La collana

La collana pubblica linee guida e codici tecnico scientifici, progetti, dispense, presentazioni a conferenze e convegni, versioni preprint, materiali d'archivio del Centro Interdipartimentale per l'Etica e l'Integrità nella Ricerca del Consiglio Nazionale delle Ricerche.

Elena Mancini

Primo tecnologo, coordina la Segreteria scientifica della Commissione per l'Etica e l'Integrità nella Ricerca del CNR. Presso il Centro Interdipartimentale per l'Etica e l'Integrità nella Ricerca del CNR è referente privacy, responsabile scientifico dell'Unità di Ricerca su Etica e Privacy e del WP Bioetica del progetto di CNCCS, "Centro per la ricerca di nuovi farmaci per le malattie rare, trascurate e della povertà", Docente in bioetica per l'insegnamento Principi di bioetica e deontologia, principi di diritto ed economia aziendale (Sapienza) è coordinatore del Comitato bioetico per la veterinaria e l'agroalimentare dell'omologo Istituto.

Daniela Niccoli

Già Primo Tecnologo presso la Direzione Generale del CNR, è ricercatore associato del Centro Interdipartimentale per l'Etica e l'Integrità nella Ricerca del CNR con responsabilità sull'implementazione di norme, regolamenti e codici di interesse etico-deontologico, in particolare sulla protezione dei dati. Collabora con il Direttore Generale del CNR in qualità di esperto in materia giuridico-amministrativa nonché per l'elaborazione degli strumenti e delle procedure in applicazione del Regolamento (UE) 2016/679 RGPD. Fino al 2007 ha fatto parte dei ruoli del MUR presso lo Staff prima del Direttore Generale dell'Università e successivamente del Capo del Dipartimento dell'Università e della Ricerca.

Cinzia Caporale

Coordinatore del Centro Interdipartimentale per l'Etica e l'Integrità nella Ricerca del CNR e dell'omonima Commissione. Componente del Comitato Nazionale per la Bioetica dal 2002 e del Comitato Etico Nazionale per le sperimentazioni cliniche relative alle terapie avanzate. È stata due volte Presidente del Comitato Intergovernativo di Bioetica dell'Unesco. Ha presieduto il Comitato Etico dell'INMI L. Spallanzani e il Comitato etico unico nazionale per le sperimentazioni su Covid-19. È membro della Consulta scientifica del Cortile dei Gentili (Pontificio Consiglio della Cultura) e Presidente onorario del Comitato Etico della Fondazione Umberto Veronesi.

ISSN 2785-4779

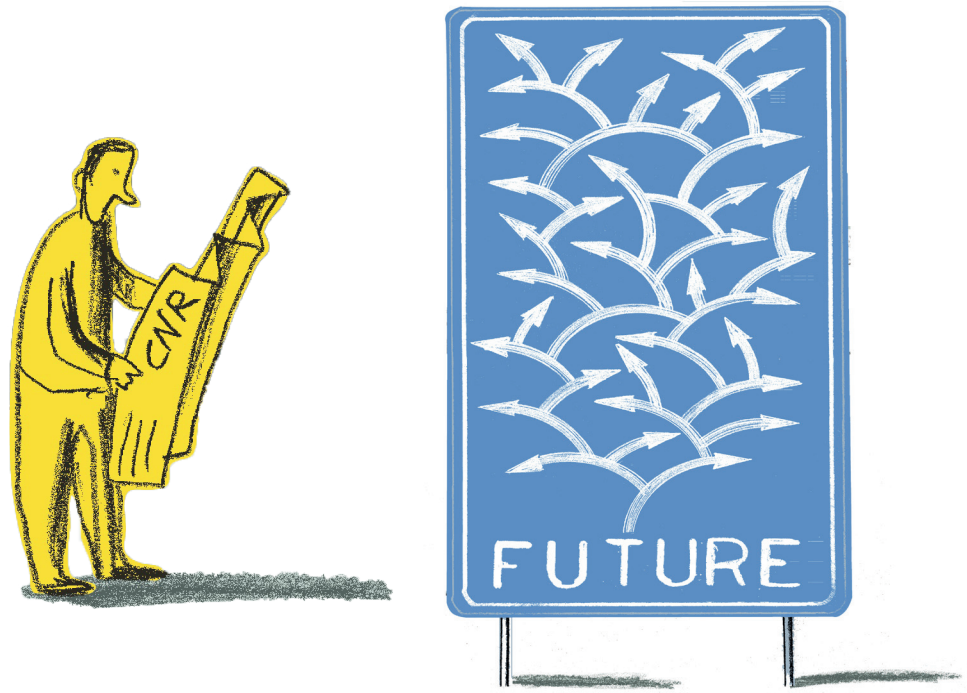
Collana di Rapporti Tecnici e di Ricerca
Technical and Research Reports Collection

6, 2023

Misure organizzative per la protezione dei dati

(ai sensi degli artt. 24 e 25 del Reg. UE 2016/679)

di Elena Mancini, Daniela Niccoli e Cinzia Caporale



Collana di Rapporti Tecnici e di Ricerca
Technical and Research Ethics Collection
6, 2023

CID ETHICS
Centro Interdipartimentale per l'Etica e l'Integrità nella Ricerca

Misure organizzative per la protezione dei dati

(ai sensi degli artt. 24 e 25 del Reg. UE 2016/679)

di Elena Mancini, Daniela Niccoli e Cinzia Caporale

Centro Interdipartimentale per l'Etica e l'Integrità nella Ricerca
Consiglio Nazionale delle Ricerche

elena.mancini@cnr.it
daniela.niccoli@cnr.it
cinzia.caporale@cnr.it

Collana di Rapporti Tecnici e di Ricerca
Technical and Research Ethics Collection

Direttore scientifico
Cinzia Caporale

Responsabile di redazione
Annarita Liburdi

Comitato di redazione
Giorgia Adamo, Tiziana Ciciotti *(impaginazione del testo),* Paola Grisanti, Emiliano Liberatori

Cura editoriale
Marco Arizza

Ha funzioni di comitato scientifico della Collana la Segreteria scientifica della Commissione per l'Etica e l'Integrità nella Ricerca del CNR.

Per informazioni:
info@ethics.cnr.it

Editore
CNR - Centro Interdipartimentale per l'Etica e l'Integrità nella Ricerca
Via dei Taurini, 19 - 00185 Roma

ISSN: 2785-4779

In copertina immagine tratta da un'illustrazione di Guido Scarabottolo, per gentile concessione dell'autore.

INDICE

Abstract

Il presente rapporto tecnico nasce dall'esigenza di offrire un quadro normativo di riferimento per il trattamento di dati personali per finalità di ricerca. A tal fine è proposta una breve ricostruzione dell'evoluzione del concetto di privacy che ne evidenzi i fondamenti valoriali allo scopo di facilitarne l'interpretazione e la comprensione delle profonde connessioni con i principi e le norme di etica e integrità nella ricerca. In questo contesto, sono illustrate le misure organizzative adottate dal Centro Interdipartimentale per l'Etica e l'Integrità nella Ricerca nell'implementazione delle disposizioni del Regolamento (UE) 2016/679, della normativa nazionale e interna all'Ente. In particolare, sono presentate le *Linee guida in materia di trattamento dei dati personali del Centro Interdipartimentale per l'Etica e l'Integrità nella Ricerca* elaborate per rispondere alla necessità di assicurare un adeguato livello di *accountability* di sistema, dato dalla chiara individuazione dei ruoli e delle responsabilità e da un'adeguata distribuzione dei compiti e delle funzioni inerenti al trattamento dei dati personali.

