

**VALUTAZIONE D’IMPATTO PER PROGETTI DI RICERCA IN AMBITO SANITARIO**

**SU DATI RETROSPETTIVI**

**(ART. 110 D. LGS. 196/2003, Provvedimento Garante n. 146/2009)**

La valutazione di impatto (DPIA) consente di identificare in modo puntuale i rischi per la protezione dei dati personali quando vengono pianificati nuovi progetti di ricerca o aggiornati progetti di ricerca in corso e di individuare le azioni necessarie per mitigare tali rischi.

**Una valutazione di impatto, secondo l’Autorità Garante per la protezione dei dati personali, deve sempre essere effettuata negli studi retrospettivi quando:**

* il trattamento dei dati personali è su larga scala;
* vengono trattate categorie particolari di dati, ad esempio dati genetici;
* l’attività comporta il data linkage di molteplici e diversi archivi di dati;
* l’attività prevede la rilevazione di dati per individui vulnerabili (minori, soggetti con patologie psichiatriche, anziani, ecc.);
* la base giuridica per il trattamento dei dati non è riferibile al consenso al trattamento, a ricerche condotte sulla base di disposizioni di legge o regolamento o al diritto, o ad altre specifiche fattispecie previste dal GDPR e dal Codice Privacy.

**Titolo dello studio** Rene e sport: incidenza e prevalenza di anomalie urinarie in giovani atleti sottoposti a visita medico-sportiva agonistica

**Codice di Protocollo** 113/2024/OSS\*/AUSLMO SIRER ID 7271 – Rene&Sport “

**Titolare del trattamento: AZIENDA USL DI MODENA**

**U.O.C. Servizio** Medicina dello Sport-Ausl Modena

**Soggetto delegato:** Dott. Gustavo Savino

**Data compilazione 08/06/2024**

|  |  |
| --- | --- |
| **TRATTAMENTO DEI DATI** |  |
| **Descrizione del trattamento** *(compilare i campi successivi o allegare il modulo di fattibilità dello studio)* |  |
| ***Obiettivi dello studio*** | L’obiettivo dello studio è di stimare la prevalenza di anomalie urinarie in giovani atleti sottoposti a visita medico sportiva per concessione di idoneità alla pratica di attività sportiva agonistica. |  |
| ***Breve sintesi del progetto; numero pazienti arruolati, anni di riferimento, esplicitazione dei motivi per cui non è possibile acquisire il consenso di tutti i pazienti o di parte di essi, descrizione delle attività poste in essere per contattare gli interessati***  | Saranno raccolti i dati dei soggetti che hanno svolto visita per idoneità agonistica presso il servizio di Medicina dello Sport dell’AUSL di Modena (via Rita Levi Montalcini) nel periodo che va da 01/01/2023 al 31/12/2023. Gli atleti agonisti che hanno svolto una visita medico sportiva agonistica nella sede indicata precedentemente sono circa 5000. Lo scopo dello studio è quello di stimare la prevalenza di anomalie urinarie in giovani atleti sottoposti a visita medico sportiva per concessione di idoneità alla pratica di attività sportiva agonistica. Lo Studio non garantisce che sia sempre possibile raccogliere il consenso informato dei pazienti potenzialmente arruolabili, in quanto all’esito di ogni ragionevole sforzo compiuto per contattarli (anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l’impiego dei recapiti telefonici eventualmente forniti, nonché l’acquisizione dei dati di contatto presso l’anagrafe degli assistiti o della popolazione residente) alcuni di essi potrebbero risultare deceduti o non contattabili, in conformità alle previsioni del GDPR n. 2016/679, dell’art. 110 del D. Lgs. 196/2003, come modificato dalla L. 56/2024 e dal Provvedimento del Garante per la protezione dei dati personali n. 146 del 05/06/2019. |  |
| ***Promotore*** | Prof. Maria Grazia Modena |  |
| **Tipologia di dati raccolti**  |  |
| ***Modalità di raccolta*** *(barrare anche più caselle)* | [x] consultazione cartelle cliniche/documentazione sanitaria[ ]  archivi di dati clinici[ ]  archivi di test diagnostici[ ]  dati di laboratorio [ ]  altro (specificare)Fare clic o toccare qui per immettere il testo. |  |
| ***Trattamento dei dati*** *(indicare il supporto utilizzato per la rilevazione e conservazione dei dati)* | Formato digitaleSe altro, specificare:Fare clic o toccare qui per immettere il testo. |
| ***Categorie di persone interessate*** | [ ]  Pazienti[x]  Persone sane[ ]  Operatori sanitari[ ]  Soggetti vulnerabili[ ]  Altro (specificare)Fare clic o toccare qui per immettere il testo. |
| ***Categorie di dati trattati*** | [x]  dati sulla salute fisica o psichica[ ]  dati genetici [ ]  informazioni sulla vita sessuale[ ]  informazioni sull’orientamento sessuale[ ]  informazioni sugli stili di vita e le condizioni socioeconomiche[ ]  informazioni su istruzione e formazione professionale[ ]  anamnesi lavorativa[ ]  informazioni su religione o altre credenze[ ]  altro (specificare)Fare clic o toccare qui per immettere il testo. |  |
| ***I dati personali (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono comunicati/condivisi con altri?*** | [ ] No[x] SìSe sì, selezionare uno o più ambiti di comunicazione:[ ] Promotori[ ] CRO[ ] Altro X PromotoriCROaltro (specificare)Il Centro sperimentatore condivide i dati attraverso un file Excel protetto da password |  |
| ***I dati personali (pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono trasferiti all’estero?*** | [x] No[ ] SìSe sì:[ ] Paesi Area UE[ ] Paesi Area EXTRA UEIn quale/i Paese/i all’interno dell’area o extra UE?Fare clic o toccare qui per immettere il testo. |  |
| **Misure di protezione dei dati** |  |
| ***Verranno conservati i dati identificativi dei soggetti dello studio?*** | [x] No[ ] SìSe sì, specificare le ragioni sottese a tale esigenza:Fare clic o toccare qui per immettere il testo. |  |
| ***Descrivere le procedure utilizzate per*** ***a) non identificare direttamente o pseudonimizzare*** ***b) rendere anonimi i dati dei partecipanti nelle diverse fasi della ricerca******ALTERNATIVI*** | 1. Per non identificare direttamente l’interessato sono adottate le seguenti misure:

