ACCREDIA

L'ENTE ITALIANO DI ACCREDITAMENTO

UNI EN ISO 20387:2020 E PRIVACY

Milano, 8 Aprile 2022

Dipartimento Laboratori di taratura

ACCREDIA

L'ENTE ITALIANO DI ACCREDITAMENTO

Avv. Francesca Marchini

Esperto Tecnico Accredia Privacy Biobanche

Milano, 8 Aprile 2022

OBIETTIVO DELL'INCONTRO

Il presente incontro ha il fine di condividere il percorso del trattamento del dato personale secondo la ISO 20387 e la disciplina Privacy in materia.
Non vi è pertanto alcun indirizzo nei confronti delle biobanche circa le loro attività di gestione della conformità in tale ambito, atteso che le biobanche individualmente operano le relative valutazioni applicative in funzione del proprio contesto organizzativo.

UNI EN ISO 20387:2020 E PRIVACY

- **Disciplina Privacy e logiche privacy**
  - GDPR
  - D.Lgs. 101/2018
  - Provv. Garante n.146/2019

- **UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy**
  - Definizioni
  - Requisiti norma
  - Disciplina Privacy
  - Controlli Privacy

- **Conclusioni**

Fonti normative - disciplina e logiche Privacy

GDPR + D.LGS.196/2003 Codice Privacy + D.LGS 101/2018 che novella Codice Privacy + PROVVEDIMENTI GARANTE PROTEZIONE DEI DATI

GDPR → Vigente da maggio 2016 Cogente da 25 maggio 2018

D.LGS 101/2018 che novella Codice Privacy → Vigente Da 19 Settembre 2018

Fonti normative – disciplina e logiche Privacy

PROVVEDIMENTI GARANTE PROTEZIONE DEI DATI

Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.s. 10 agosto 2018, n. 146 del 5 giugno 2019 All. n. 4 e 5

All. n. 4 Prescrizioni relative al trattamento dei dati genetici (aut. gen. n. 8/2016)

All. 5 Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016)

Fonti normative – disciplina e logiche Privacy

Consapevolezza

Dimostrabilità

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy
Definizioni

TRATTAMENTO

GDPR

CLASSIFICAZIONE DEI DATI

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, processi automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la strutturazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la limitazione, la cancellazione e la distruzione dei dati, anche se non registrati in una banca dati.

Personali: qualunque informazione relativa alla persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale

Comuni: tutti i dati che non sono Sensibili o Giudiziari: nome, indirizzo, numero di identificazione, identificativo online

«Sensibili»: Categorie particolari di dati personali: i dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita e orientamento sessuale, dati biometrici e genetici

Giudiziari: I dati personali idonei a rivelare provvedimenti in materia di casellario giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reato e relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi del codice di procedura penale.

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy
Definizioni

ISO 20387

3.3 Dati associati: Ogni informazione collegata al materiale biologico, compresi ma senza limitarsi ad essi dati, fenotipici, clinici, epidemiologici procedurali e di ricerca

3.12 Catena di custodia: Responsabilità o controllo dei materiali e dati associati mano a mano che si spostano attraverso ciascun passaggio di un processo

3.14 Reclamo: Espressione di malcontento, diverso dal ricorso, da parte di una persona o di una organizzazione nei confronti di una biobanca, relativamente alla attività prodotti o risultati di tale biobanca in cui si prevede una risposta

3.18 Distruzione: Processo di eliminazione del materiale biologico e/o eliminazione dei dati associati, oltre ogni possibile ricostruzione

3.19 Smaltimento: Atto di rimuovere un materiale biologico e/o dati associati, solitamente per l'eliminazione, la distruzione o la restituzione al fornitore

3.20 Distribuzione: Processo di fornitura di materiale biologico selezionato e/o dati associati al destinatario/utilizzatore

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy
Definizioni

ISO 20387

3.21 Informazioni documentate: informazioni che devono essere tenute sotto controllo e mantenute da parte di un'organizzazione ed il mezzo che le contiene

3.22 donatore: Entità organica, come per esempio un essere umano, animale, pianta ecc. dalla quale sono raccolti materiale biologico e/o dati associati per il «biobanking»

3.33 Personale: Persona(e) dipendente (i) o che lavora(no) per la biobanca

3.36 Processamento: Esecuzione di ogni attività sul materiale biologico e dati associati durante tutte le fasi del ciclo di vita (dalla raccolta, se applicabile, acquisizione o ricezione alla distribuzione, smaltimento o distruzione (3.29))

3.41 fornitore; depositante: Persona o entità dalla quale il materiale biologico e/o i dati associati è ricevuto o acquisito per biobanking

3.42 pseudonimizzazione: processamento dei dati in modo tale che questi dati non più essere attribuita uno specifico soggetto dei dati senza 'utilizzo di informazioni aggiuntive

3.44 destinatario: Persona o entità alla quale il materiale biologico è distribuito.