Prima parte

A. Il trattamento dei dati personali per finalità di ricerca: il quadro normativo

Affermata originariamente come diritto alla tutela della sfera privata individuale - intesa come dimensione sottratta al controllo pubblico, e alla riservatezza e confidenzialità delle informazioni - la privacy è divenuta, nell'attuale regime, oggetto di un quadro normativo diretto preminentemente alla protezione dei dati personali. In questo senso, un primo fondamento teorico è da rintracciarsi, già nel 1948, nel diritto non subire interferenze arbitrarie nella propria vita privata e familiare affermato all'art. 12 della Dichiarazione universale dei diritti umani delle Nazioni Unite e, più chiaramente, nel diritto al rispetto della vita privata e familiare sancito nel 1950 dalla Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del Consiglio d'Europa (art. 8) - base giuridica, quest'ultima, che ha motivato diverse sentenze della Corte europea dei diritti dell'uomo in favore del riconoscimento dei cosiddetti diritti di quarta generazione (tra cui, in particolare, l'accesso alla fecondazione eterologa).

Nell'ambito più strettamente connesso al trattamento dei dati personali, uno dei primi strumenti normativi dedicati è costituito dalla Convenzione n. 108 del Consiglio d'Europa, del 28 gennaio 1981 sulla protezione delle persone in relazione al trattamento automatizzato dei dati di carattere personale (aggiornata nel 2018). Un significativo sviluppo è stato successivamente raggiunto con la Direttiva 95/46/CE, che ha individuato i principi valoriali di riferimento nel trattamento dei dati personali, principi rimasti pressoché immutati anche nell'attuale Regolamento (UE) 2016/679 (Regolamento generale sulla protezione dei dati) - di seguito Regolamento - che pur abroga la Direttiva.

Successivamente, la Carta dei diritti fondamentali dell'Unione europea, approvata nel 2000 - avente medesimo valore giuridico dei trattati ai sensi dell'art.6 del Trattato di Lisbona - riconosce il diritto alla vita privata e familiare (art.7), mentre all'art. 8 recita**:** «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il *principio di lealtà*, per *finalità determinate* e in base al *consenso* della persona interessata o a un altro *fondamento legittimo* previsto dalla legge. Ogni persona ha il diritto di *accedere* ai dati raccolti che la riguardano e di ottenerne la *rettifica*. 3. Il rispetto di tali regole è soggetto al controllo di *un'autorità indipendente*».

Una specifica attenzione al tema della tutela della privacy è presente anche nei dispositivi giuridici in ambito bioetico. Il diritto alla vita privata e all'informazione è affermato all'art. 10 della Convezione sui diritti dell'uomo e la biomedicina del Consiglio d'Europa, sottoscritta dagli Stati membri ad Oviedo il 4 aprile 1997 e ratificata dall'Italia con la legge 2001/145. La Dichiarazione universale sulla bioetica e i diritti umani adottata per acclamazione dall'Assemblea generale dell'UNESCO il 19 ottobre 2005 - il principale strumento regolatorio di bioetica a livello internazionale - asserisce all'art. 9 il dovere di rispettare «la riservatezza per quanto concerne le persone interessate e i loro dati personali. Tali informazioni non devono essere utilizzate o diffuse per fini diversi da quelli per cui sono state raccolte o sui quali è stato prestato il consenso, nel rispetto del diritto internazionale e in particolare del diritto internazionale dei diritti umani**».**

Nell'attuale regime, scopo del Regolamento è assicurare la libera circolazione dei dati all'interno dell'Unione e tutelare al contempo i diritti e le libertà delle persone relativamente al trattamento dei loro dati personali. Tale

impostazione favorisce il trattamento dei dati per finalità di interesse pubblico, e per il mercato interno, superando la disomogeneità nei livelli di tutela generata dalla differente implementazione della Direttiva 95/46/CE tra gli Stati dell'Unione e la conseguente inefficienza economica connessa alla circolazione dei dati. L'adozione di uno strumento normativo immediatamente vincolante per gli Stati membri ha avuto come obiettivo proprio quello di giungere ad una uniformità della disciplina europea in materia di protezione dei dati (come disposto dal Trattato sul funzionamento dell'Unione europea).

Mentre la Direttiva 95/46/CE, si basava su meccanismi di controllo preventivo e di autorizzazione al trattamento da parte delle Autorità a livello nazionale (per l'Italia l'Autorità garante per la protezione dei dati personali), il Regolamento, anche al fine di superare le difficoltà poste da tale meccanismo in alcuni Stati membri, si fonda invece sul principio di responsabilizzazione (*accountability*) del titolare del trattamento. Di conseguenza, la norma è focalizzata sulla previsione e gestione dei rischi connessi al trattamento, il che comporta, per il titolare, l'obbligo di adottare comportamenti proattivi e di adeguare le misure di protezione alla rilevanza dei rischi prevedibili (art.24). Il titolare ha, in particolare, il compito e la responsabilità di decidere autonomamente quali modalità, garanzie e limiti del trattamento dei dati personali, siano più adeguate a rispettare le disposizioni della norma. L'autorizzazione preventiva è, in altre parole, sostituita dall'obbligo per il titolare, di valutare quali misure siano più adeguate a mitigare i rischi sin dalla fase di progettazione del trattamento (privacy by design e by default, art. 25).

Secondo la definizione del Garante, per rischio deve intendersi «uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità per i diritti e le libertà individuali» (cfr sito web del Garante). La valutazione inoltre deve essere riferita non solo alla sicurezza del trattamento in quanto tale ma anche a quelli che possono essere i suoi effetti complessivi e ai rischi correlati: in questo senso una interpretazione di cosa debba intendersi per rischio può essere rintracciata ai considerando 75 e 76 del Regolamento, relativamente ai parametri della probabilità dell'evento e della gravità della lesione. Qualora la procedura di risk assessment, per la mole di dati, il numero di persone coinvolte, la durata del trattamento o la natura stessa dei dati abbia evidenziato un rischio rilevante per i diritti e le libertà delle persone interessate, è richiesto al titolare l'esecuzione di una valutazione preliminare di impatto (art. 35).

La valutazione deve contenere «le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione» (art. 35 c. 7, lettera d). Nel caso in cui la valutazione di impatto evidenzi un rischio elevato per il quale non si ritiene di avere misure di mitigazione idonee, il titolare non può procedere al trattamento senza una consultazione preventiva dell'Autorità di controllo (art.36). Quest'ultima può indicare, attraverso un proprio parere, quali misure ulteriori devono essere adottate, come pure procedere, nel caso in cui verifichi una violazione del Regolamento, con le misure correttive di cui all'art. 58 (ammonimento del titolare, limitazione o divieto di trattamento).

L'Autorità garante per la protezione dei dati personali, in adempimento a quanto richiesto dallo stesso Regolamento (art. 35 comma 4), ha reso un Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018. L'esecuzione di una procedura di valutazione di impatto è inoltre consigliata nell'ottica dell'atteggiamento proattivo alla protezione dei dati: si vedano al riguardo le Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" del Comitato europeo per la protezione dei dati, istituito ai sensi dell'art. 68 del Regolamento. Si osservi come il Comitato rappresenti la fonte di interpretazione autentica della norma.