[ ]  Adozione di tecniche crittografiche[x]  Utilizzo di codici univoci per ciascun partecipante. Solo il responsabile della ricerca o altri soggetti autorizzati, possono (con l’uso di mezzi ragionevoli) collegare i codici all’identità dei partecipanti[ ]  Altro, specificare in dettaglioFare clic o toccare qui per immettere il testo.1. Per rendere anonimi o aggregare i dati, anche in un momento successivo alla raccolta, sono adottate le seguenti misure:

[ ]  I dati personali, a seguito della raccolta sono eliminati definitivamente senza la possibilità di risalire ai dati originali[ ]  I dati personali sono sostituti da uno o più identificatori, che possono essere utilizzati per un set di dati o per ogni singolo dato con distruzione del dato personale originario[ ]  Sono distrutti i dati che possono essere idonei a identificare gli interessati e sono conservati i soli dati aggregati[ ]  Altro (specificare) Fare clic o toccare qui per immettere il testo. |  |

|  |  |
| --- | --- |
| **PRINCIPI, FINALITA’ E BASI GIURIDICHE** |  |
| **Necessità e proporzionalità** |  |
| ***Sono trattati solo i dati necessari e pertinenti al perseguimento delle finalità della ricerca (Minimizzazione)?*** | [x]  Sì [ ]  NoSe no, specificare i motivi e le azioni previste Fare clic o toccare qui per immettere il testo. |  |
| **Integrità ed esattezza** |  |
| ***Sono state messe in campo azioni per garantire l’integrità ed esattezza dei dati?*** | [x]  Sì [ ]  NoSe no, specificare i motivi e le azioni previste Fare clic o toccare qui per immettere il testo. |
| **Limitazione della conservazione** |  |
| ***Per quanto tempo verranno conservati i dati raccolti?*** | Indicare il numero di anni 7Decorso tale termine i dati verranno:[x]  Anonimizzati completamente[ ]  Distrutti[ ]  altro (*specificare*)Fare clic o toccare qui per immettere il testo. |  |
| **Basi giuridiche**  |  |
| ***Quali sono le basi giuridiche del trattamento?*** | [ ]  art. 9, par. 2, lett. j) GDPR[[1]](#footnote-1) [ ]  art. 110, co. 1 primo periodo Codice Privacy[[2]](#footnote-2) [x]  art. 110, co. 1, secondo periodo Codice Privacy[[3]](#footnote-3)  |  |