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

Requisiti Norma

4
RISERVATEZZA

- **4.3.1** proteggere info riservate di donatori, destinatari, utilizzatori
- **4.3.2** accordi riservatezza e informativa donatore/fornitore
- **4.3.4** obbligo riservatezza del Personale

5
REQUISITI STRUTTURALI

- **5.3** governance della BBK per questioni scientifiche, amministrative, tecniche e altre
- **5.4** BBK responsabile per attività eseguite al proprio interno

6
REQUISITI RELATIVI ALLE RISORSE

- **6.2.1.2** riservatezza personale
- **6.2.1.4** compiti e responsabilità del personale
- **6.2.3.1 Formazione**
- **6.4.1.2 fornitori selezionati per conformità ai requisiti**
- **6.5.1** accessi controllati
- **6.5.4** attrezzature critiche

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

Requisiti Norma

7
REQUISITI DI PROCESSO

- **7.1.1 ciclo di vita materiale biologico e dati associati identificati e processi definiti e verificati**
- **7.2.3.4** principi etici e consenso
- **7.3.2.4 isolamento mat. Biologico e dati associati per verifica conformità legale/etica prima utilizzo**
- **7.4.7** trasferimento dati progettato per assicurare integrità e riservatezza
- **7.7.4** ubicazione della conservazione materiale biologico e dati associati
- **7.7.8** revoca consenso paziente
- **7.11.2 - 3** output non conforme e comunicazione
- **7.13** gestione reclami

8
REQUISITI SISTEMA GESTIONE QUALITA'

- **8.5.1 azioni per affrontare rischi e opportunità**
- **8.5.2** piani di azioni per affrontare rischi/opportunità
- **8.5.3** proporzionalità delle azioni intraprese all'impatto potenziale sul biobanking
- **8.6.1 miglioramento**
- **8.7** azioni correttive output NC
- **8.8 audit interni**
- **8.9.1 riesame direzione SGQ: idoneità, adeguatezza, efficacia**

Requisiti ISO 20387 e GDPR

4
RISERVATEZZA

- **4.3.1** proteggere info riservate di donatori, destinatari, utilizzatori
- **4.3.2** informativa donatore/fornitore e accordi
- **4.3.4** obbligo riservatezza del Personale

GDPR/Autorizzazioni Garante PDP 146/2019

Art.32 GDPR – sicurezza del trattamento

4.3.1 proteggere info riservate di donatori, destinatari, utilizzatori

4.2 Prescrizioni specifiche custodia e la sicurezza dei dati genetici e dei campioni biologici

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

Disciplina Privacy

4
RISERVATEZZA

Art.32 GDPR – sicurezza del trattamento

Articolo 32 Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del **rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative a**deguate per garantire un **livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

Disciplina Privacy

4 RISERVATEZZA

Art.32 GDPR – sicurezza del trattamento

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

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

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

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

4 RISERVATEZZA

4.2 Prescrizioni specifiche custodia e la sicurezza dei dati genetici e dei campioni biologici

4.2 Prescrizioni specifiche

Per la custodia e la sicurezza dei dati genetici e dei campioni biologici sono adottate, in ogni caso, le seguenti cautele:

a) l'accesso ai locali deve avvenire secondo una documentata procedura prestabilita dal titolare del trattamento, che preveda l'identificazione delle persone, preventivamente autorizzate, che accedono a qualunque titolo dopo l'orario di chiusura. Tali controlli possono essere effettuati anche con strumenti elettronici. È ammesso l'utilizzo dei dati biometrici con riguardo alle richiamate procedure di accesso fisico, nel rispetto dei principi in materia di protezione dei dati personali e dei requisiti specifici del trattamento di cui all'art. 9 del Regolamento;

b) la conservazione, l'utilizzo e il trasporto dei campioni biologici sono posti in essere con modalità volte anche a garantirne la qualità, l'integrità, la disponibilità e la tracciabilità;