Il Regolamento ha inoltre garantito agli Stati membri, nell'adeguamento della normativa nazionale, la possibilità di introdurre ulteriori condizioni quali più specifiche misure di garanzia, limitazioni o deroghe come si evince ad esempio dalla lettura degli artt. 9 e 89 dedicati al trattamento di dati appartenenti a categorie particolari. L'adeguamento della norma nazionale italiana al Regolamento europeo è avvenuto con il D.lgs. 10 agosto 2018, n. 101, ed ha portato ad una significativa riduzione del corpus del Codice in materia di protezione dei dati personali, emendato di tutte le disposizioni non compatibili o soverchie. In particolare, l'impostazione basata sul rischio e sulla responsabilizzazione del titolare del trattamento ha richiesto l'eliminazione dell'allegato b del Codice dedicato alle misure minime di sicurezza. Si noti, di converso, l'introduzione di norme specifiche

per la ricerca biomedica di cui agli art.110 e 110 bis del Codice novellato, in coerenza alle deleghe agli Stati membri di cui all'art. 89 del Regolamento. Ulteriori specifiche disposizioni riguardanti la ricerca scientifica sono costituite dalle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del D.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018, che integrano la norma e il cui rispetto costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali (art. 2 - quater c. 4 del Codice).

Si osservi, in particolare, come le Regole di deontologiche all'art. 3 c. 1, stabiliscano che presupposto del trattamento per finalità di ricerca è che questa sia «effettuata sulla base di un progetto redatto conformemente agli standard metodologici del pertinente settore disciplinare, anche al fine di documentare che il trattamento sia effettuato per idonei ed effettivi scopi statistici o scientifici», e al comma 2 lettera c) che la documentazione di progetto debba contenere «una dichiarazione di impegno a conformarsi alle presenti regole deontologiche. Un'analoga dichiarazione è sottoscritta anche dai soggetti - ricercatori, responsabili e persone autorizzate al trattamento - che fossero coinvolti nel prosieguo della ricerca». Tale documentazione è conservata unitamente al progetto di ricerca presso le strutture cui afferisce il personale di ricerca coinvolto nel progetto, per 5 anni dalla sua conclusione. Il principio di autonomia, declinato in termini giuridici come diritto all'autodeterminazione informativa, richiede infine, che i partecipanti siano sempre adeguatamente informati dei rischi per la privacy inerenti alle attività sperimentali: nel caso in cui la somministrazione dell'informativa comporti uno sforzo sproporzionato rispetto al diritto tutelato, devono essere adottate, in sua vece, idonee forme di pubblicità, esemplificate all'art. 6 c. 3. In luogo, infine, di prevedere requisiti e condizioni che possano giustificare un'autorizzazione generale al trattamento, come nella precedente disciplina, il Garante per la protezione dei dati personali ha individuato prescrizioni specifiche per il trattamento di categorie particolari di dati, anche a fini di ricerca di cui al par. 4.11 delle Prescrizioni relative al trattamento dei dati genetici, che sostituisce l'autorizzazione generale n. 8/2016 e al par. 5 Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica, che sostituisce l'autorizzazione generale n. 9/2016, del Provvedimento 146/2019.

La ricerca scientifica, per la complessità e la pervasività delle tecnologie che comportano l'utilizzo di dati personali, e la variabilità dei contesti del

trattamento in ragione delle diverse attività sperimentali, costituisce uno dei contesti in cui è sempre più evidente la necessità di identificare, sin dalla progettazione, le possibili criticità e di definire misure specifiche di gestione del rischio di forme, anche indirette, di violazione dei diritti dei partecipanti.

Tale approccio proattivo, noto come privacy by design, è definito all'art. 25 c. 1 del Regolamento nei termini seguenti: «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente Regolamento e tutelare i diritti degli interessati».

Sono parte di tale approccio proattivo i principi dell'ethics by design, diretti ad individuare i rischi etici connessi alle attività sperimentali, anche in ragione di specifiche fragilità o condizioni di vulnerabilità dei partecipanti. Del pari, l'integrità nella ricerca, diretta ad assicurare la qualità del dato e la verificabilità dei risultati, garantisce il rispetto degli standard internazionali che fanno della ricerca una finalità di rilevantissimo interesse pubblico in ragione del quale è lecito il trattamento di dati personali anche particolari.
In ottemperanza alla norma, le stesse regole di integrità nella ricerca prevedono, quali elementi essenziali a tutela dei partecipanti, misure adeguate per la protezione dei dati personali sin dalla fase di progettazione, come recitano Le linee guida per l'integrità nella ricerca della Commissione per l'Etica e l'Integrità nella Ricerca del CNR, (parte I par. A punto 7): «il Responsabile del trattamento dei dati della struttura presso la quale il progetto verrà svolto designa formalmente la/e persona/e autorizzata/e al trattamento dei dati personali che verranno raccolti nel corso delle attività di ricerca.

Tra le persone autorizzate vi è preferibilmente il responsabile scientifico del progetto. Le persone autorizzate comunicano al Responsabile del trattamento la tipologia di dati raccolti, le finalità di progetto connesse al trattamento, la base giuridica del trattamento, l'informativa relativa

al trattamento resa agli interessati, chi tra il personale coinvolto nel progetto avrà accesso ai dati, quali misure di sicurezza siano previste per il trattamento e la conservazione dei dati (logiche, tecniche e organizzative), l'esito della valutazione preliminare di impatto del trattamento sui diritti degli interessati, compilata ai sensi delle norme vigenti, e tutti gli elementi utili ai fini dell'aggiornamento del Registro relativo al trattamento dei dati personali istituito presso l'ente di afferenza».
In questa prospettiva, sono qui di seguito riportati i principali dispositivi giuridici e strumenti di indirizzo il cui rispetto è indispensabile ai fini della liceità del trattamento dei dati personali dei partecipanti ai progetti di ricerca sia raccolti nell'ambito di uno specifico progetto, che nel successivo utilizzo per ulteriori attività di ricerca.

B. Riferimenti normativi

- Convenzione di Strasburgo 108/1981 "Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, del Consiglio d'Europa del 28 gennaio 1981" modificata dal Protocollo di emendamento alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, fatto a Strasburgo il 10 ottobre 2018, ratificato dall'Italia con la legge 60/2021 (Gazzetta Ufficiale Serie Generale n.110 del 10 maggio 2021).

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) aggiornato con le rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea n.127 del 23 maggio 2018.

- Decreto legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" (S.O n. 123 alla Gazzetta Ufficiale del 29 luglio 2003 n.174) integrato con le modifiche introdotte dal Decreto legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali

dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)" (Gazzetta Ufficiale n.205 del 4 settembre 2018).

- Decreto legislativo 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)." (18G00129) - Gazzetta Ufficiale n.205 del 4 settembre 2018.

- Decreto legislativo 25 novembre 2016, n. 218 "Semplificazione delle attività degli enti pubblici di ricerca ai sensi dell'articolo 13 della legge 7 agosto 2015, n. 124", art. 2 Carta Europea dei Ricercatori (Gazzetta Ufficiale Serie Generale n. 276 del 25 novembre 2016).