|  |
| --- |
| **MISURE A TUTELA DEI DIRITTI DELL’INTERESSATO** |
| **Informativa e consenso** |
| ***SOLO SE LA BASE GIURIDICA È L’ART. 110, CO. 1, SECONDO PERIODO******Indicare i motivi per i quali non è possibile fornire l'informativa ai partecipanti allo Studio (soggetti interessati) e acquisirne il consenso*** | [ ]  motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione[x]  sebbene sia stato svolto ogni ragionevole sforzo organizzativo, non è possibile contattare gli interessati in ragione: [x]  del numero molto alto di interessati che è stato stimato [ ]  deceduti o non contattabili |
| ***Nel caso di studi retrospettivi su dati genetici, ove non sia possibile ottenere il consenso informato, indicare se ricorrono le condizioni indicate*** | [ ]  indagini statistiche o ricerche scientifiche previste dal diritto dell’Unione europea, dalla legge o, nei casi previsti dalla legge, da regolamento[ ]  scopi scientifici e statistici direttamente collegati con quelli per i quali è stato originariamente acquisito il consenso informato degli interessati[ ]  sebbene sia stato svolto ogni ragionevole sforzo organizzativo, non è possibile contattare gli interessati e il programma di ricerca comporta l’utilizzo di campioni biologici e di dati genetici che in origine non consentono di identificare gli interessati, ovvero che, a seguito di trattamento, non consentono di identificare i medesimi interessati e non risulta che questi ultimi abbiano in precedenza fornito indicazioni contrarie |
| **Esercizio da parte dell’interessato dei diritti ex artt.15-22 DPR** |
| ***E’ stata predisposta una procedura ad hoc da parte dell’Ente?*** |  X Sì* No
 |

|  |
| --- |
|  **MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO** (standardizzare per singola Azienda) |
| **MISURA** | Esistenti | Note |
| Organigramma interno | X | Delibera 227/2018 |
| Nomine responsabili esterni | Non sono presenti  |  |
| Nomina DPO | X | Delibera 110/2018 e ss. |
| Informativa  | X | Sempre |
| Istruzioni persone autorizzate trattamento | X | Emanuela Paoloni, Maria Luisa Poli, Roberta D’Alisera. |
| Formazione | X | Non necessaria |
| Registri | X  | Non sono presenti dei registri specifici |
| Procedure | X | Non sono presenti delle procedure specifiche |
| Politiche di tutela della privacy | X | AUSL MODENA ha nominato un DPO e ha prodotto procedure di adeguamento alla normativa privacy quali ad esempio: riorganizzazione organigramma, regolamento privacy, disciplinare sull’utilizzo degli strumenti informatici….  |
| Distruzione/smaltimento sicuro cartaceo | X |  |
| Inventario degli asset | X | Le postazioni di lavoro aziendali sono censite nel programma di gestione aziendale. Non è prevista una abilitazione specifica per le postazioni utilizzate per l’accesso alla cartella condivisa  |
| Misure anti – intrusive (cartelli di divieto di accesso ai locali, strumenti per la rilevazione degli accessi, guardiania, portineria, serrature armadi, schedari, ecc.) | X | I sistemi server sono ospitati presso il Data Center aziendale che risponde ai requisiti tier 3 ed anche i Datacenter regionali gestiti da Lepida S.c.p.A rispondono ai requisiti tier 3 |
| Politiche di sicurezza informatica | X | Sulle postazioni aziendali e sul file server viene garantito l’aggiornamento dei Sistemi Operativi e di un programma di antivirus e di anti-malware completo. Sul file server è anche attivo il firewall locale |
| Controllo accessi (log) | X | Essendo una cartella condivisa non sono presenti politiche di audit all’accesso |
| Antivirus / firewall | X | Antivirus presenti e gestiti sia sui PC che sul file server (vedi sopra)File server protetto da firewall di Datacenter (non firewall locale) |
| Politiche di clear screen | X | Attivate sui PC Aziendali (timeout e nuova richiesta di utente e password per lo sblocco) |
| Back – up dei dati | X | La cartella condivisa utilizzata come unità di memorizzazione dello studio è situata nei file server aziendali e viene quotidianamente salvata attraverso le normali procedure di Backup aziendali su due copie, una locale e una remota presso il datacenter di Lepida di Modena |
| Politiche di trasmissione dei dati | x | Trasmissione sicura dei dati da Ausl a Unimore mediante posta elettronica e file protetto da pwd (pwd comunicata o concordata con mezzo diverso) |
| nel caso si utilizzi un sito web esterno: | x | Per questo studio non si usa un sito web esterno |
| Connessione sicura | x | La cartella condivisa è accessibile solo dall’interno dell’Azienda AUSL di Modena, NON vengono usati protocolli di criptazione/protezione della connessione ma la connessione tra i PC ed il file server è protetta dal firewall di datacenter. |
| Accesso protetto da utenza personale | x | La cartella condivisa è accessibile ai soli utenti autorizzati e identificati con credenziali di Active Directory |
| Crittografia |  | Lo strumento utilizzato per la raccolta dati (Excel)non prevede la crittografazione |
| Anonimizzazione |  |  |
| Pseudonimizzazione | x | Codici identificativi alfanumerici |
| Sicurezza dei documenti cartacei |  | I dati non vengono raccolti in formato cartaceo |
| Gestione postazioni | X | Le postazioni sono accessibili dai soli utenti aziendali. È presente un disciplinare aziendale sull’utilizzo delle postazioni informatiche |
| Autenticazione | X | L’autenticazione avviene tramite username/password. La password è cambiata ogni 90 giorni secondo le normative vigenti |
| Policy di gestione data breach | X | L’Azienda ha adottato una procedura di gestione delle violazioni dei dati personali in cui sono definite le modalità operative da seguire in caso di incidente. La medesima procedura viene fornita ai Responsabili del trattamento in quanto disciplina anche le violazioni esterne all’Azienda. È previsto un registro aziendale delle violazioni |
| Altro: |  |  |

