gestione della security, ecc.).

7. Sub-responsabili esterni

Indicare la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del CNR, ai sensi dell'articolo 28 par. 2 del RGPD, previa autorizzazione del Titolare, nonché il RPD ove nominato.