- Garante per la protezione dei dati personali, "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica" pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 (Gazzetta Ufficiale Serie Generale n. 11 del 14 gennaio 2019).

- Decreto del Ministro della Giustizia del 15 marzo 2019, recante inserimento nell'allegato A del decreto legislativo 30 giugno 2003, n. 196, delle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, pubblicate ai sensi dell'articolo 20, comma 4, del decreto legislativo 10 agosto 2018, n. 101 (Gazzetta Ufficiale Serie Generale n.71 del 25 marzo 2019).

- Garante per la protezione dei dati personali, "Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice 13 dicembre 2018", (Registro dei provvedimenti n. 497 del 13 dicembre 2018).

- Garante per la protezione dei dati personali, "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101" (Provvedimento 146/2019 - Gazzetta Ufficiale Serie Generale n. 176 del 29 luglio 2019).

– Garante per la protezione dei dati personali "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018" (Gazzetta Ufficiale Serie Generale n.269 del 19 novembre 2018).

– Garante per la protezione dei dati personali, Provvedimento per la notifica delle violazioni dei dati personali (data breach) procedura telematica (on line): https://servizi.gpdp.it/databreach/s/.

– Regolamento di Organizzazione e Funzionamento del CNR, emanato con provvedimento del Presidente del CNR n. 14 prot. AMMCNT-CNR n. 0012030 del 18 febbraio 2019, di cui è stato dato l'avviso di pubblicazione sul sito del Ministero dell'Istruzione, dell'Università e della Ricerca, in data 19 febbraio 2019, entrato in vigore dal 1° marzo 2019 (art. 19 bis).

– Linee guida per l'integrità nella ricerca (2019) della Commissione per l'Etica e l'Integrità nella Ricerca del CNR, https://www.cnr.it/it/documenti-commissione (Parte I, par. A punto 7).

– Si vedano infine i pareri del Comitato europeo per la protezione dei dati, https://edpb.europa.eu/concernant-le-cepd/concernant-le-cepd/who-we-are_it e i provvedimenti del Garante per la protezione dei dati personali Provvedimenti - Garante Privacy.

Seconda parte

1. Premessa

Principio ispiratore e innovativo del Regolamento generale sulla protezione dei dati (Reg. UE 2016/679) è la *responsabilizzazione* (*accountability*) intesa come adozione da parte dei titolari e responsabili del trattamento, di un atteggiamento proattivo che deve tradursi nella previsione del rischio e nell'individuazione e messa in atto di misure di sicurezza in grado di assicurare un adeguato livello di protezione dei dati. Nel rispetto del principio di *accountability*, la norma europea ha previsto quale adempimento preliminare in capo al titolare, l'istituzione di un registro delle attività di trattamento la cui funzione è quella di assicurare un monitoraggio costante dei dati raccolti e

delle modalità e finalità dei trattamenti (art. 30). Il Consiglio Nazionale delle Ricerche, in attuazione delle disposizioni della norma europea, con proprio atto interno, ha fatto obbligo a tutti i direttori e responsabili di strutture tecnico-scientifiche dell'Ente, di istituire un registro relativo sia ai trattamenti per finalità di ricerca sia a quelli per finalità di tipo gestionale-amministrativo (di cui alle circ. 10/2018, 24/2019 e 12/2020).

A seguito della costituzione nel febbraio 2020 del Centro Interdipartimentale per l'Etica e l'Integrità nella Ricerca e del trasferimento del personale precedentemente afferente alla Sede Secondaria di Roma dell'Istituto di Tecnologie Biomediche del CNR (ITB-CNR), completato nel mese di agosto 2020, il dirigente dott.ssa Cinzia Caporale istituiva nell'aprile 2021 il registro dei trattamenti interno alla struttura (precedentemente le attività di trattamento dei dati erano inserite nel registro interno all'ITB-CNR in quanto svolte presso una Sede Secondaria dell'Istituto). Inoltre, considerate le funzioni di supporto scientifico, tecnico e gestionale alle attività della Commissione per l'Etica e l'Integrità nella Ricerca, la stessa istituiva, già nel maggio 2018, uno specifico registro per i trattamenti effettuati nell'ambito dello svolgimento di tali funzioni.

Entrambi i registri sono posti sotto la responsabilità del Coordinatore del Centro Interdipartimentale, nonché Coordinatore della Commissione per l'Etica e l'Integrità della Ricerca, dott.ssa Cinzia Caporale, in qualità di responsabile interno del trattamento. I registri, in coerenza con la natura dinamica dello strumento, sono stati regolarmente aggiornati e sottomessi al Responsabile della Protezione Dati dell'Ente, le cui richieste di revisione e integrazione sono state puntualmente accolte, e successivamente trasmessi alla direzione del Dipartimento di Scienze Biomediche da cui il Centro dipende funzionalmente (di cui in ultimo in data 5 ottobre 2022). La compilazione e aggiornamento dei registri è oggetto di uno specifico incarico, affidato alla dott.ssa Giorgia Adamo (di cui al prot. n.0006634/2021 del 29/01/2021). Quest'ultima opera sotto la supervisione del Coordinatore del Centro e della Commissione, in qualità di responsabile interno del trattamento, e del referente interno in materia di protezione dei dati, dott.ssa Elena Mancini (di cui al prot. n.0006635/2021 del 29/01/2021).

L'atto di designazione nel referente interno in materia di protezione dei dati, finalizzato ad assicurare il necessario coordinamento con la Direzione

Generale e con il Responsabile della Protezione Dati dell'Ente, di cui al decreto del Presidente del CNR n. 27/2019, ha previsto in particolare il supporto nella gestione degli adempimenti connessi alla protezione dei dati e nella verifica del rispetto, da parte dei soggetti autorizzati al trattamento dei dati, di norme e misure tecniche e organizzative nonché delle istruzioni impartite dal direttore della struttura scientifica. Le disposizioni del citato provvedimento presidenziale e s.m.i in ottemperanza alla norma europea - che prevede la possibilità per il titolare del trattamento di designare persone autorizzate al trattamento che agiscono sotto la sua autorità - affidano ai direttori delle strutture scientifiche dell'Ente la responsabilità di fornire adeguate informazioni e istruzioni al personale tecnico e di ricerca che opera in qualità di persone autorizzate al trattamento" (decreto del Presidente n. 27/2019 art. 1 lett. a).

In adempimento a tali disposizioni normative, al personale del Centro è fatto obbligo di aderire a regole di comportamento che assicurino la massima riservatezza in merito ai dati trattati e la tempestiva comunicazione in merito all'avvio di nuovi trattamenti non precedentemente inclusi nel registro con lo scopo di un suo costante aggiornamento. Ai fini dell'espletamento di tale obbligo, il personale ha sottoscritto una specifica dichiarazione in materia. La raccolta, archiviazione e monitoraggio delle dichiarazioni è oggetto di uno specifico incarico, affidato al sig. Emiliano Liberatori che opera sotto la supervisione del responsabile interno e del referente interno in materia di protezione i dati personali (prot. n. 003391/2023 del 11/01/2023).