|  |
| --- |
| **MINACCE** |
| **ACCESSO ILLEGITTIMO AI DATI** |
| **Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?**Perdita di riservatezza dei dati personali coperti da segreto professionale; perdita del controllo dei propri dati; decifratura non autorizzata dei dati pseudonimizzati; diffusione dei dati non autorizzata**Quali sono le principali minacce che potrebbero concretizzare il rischio?**Utilizzo inappropriato delle password di accesso ai pc aziendali e al database di raccolta dati; sottrazione delle password di accesso da parte di un terzo; operatori abilitati che sfruttano i privilegi di accesso per accedere illegittimamente alle informazioni; attacco informatico; errata profilazione degli utenti; virus**Quali sono le fonti di rischio?**Fonti umane interne (lasciare incustodita la postazione di lavoro, errore di integrazione applicativa). Fonti umane esterne (hacker). Fonti non umane (virus, applicativi che interoperano con il SW, introduzione di bug in seguito ad aggiornamento dell'applicativo)**Quali misure fra quelle individuate contribuiscono a mitigare il rischio?**Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; Controllo accessi (log); Antivirus/firewall; Politiche di trasmissione dei dati; Crittografia; Pseudonimizzazione**Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?**Bassa: l’impatto sugli interessati potrebbe essere elevato, tuttavia le misure previste per evitare gli accessi non autorizzati rendono limitata la probabilità di accadimento **Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?**Molto bassa: le politiche di sicurezza informatica e le misure adottate a protezione delle postazioni di lavoro e degli archivi cartacei rendono quasi nulla la probabilità di accadimento |
| **MODIFICHE INDESIDERATE DEI DATI** |
| **Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?**Perdita di integrità del dato; la modifica potrebbe essere definitiva e avere conseguenze sulla attendibilità dei risultati dello studio fino a conseguenze sulla cura dei pazienti**Quali sono le principali minacce che potrebbero concretizzare il rischio?**Utilizzo inappropriato delle password di accesso ai pc aziendali e al database di raccolta dati; sottrazione delle password di accesso da parte di un terzo; operatori abilitati che sfruttano i privilegi di accesso per accedere illegittimamente alle informazioni; attacco informatico; errata profilazione degli utenti; virus**Quali sono le fonti di rischio?**Fonti umane interne (lasciare incustodita la postazione di lavoro, alterazione volontaria di dati, errore umano involontario). Fonti umane esterne (hacker). Fonti non umane (virus, applicativi che interoperano con il SW)**Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?**Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; Controllo accessi (log); antivirus/firewall; Back – up dei dati**Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?**Bassa: l’impatto sugli interessati potrebbe essere elevato, tuttavia le misure di gestione dell'accesso all'applicativo e le misure adottate a protezione delle postazioni di lavoro riducono notevolmente la probabilità di accadimento. **Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?**Molto bassa: le misure adottate a protezione delle postazioni di lavoro rendono quasi nulla la probabilità di accadimento,  |
| **PERDITA DI DATI** |
| **Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?**Una perdita dei dati potrebbe causare l’alterazione dei risultati dello Studio o la impossibilità di proseguire lo Studio; tuttavia non si tratta di dati originali**Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?** La minaccia principale è quella di una distruzione o cancellazione erronea o volontaria dei dati Le principali minacce possono essere di natura informatica (infezione da ransomware che blocca il sistema di accesso ai propri data base, provocando anche solo in modo temporaneo una impossibilità ad accedere al server, guasto che determina il danneggiamento, l'interruzione o la non disponibilità del sistema, che andando a colpirne elementi chiave possa mettere a rischio la disponibilità dei dati) o derivare da una azione umana (utilizzo improprio della posta elettronica da parte di un operatore attraverso cui un virus potrebbe bloccare il sistema aziendale; Incidente tecnico al datacenter (incendio, inondazione, fulmini…)**Quali sono le fonti di rischio?** Fonti umane interne (operatori autorizzati che abusino del proprio ruolo o colposamente operino cancellazioni sui dati per inesperienza o imperizia; lasciare incustodita la postazione di lavoro; errore progettuale/realizzativo che opera una modifica impropria ai dati gestiti); Fonti umane esterne (hacker); Fonti di rischio non umane (virus informatico; calamità naturali; guasto all'impianto elettro-idraulico del datacenter)**Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?**Back – up dei dati; Controllo accessi (log); Misure anti – intrusive; antivirus/firewall; Tracciabilità, Gestione postazioni; Politiche di tutela della privacy¸ Politiche di sicurezza informatica**Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?**Molto bassa: i dati non sono originali, quindi l’impatto sugli interessati non è elevato, inoltre le misure previste per evitare la perdita dei dati rendono limitata la probabilità che essa si verifichi**Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?**Molto bassa: le misure adottate a protezione delle postazioni di lavoro rendono quasi nulla la probabilità di accadimento |