Nella prospettiva di offrire al personale afferente al Centro un quadro coerente e completo delle responsabilità inerenti i compiti e le funzioni che comportano il trattamento di dati personali, sono state elaborate le Linee guida qui di seguito riportate. Le Linee guida sono rivolte a tutto il personale afferente al Centro, sia pur in relazione alla specificità dei trattamenti effettuati e alla tipologia di dati trattati per il conseguimento delle diverse finalità, e sono state elaborate dal referente interno in materia di protezione dei dati, dott.ssa Elena Mancini, dal componente del gruppo di lavoro in materia di protezione dei dati a supporto del Direttore Generale dell'Ente, dott.ssa Daniela Niccoli e dal Coordinatore del Centro e della Commissione in qualità di responsabile interno del trattamento, dott.ssa Cinzia Caporale. La versione finale del documento si è avvalsa della lettura e dei suggerimenti del Responsabile della Protezione dei Dati dell'Ente, dott. Raffaele Conte,

e del Corrispondente presso il Dipartimento di Scienze Biomediche, avv. Laura Milita. I rispettivi commenti sono stati tutti accolti nel testo finale.

Il documento intende rispondere all'esigenza di assicurare un adeguato livello di *accountability* di sistema nelle strutture cui è destinato, dato dalla chiara individuazione dei ruoli e delle responsabilità e da un'adeguata distribuzione dei compiti e delle funzioni inerenti al trattamento dei dati personali.

2. Linee guida in materia di trattamento dei dati personali del Centro Interdipartimentali per l'Etica e l'Integrità nella Ricerca

2.1 - Contesto del trattamento

Il Centro Interdipartimentale per l'Etica e l'Integrità nella Ricerca, di seguito Centro, dei sette Dipartimenti del Consiglio Nazionale delle Ricerche effettua trattamenti dei dati personali che possono essere suddivisi rispetto a due finalità: i trattamenti dei dati personali finalizzati alla gestione del rapporto di lavoro del personale afferente al Centro e alla gestione degli adempimenti amministrativi; i trattamenti finalizzati allo svolgimento delle attività assegnate per competenza al Centro. In entrambi i casi, i dati personali riconducibili a quelli compresi negli artt. 9 e 10 del Reg. UE 2016/679 sono trattati in coerenza con le disposizioni ad essi applicabili. La base giuridica per il trattamento dei dati personali trattati presso il Centro deve essere individuata nell'esercizio dei compiti istituzionali ad esso attribuiti, ex art 6 lettera c) e lettera e) del Reg. UE 2016/679, come descritti nell'Allegato 1 al Provvedimento del Presidente n. 13 del 14 febbraio 2020 istitutivo del Centro.

Il Centro opera quale struttura scientifica: progetta e svolge attività di ricerca nell'ambito delle tematiche di propria competenza, nonché svolge attività di supporto scientifico alla Rete scientifica del CNR e di supporto tecnico-scientifico, gestionale e amministrativo alla Commissione per l'Etica e l'Integrità nella Ricerca. Pur trattandosi di ricerche di natura perlopiù strettamente teorica, alcuni studi comportano l'impiego di metodologie e strumenti elettivi dell'indagine qualitativa, quali interviste, *survey* online, somministrazione di questionari, nonché la raccolta di dati provenienti da soggetti terzi, quali ad esempio istituzioni di ricerca pubbliche o private, università, strutture sanitarie con cui è in atto una collaborazione scientifica o un partenariato di progetto. Il trattamento riguarda dati personali

comuni, dati sanitari, dati relativi a opinioni personali, di orientamento politico, filosofico o religioso.

2.2 - Categorie di destinatari dei dati personali

I dati personali trattati dal Centro possono essere comunicati nell'ambito del CNR (ad altro responsabile interno CNR) a: Organi di vertice e organismi di controllo CNR; Strutture dell'Amministrazione centrale e della Rete scientifica interessate anche in quanto parti di un procedimento complesso nella gestione del flusso dei dati. Possono essere comunicati ad altri soggetti pubblici, quali a titolo esemplificativo, ma non esaustivo: Autorità indipendenti, Ministeri vigilanti, agenzie di finanziamento della ricerca pubbliche e private, enti autorizzativi, partner di progetto, soggetti terzi con i quali sono attive convenzioni o accordi di collaborazione, etc., qualora sia previsto da una disposizione di legge o di regolamento ovvero sia necessario per l'esercizio delle funzioni istituzionali. La comunicazione di dati a soggetti privati è effettuata qualora sia prevista da un contratto in essere, una norma di legge o regolamento, o da un accordo tra le parti. I dati personali trattati dal Centro possono essere diffusi solo ove previsto da specifici adempimenti contrattuali, ivi compresi a titolo esemplificativo ma non esaustivo: gli accordi di collaborazione scientifica, i protocolli dei progetti di ricerca, le convenzioni operative, disposizioni normative nazionali o dell'Unione.

I dati relativi ai trattamenti in materia di gestione amministrativa e di gestione del personale, di norma non sono trasmessi a Paesi extra UE. Potranno essere oggetto di trasmissione a Paesi extra UE atti contenenti dati personali strettamente necessari allo scopo, esclusivamente previa adozione delle misure di volta in volta adeguate, in coerenza con le disposizioni previste dal Reg. (UE) 2016/679 e sulla base delle decisioni di adeguatezza della Commissione europea.

2.3 - Descrizione delle basi giuridiche

2.3.a - Per la gestione del rapporto di lavoro

Per quanto riguarda il trattamento dei dati relativi al personale del Centro (dipendente e afferente) nell'ambito delle attività concernenti attestati di presenza, SIGLA e altre piattaforme informatiche dell'Ente, la base giuridica è: art.6 lett. b), c) ed e) del Reg.(UE) 2016/679; Regolamento del personale

CNR; Decreto legislativo 165/2001; decreto legislativo 127/2003; Decreto legislativo 218/2016; Legge 104/92; CCNL e CCNI.

Con riferimento al trattamento finalizzato all'adempimento delle procedure concorsuali (persone fisiche) - Selezioni online CNR per partecipanti a bandi di concorso - la base giuridica è: art. 6 lett. e) del Reg. (UE) 2016/679; Regolamento del personale CNR; DPR n. 487/94, etc. Per quanto concerne il trattamento finalizzato agli adempimenti amministrativi e fiscali derivanti da obblighi contrattuali verso i fornitori di beni e servizi e agli adempimenti previsti per le convenzioni operative con soggetti terzi per finalità di ricerca, la base giuridica è: art.6 lettera c) ed e) e art. 10 del Reg. (UE) 2016/679; D.Lgs.50/2016; Artt. 46 e 47 del D.P.R. n. 445/2000 e s.m.i. (Verifica delle dichiarazioni).

2.3.b - Per scopi scientifici

Con riferimento al trattamento dei dati per scopi scientifici, la base giuridica è diversificata in ragione delle due principali finalità di trattamento, che sono le seguenti: una costituita dai progetti di ricerca ideati e/o condotti dal Centro e l'altra dall'attività di supporto scientifico, tecnico, gestionale e amministrativo alla Commissione.

a) In riferimento alla prima finalità di trattamento, la base giuridica è costituita dall'art. 6, comma 1 lettera a) del Reg (UE) 2016/679 "l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità", nonché dagli articoli del Reg.(UE) 2016/679 n. 9 "Trattamento di categorie particolari di dati personali", lett. j), e n. 89 "Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici".

b) In riferimento alla seconda finalità di trattamento costituita dall'attività di supporto tecnico/scientifico alla Commissione: (i) per quanto riguarda il trattamento dei dati nell'ambito delle attività della Commissione per l'Etica e l'Integrità nella Ricerca finalizzato al servizio di consulenza etica per i progetti di ricerca esterni al CNR e al relativo espletamento degli adempimenti amministrativi per la stipula dei contratti con i soggetti esterni al CNR richiedenti il servizio di consulenza etica, la base giuridica è la seguente: art. 6, comma 1 lettera b) e art. 10 del Reg.(UE) 2016/679. Tale attività rientra tra i compiti istituzionali attribuiti alla Commissione dal provvedimento del Presidente all'art. 1, comma 2, lettera j) (prot. n.

0065527/2019 del 23/09/2019); (ii) per quanto riguarda il trattamento dei dati per finalità di verifica di presunti casi di condotta scorretta nella ricerca, la base normativa è la seguente: art. 6, comma 1 lettera e) del Reg. (UE) 2016/679 "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento". Tale attività rientra tra i compiti istituzionali attribuiti alla Commissione dal provvedimento del Presidente all'art. 1, comma 2, lettera g) (prot. n. 0065527/2019 del 23/09/2019). Si richiamano inoltre le disposizioni di cui al Codice di comportamento per i dipendenti del CNR e alle Linee guida per l'integrità nella ricerca della Commissione per l'Etica e l'Integrità nella Ricerca del CNR (2019).

2.4 - Descrizione delle categorie dei dati

In ragione delle competenze attribuite e sopra descritte, il Centro esegue il trattamento di dati personali comuni (dati di contatto e dati necessari alle finalità amministrative, ad es. conto corrente, etc.), di dati particolari (raccolti nell'ambito dei progetti di ricerca ai quali partecipa il Centro) e di dati comuni e di contatto nella misura strettamente necessaria per le attività svolte a supporto della Commissione per l'Etica e l'Integrità nella Ricerca nell'espletamento dei propri compiti e funzioni istituzionali.

2.5 - Misure organizzative e misure tecniche di sicurezza generali

a) Ciascun collaboratore assegnatario di una pratica di carattere amministrativo contenente dati personali appartenenti a categorie particolari, si impegna a custodire la documentazione durante il periodo di lavorazione con la massima cura al fine di evitare la visione a terzi non autorizzati. Analogamente, sarà posta la massima cura ove questi dati siano parte delle documentazioni di un progetto o di uno studio.
   La documentazione cartacea va trattata per la lavorazione in modo da escludere, per quanto possibile, la visione da parte di terzi non autorizzati e possibilmente custodita in archivi/armadi chiusi a chiave al termine della giornata lavorativa. Va inoltre evitata la comunicazione a terzi non autorizzati delle informazioni presenti nella pratica, e quindi anche dei dati personali oggetto del trattamento, nel caso in cui da tali comunicazioni ne possa derivare una lesione o pregiudizio rispetto ai diritti fondamentali della persona.

La documentazione informatica deve essere trattata preferibilmente in dispositivi fissi secondo le regole di sicurezza adottate nella sede di afferenza oppure su dispositivi portatili sempre dotati di credenziali di accesso. Ove siano presenti dati particolari, si raccomanda l'uso di supporti mobili cifrati (dispositivi di archiviazione di massa USB).
Il trattamento dei dati personali relativi alla gestione delle presenze del personale CNR afferente al Centro viene processato da un solo incaricato preventivamente individuato e istruito. L'incaricato è autorizzato a processare la documentazione per la finalità di redazione degli attestati di presenza e si impegna a mantenere segrete le proprie credenziali di accesso e a segnalare tempestivamente l'eventuale uso non autorizzato delle stesse, così come l'eventuale accesso di terzi non autorizzati.

L'incaricato si impegna altresì a non divulgare i documenti che contengono i dati personali oggetto del trattamento e, per quanto nelle sue possibilità, a vigilare a che altri non diffondano tali materiali. Al personale incaricato del trattamento consistente nella compilazione degli attestati di presenza viene consegnato tra gli altri il Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016 e 2/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice - 13 dicembre 2018 e le "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" del 14 giugno 2007 con la precisazione che a decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi nella misura in cui siano compatibili con il Reg. UE 2016/679 e con il D.lgs. 101/2018 (cfr. art. 22, co. 4, d.lgs. n. 101/2018). I dati particolari saranno trasmessi al competente Ufficio Gestione Risorse Umane del CNR al solo personale autorizzato.

Ai sensi dell'art. 13 del Regolamento è stata predisposta opportuna informativa sul trattamento dei dati personali in relazione alla gestione del rapporto di lavoro tra il CNR e il personale afferente al Centro Interdipartimentale per l'Etica e l'integrità nella ricerca.

Le misure tecniche per le postazioni di lavoro a presidio dei dati personali nell'ambito del loro trattamento sono state predisposte a cura dell'Ufficio ICT e a cui sin da ora si rinvia. Il Centro adotta quale misura tecnica locale la protezione delle postazioni di lavoro con password.

b) Per quanto concerne i dati raccolti per finalità di ricerca, sono adottate le seguenti misure organizzative: i) la pseudonimizzazione nel caso di interviste *de visu*; ii) ove possibile, per i dati trasmessi da partner di progetto o soggetti con cui è in atto una collaborazione scientifica, il trattamento di dati trasmessi già privi di ogni dato identificativo; iii) la generalizzazione dei dati escludendo ogni fattore non necessario che possa condurre all'identificazione indiretta degli interessati; iv) la somministrazione di questionari anonimi ove compatibile con gli obiettivi della ricerca; v) preferibilmente l'impiego di piattaforme che non attivino tracciatura informatica; vi) la cancellazione dei dati personali dei partecipanti alla ricerca (studi che comportano interviste, questionari online, ecc.) effettuata trascorsi i 5 anni dalla conclusione della ricerca. (La conservazione dei dati di contatto successivamente ai 5 anni è finalizzata al ricontatto dei partecipanti previo consenso dei medesimi. Nel caso di invito alla partecipazione effettuato per posta elettronica è data facoltà al partecipante di chiedere l'esclusione dalla *mailing list*).

c) Per quanto concerne i dati trattati per le finalità di supporto alle attività della Commissione, sono adottate le seguenti misure di sicurezza tecniche e organizzative:
   - informazione del personale in merito alle disposizioni della presente privacy policy;
   - clausola di riservatezza per le persone autorizzate al trattamento;
   - autenticazione tramite password per il supporto informatico e per alcuni file;
   - backup eseguito su base almeno trimestrale dei dati in modo da ovviare alla loro perdita in caso di incidente fisico o tecnico (finalità di ripristino) e aggiornamento periodico dei software utilizzati in modo da garantire la sicurezza dei dati e la loro accessibilità da parte del personale autorizzato.

   Inoltre, sono adottate le seguenti misure di garanzia:
   - le comunicazioni riguardanti le attività svolte dal Centro a supporto dell'espletamento delle finalità istituzionali della Commissione per l'Etica e l'Integrità nella Ricerca avvengono tramite account di posta elettronica dedicati, il cui accesso è riservato esclusivamente al Coordinatore della Commissione (integrity@cnr.it) o anche ai Responsabili della segreteria scientifica e della segreteria tecnica

della stessa (cnr.ethics@cnr.it). Le pratiche relative all'espletamento della fase istruttoria della procedura per il rilascio di pareri di *Ethical Clearance* e di valutazione tecnica preliminare di presunti casi di condotta scorretta nella ricerca possono essere tuttavia affidate a collaboratori che riferiscono direttamente al Coordinatore del Centro e della Commissione oppure ai Responsabili delle segreterie summenzionate.