**VALUTAZIONE DEL RISCHIO**

|  |  |  |
| --- | --- | --- |
| ***PROBABILITA’ (P)*** | ***IMPATTO (I)*** | ***RISCHIO (R=P\*I)*** |
| Probabilità molto bassa: 1Probabilità bassa: 2Probabilità media: 3Probabilità alta: 4Probabilità molto alta: 5 | Impatto molto basso: 1Impatto basso: 2Impatto medio: 3Impatto alto: 4Impatto molto alto: 5 | Rischio basso: R< 7Rischio medio: 7<R<11Rischio alto: R>11 |

**MATRICE DI VALUTAZIONE DEL RISCHIO**

|  |  |  |
| --- | --- | --- |
|  |  | **IMPATTO§§** |
| **PROBABILITA’** | **MOLTO ALTO§** | 5 | 10 | 15 | 20 | 25 |
| **ALTO** | 4 | 8 | 12 | 16 | 20 |
| **MEDIO** | 3 | 6 | 9 | 12 | 15 |
| **BASSO** | 2 | 4 | 6 | 8 | 10 |
| **MOLTO BASSO** | 1 | 2 | 3 | 4 | 5 |
|  |  | **MOLTO BASSO** | **BASSO** | **MEDIO** | **ALTO** | **MOLTO ALTO** |

**§** Frequenza con la quale si possono verificare criticità nel trattamento dei dati: **Rischio molto basso**: è probabile che non si verifichi mai; **Basso**: non è probabile che si verifichi, ma può accadere; **Medio**: si può verificare occasionalmente; **Alto**: è probabile che si verifichi, ma non in modo persistente/stabile; **Molto alto**: è quasi certo che si verifichi, possibilmente in modo frequente

**§§** Impatto atteso: **Molto basso**: è improbabile che possa avere un qualsiasi impatto; **Basso**: può avere un impatto; **Medio**: è probabile che abbia un impatto; **Alto**: molto probabile che abbia un impatto significativo; **Molto alto**: correlato ad un impatto maggiore

**minacce’SSORISCHIOZZATOZZATA**

|  |  |  |  |
| --- | --- | --- | --- |
| **MINACCIA** | **VALORE DEL RISCHIO (P\*I)** | **LIVELLO DI RISCHIO** | **VALUTAZIONE COMPLESSIVA (SOMMA COLONNA LIVELLO RISCHIO)** |
| **ACCESSO ILLEGITTIMO** | 2\*1 | 2 | **5** |
| **MODIFICHE INDESIDERATE DEI DATI** | 2\*1 | 2 |
|  **PERDITA DI DATI** | 1\*1 | 1 |

|  |  |
| --- | --- |
| **Classificazione** | **Intervallo del rischio** |
| Assenza di Rischio | Valore finale tra 0 e 1 compresi |
| Rischio Basso | Valore finale tra 2 e 6 compresi |
| Rischio Medio | Valore finale tra 7 e 11 compresi |
| Rischio Elevato | Valore finale tra 12 e 16 compresi |

1. il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. [↑](#footnote-ref-1)
2. Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità' all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento. [↑](#footnote-ref-2)
3. Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. [↑](#footnote-ref-3)