2.6 - Gestione del protocollo ordinario e archivio cartaceo

Il personale incaricato di interagire con il protocollo ordinario afferisce al Centro, tra questi vi è il Responsabile amministrativo del Centro. Il personale incaricato e formalmente autorizzato è preventivamente istruito anche con particolare riferimento al trattamento dei dati personali. L'accesso al protocollo avviene previo inserimento delle credenziali personali ad esso assegnate. L'incaricato si impegna a mantenere segrete le credenziali, a segnalare tempestivamente l'eventuale uso non autorizzato delle stesse così come l'eventuale accesso di terzi non autorizzati, a non divulgare il contenuto dei documenti che contengono i dati personali oltre che dei dati stessi, oggetto del trattamento.

L'archivio amministrativo cartaceo corrente è custodito in armadi chiusi a chiave nelle stanze ad uso del Responsabile amministrativo del Centro. Le chiavi sono nella disponibilità del Responsabile amministrativo del Centro nonché custodite dal Coordinatore.

2.7 - Gestione del protocollo e archivio riservato

Trattasi di un protocollo distinto ed autonomo rispetto a quello ordinario. L'accesso al protocollo riservato avviene previo inserimento delle credenziali ad esso assegnate e segue le indicazioni fornite dall'Ufficio Gestione Documentale del CNR. Il personale incaricato del trattamento dei dati mediante l'utilizzo del protocollo riservato della Commissione per l'Etica e l'Integrità nella Ricerca, afferisce alla Segreteria scientifica della Commissione stessa e in particolare alla Research Integrity Unit di cui all'art. 3, comma 2 del provvedimento in data 23 settembre 2019 del Presidente del CNR recante "Scioglimento e ricostituzione della Commissione per l'Etica e l'Integrità nella Ricerca", ed è preventivamente incaricato ed istruito. L'accesso al protocollo riservato avviene previo inserimento delle credenziali personali ad esso assegnate.

L'incaricato si impegna a mantenere segrete le credenziali, a segnalare tempestivamente l'eventuale uso non autorizzato delle stesse così come l'eventuale accesso di terzi non autorizzati al protocollo riservato, a non divulgare il contenuto dei documenti che contengono i dati personali oltre che dei dati stessi, oggetto del trattamento. La trasmissione di pareri di consulenza etica relativa a presunti casi di condotta scorretta avviene esclusivamente tramite protocollo riservato.

2.8 - Conservazione dei documenti

La documentazione relativa alle attività della Commissione viene conservata:

- per contatti con i componenti: i dati comuni sono conservati nel rispetto della normativa vigente nonché del Massimario di conservazione e selezione dei documenti d'archivio del CNR, ex art. 68 DPR 445/2000.
- Per contatti con i ricercatori: sono trattati dati comuni relativi ai ricercatori richiedenti i pareri/consulenza ai sensi dell'articolo 6 par. 1 lettere c) ed e) del Reg. UE 2016/679. La motivazione della conservazione è data dalla necessità di ricontatto dei ricercatori per richieste di ulteriori informazioni e chiarimenti, in particolare nel caso di emendamenti in merito ai progetti già approvati dalla Commissione, e in caso di aggiornamenti/integrazioni della documentazione progettuale prodotta. La durata della conservazione è strettamente dipendente dal perseguimento di dette finalità.

I progetti di ricerca trasmessi alla Commissione a corredo della richiesta di un parere di *Ethical Clearance* contengono di norma esclusivamente dati comuni riferiti al personale di ricerca coinvolto nel progetto. Non sono presenti in alcun modo dati riferibili ai partecipanti ai progetti.

I moduli di consenso informato sono sottomessi quali modelli standard, da approvare preliminarmente all'arruolamento. Ove si trattasse di moduli sottoscritti dai partecipanti in una fase anteriore al progetto, i moduli sono acquisiti solo se previamente anonimizzati. La conservazione della documentazione di progetto è finalizzata esclusivamente a consentire la verifica documentale e l'accertamento della correttezza degli atti. Il consenso al trattamento dei dati dei ricercatori è inerente alla richiesta stessa, effettuata tramite procedure codificate e pubblicate sul sito web istituzionale della Commissione; si tratta inoltre di dati di contatto, afferenza e posizione lavorativa pubblici. Si applica, di conseguenza, il Massimario di conservazione,

selezione e scarto che così determina il tempo di conservazione in "illimitato". La documentazione di progetto ricevuta dai ricercatori viene utilizzata al solo fine della valutazione dei profili etico-giuridici preliminare al rilascio di un parere di *Ethical Clearance* con valore autorizzativo, conservata in formato elettronico in dispositivi dotati di credenziali di accesso e in modo tale da garantire la riservatezza e confidenzialità dei materiali (anche ai fini della tutela dei diritti di autore) per un tempo illimitato. Per i rimanenti e differenti documenti amministrativi di pertinenza della Commissione, il termine previsto per la loro conservazione è di 5 anni in archivio corrente e di 5 anni nell'archivio di deposito in coerenza con le disposizioni del Manuale di gestione – Massimario di conservazione e selezione dei documenti d'archivio del CNR del Delegato alla gestione documentale. Decorso tale periodo, effettuata la verifica sul Massimario di selezione e scarto del CNR, il documento sarà distrutto oppure inserito nell'archivio storico. Sono fatti salvi i termini specifici indicati nel Manuale di gestione e i casi differenti e specifici ivi previsti.

2.9 - Obblighi di riservatezza

Il personale afferente al Centro dovrà garantire, in ogni operazione di trattamento, la massima riservatezza dovuta rispetto al caso di specie. In particolare, dovrà:

a) astenersi dal trasferire, comunicare e/o diffondere i dati amministrativi al di fuori del Centro, salvo preventiva autorizzazione del Coordinatore del Centro;
b) svolgere operazioni di trattamento unicamente su dati/banche dati ai quali si abbia legittimo accesso, nel corretto svolgimento del rapporto di lavoro, e utilizzare a tal fine gli strumenti indicati o messi a disposizione dal Centro;
c) osservare scrupolosamente gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati personali altrui;
d) in caso di allontanamento, anche temporaneo, dalla postazione di lavoro, verificare che non vi sia possibilità da parte di terzi (anche se colleghi o comunque appartenenti alla struttura) di accedere ai dati personali per i quali era in corso una qualunque operazione di trattamento, sia essa mediante supporto cartaceo o informatico;
e) astenersi dal comunicare a terzi (anche se colleghi o comunque appartenenti alla struttura) in qualsiasi forma, la/le propria/e

credenziale/i di autenticazione, necessaria/e per il trattamento dei dati personali con strumenti elettronici;

f) segnalare al Coordinatore del Centro eventuali situazioni di rischio per la sicurezza dei dati di cui sia venuto a conoscenza (ad esempio, la violazione della password, il tentativo di accesso non autorizzato ai sistemi, la penetrazione di virus informatici, il furto o smarrimento di dispositivi mobili, la distruzione o deterioramento di documentazione cartacea riservata).

Gli obblighi relativi alla riservatezza, alla comunicazione e alla diffusione dovranno essere scrupolosamente osservati anche in seguito all'eventuale cessazione del rapporto contrattuale attualmente in essere con il Centro.

2.10 - Violazione di dati personali - Data Breach

Il Regolamento richiede, in caso di *Data Breach*, l'attivazione, da parte dell'Amministrazione colpita, di una procedura che deve essere rapida e contenuta in massimo 72 ore dall'avvenuta conoscenza da parte del titolare. Qualora sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, sono consentiti anche tempi maggiori, previa adeguata documentazione al riguardo.

Con il Provvedimento n. 157 del 30 luglio 2019 il Garante per la protezione dei dati personali ha introdotto un nuovo modello ufficiale contenente le informazioni minime necessarie per effettuare una notifica di violazione dei dati personali ai sensi dell'art. 33 del Regolamento. Dal 1° luglio 2021 la procedura da utilizzare è telematica (online): https://servizi.gpdp.it/databreach/s/.

Al fine di poter effettuare la suddetta procedura entro le 72 ore richieste dal Regolamento, il personale è tenuto, quindi, ad avvisare tempestivamente il Coordinatore del Centro, anche per il tramite del referente interno in materia di protezione dei dati, nominato con provvedimento del Coordinatore del Centro di cui al prot. n. 006635/2021 del 29/01/2021, qualora si abbia evidenza o anche solo il sospetto che sia in corso una violazione dei dati personali, in modo da consentire, nel caso di accertate eventuali violazioni, l'esecuzione delle procedure di notifica secondo le modalità e i termini stabiliti dagli artt. 33 e 34 del Regolamento. E' quindi obbligo per ciascun dipendente del Centro individuare e segnalare al responsabile interno del

Centro, che a sua volta è tenuto a dare comunicazione al Responsabile della Protezione dei Dati del CNR, tempestivamente e comunque non oltre 24 ore, un'eventuale *Data Breach*, o violazione dei dati, di sua competenza e che abbia colpito il suo sistema o altri del Centro. L'obbligo di segnalazione riguarda ogni violazione di cui si abbia conoscenza.

Un tipico *Data Breach* consiste in: a) furto o smarrimento di un computer fisso o di un dispositivo portatile (es. pc portatile, disco removibile, *pen-drive* USB); b) accesso dall'esterno ai dati del Centro da parte di un criminale informatico; c) distruzione o alterazione accidentale di dati e informazioni; d) divulgazione di dati confidenziali a persone non autorizzate; e) perdita o furto di documenti cartacei contenenti dati particolari; f) divulgazione al pubblico di dati riservati; g) virus o altri attacchi al sistema informatico o alla rete; h) violazione di misure di sicurezza fisica quali, ad esempio, la forzatura di porte o finestre di particolari locali (sale macchine, depositi dei nastri del *backup*, archivi anche cartacei, locali contenenti informazioni riservate); i) invio accidentale di e-mail contenenti dati personali e/o particolari al destinatario sbagliato; l) in generale, qualsiasi situazione che possa portare un soggetto non autorizzato alla conoscenza o disponibilità di dati personali.

Nel caso in cui il computer fisso, il pc portatile, l'*hard disk*, dispositivi USB o altri supporti di memoria fossero oggetto di furto o smarrimento, occorre che il titolare nella figura del responsabile interno del Centro segnali immediatamente l'avvenimento al Responsabile della Protezione dei Dati del CNR e all'Ufficio ICT. Vanno segnalati anche tutti gli incidenti comunque correlati ai dati, quali furto di informazioni effettuate online, cancellazione accidentale di informazioni, comunicazione di informazioni a terzi per errore. Ciò anche se non vi sia stata una violazione intenzionale ma un evento accidentale.

2.11 - Riferimenti Normativi

1. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) aggiornato con le rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea n.127 del 23 maggio 2018.

2. Decreto legislativo 30 giugno 2003, n.196 recante il “Codice in materia di protezione dei dati personali” (S.O n. 123 alla Gazzetta Ufficiale n. 174 del 29 luglio 2003) integrato con le modifiche introdotte dal Decreto legislativo 10 agosto 2018, n. 101, recante “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE - Regolamento generale sulla protezione dei dati)” (Gazzetta Ufficiale n.205 del 4 settembre 2018).

3. Decreto legislativo 10 agosto 2018, n. 101 “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE -Regolamento generale sulla protezione dei dati” (Gazzetta Ufficiale n.205 del 4 settembre 2018).

4. Decreto legislativo 25 novembre 2016, n. 218 “Semplificazione delle attività degli enti pubblici di ricerca ai sensi dell’articolo 13 della legge 7 agosto 2015, n. 124”, art.2 Carta Europea dei Ricercatori (Gazzetta Ufficiale Serie Generale n. 276 del 25 novembre 2016).

5. Decreto-legge 8 ottobre 2021, n. 139 (c.d. Decreto Capienze) “Disposizioni urgenti per l’accesso alle attività culturali, sportive e ricreative, nonché per l’organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali” convertito con modificazioni nella Legge 3 dicembre 2021, n. 205 che ha apportato modifiche al Codice privacy - art.9 (Gazzetta Ufficiale Serie Generale n. 291 del 7 dicembre 2021).

6. Garante per la protezione dei dati personali, “Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice - 13 dicembre 2018” (Registro dei provvedimenti n. 497 del 13 dicembre 2018).

7. Garante per la protezione dei dati personali, “Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico” - 14 giugno 2007 (Gazzetta Ufficiale n. 161 del 13 luglio 2007) - Applicabili in quanto compatibili con il Regolamento.

8. Garante per la protezione dei dati personali, “Lavoro: le linee guida del Garante per posta elettronica e internet” (Gazzetta Ufficiale n. 58 del 10 marzo 2007).

9. Garante per la protezione dei dati personali, Provvedimento del 27 maggio 2021 - Procedura telematica per la notifica di violazioni di dati personali (data breach), (Registro dei provvedimenti n. 209 del 27 maggio 2021).

10. Gruppo di Lavoro Articolo 29 per la protezione dei dati personali, “Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679” del 3 ottobre 2017, come modificate in ultimo il 6 febbraio 2018.

11. Garante per la protezione dei dati personali, “Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021” (Gazzetta Ufficiale n. 163 del 9 luglio 2021).

12. Garante per la protezione dei dati personali, “Guida all’applicazione del Regolamento europeo in materia di protezione di dati personali”, edizione aggiornata febbraio 2018.

13. Garante per la protezione dei dati personali, “Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d’impatto sulla protezione dei dati ai sensi dell’art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018” (Gazzetta Ufficiale n. 269 del 19 novembre 2018).

14. Gruppo di Lavoro Articolo 29 per la protezione dei dati personali, “Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento “possa presentare un rischio elevato” ai sensi del Regolamento 2016/679 - WP248 rev.01”,

adottate il 4 aprile 2017, versione successivamente emendata e adottata il 4 ottobre 2017, tratto dalla pagina web.

15. Notifica delle violazioni dei dati personali (data breach) procedura telematica (on line): https://servizi.gpdp.it/databreach/s/.

16. Informativa ai sensi dell'art.13 del Reg.(UE) 2016/679 per il trattamento dei dati personali in relazione alla gestione del rapporto di lavoro tra il Consiglio Nazionale delle Ricerche e il personale del Centro Interdipartimentale per l'Etica e l'Integrità nella Ricerca.