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

4
RISERVATEZZA

4.2 Prescrizioni specifiche custodia e la sicurezza dei dati genetici e dei campioni biologici

c) il trasferimento dei dati genetici, con sistemi di messaggistica elettronica ivi compresa la posta, è effettuato con le seguenti cautele: trasmissione dei dati in forma di allegato e non come testo compreso nel corpo del messaggio; cifratura dei dati avendo cura di rendere nota al destinatario la chiave crittografica tramite canali di comunicazione differenti da quelli utilizzati per la trasmissione dei dati; ricorso a canali di comunicazione protetti, tenendo conto dello stato dell'arte della tecnologia utilizzata; protezione dell'allegato con modalità idonee a impedire l'illecita o fortuita acquisizione dei dati trasmessi, come una password per l´apertura del file resa nota al destinatario tramite canali di comunicazione differenti da quelli utilizzati per la trasmissione dei dati. E' ammesso il ricorso a canali di comunicazione di tipo "web application" che prevedano l'utilizzo di canali di trasmissione protetti, tenendo conto dello stato dell'arte della tecnologia, e garantiscano, previa verifica, l'identità digitale del server che eroga il servizio e della postazione client da cui si effettua l'accesso ai dati, ricorrendo a certificati digitali emessi in conformità alla legge da un'autorità di certificazione

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

4
RISERVATEZZA

4.2 Prescrizioni specifiche custodia e la sicurezza dei dati genetici e dei campioni biologici

d) la consultazione dei dati genetici trattati con strumenti elettronici è consentita previa adozione di sistemi di autenticazione basati sull'uso combinato di informazioni note ai soggetti all'uopo designati e di dispositivi, anche biometrici, in loro possesso;
e) i dati genetici e i campioni biologici contenuti in elenchi, registri o banche di dati, sono trattati con tecniche di cifratura o di pseudonimizzazione o di altre soluzioni che, considerato il volume dei dati e dei campioni trattati, li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità, in modo da ridurre al minimo i rischi di conoscenza accidentale e di accesso abusivo o non autorizzato.
Laddove gli elenchi, i registri o le banche di dati siano tenuti con strumenti elettronici e contengano anche dati riguardanti la genealogia o lo stato di salute degli interessati, le predette tecniche devono consentire, altresì, il trattamento disgiunto dei dati genetici e sanitari dagli altri dati personali che permettono di identificare direttamente le persone interessate

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

4
RISERVATEZZA

4.2 Prescrizioni specifiche custodia e la sicurezza dei dati genetici e dei campioni biologici

Esempi controlli documentali e in campo per verificare conformità alle prescrizioni

- Controllo accessi
- Inform per dati biometrici autorizzati
- Procedure integrità/qualità tracciabilità campione e dato personale
- piano di formazione e suo aggiornamento su queste materie

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

4
RISERVATEZZA

4.2 Prescrizioni specifiche custodia e la sicurezza dei dati genetici e dei campioni biologici

Esempi controlli documentali e in campo per verificare conformità alle prescrizioni

- Allegato e-mail
- Cifratura email
- protezione tecnologica applicata all'allegato e livello di adeguatezza della sicurezza informatica
- piano di formazione e suo aggiornamento su queste materie

Requisiti ISO 20387 e GDPR

4
RISERVATEZZA

4
RISERVATEZZA

- **4.3.1** proteggere info riservate di donatori, destinatari, utilizzatori
- **4.3.2** accordi riservatezza - informativa donatore/fornitore
- **4.3.4** obbligo riservatezza del Personale

GDPR/Autorizzazioni Garante PDP 146/2019

Artt. 24 Responsabilità del titolare, art. 28 del responsabile

4.3.2 1° par. accordi riservatezza- informativa donatore/fornitore e uttilizzatore

4.11 Trattamento di dati genetici e campioni biologici per finalità di ricerca scientifica e statistica

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

4 RISERVATEZZA

4.3.2 1° par. informativa donatore/fornitore e utilizzatore
Accordi riservatezza

La BBK deve essere responsabile, attraverso impegni giuridicamente vincolanti della gestione delle informazioni riservate ottenute o create durante le attività di «biobanking».

Art. 24 Responsabilità del titolare

Art. 28 Responsabile del trattamento

4.11 Trattamento di dati genetici e campioni biologici per finalità di ricerca scientifica e statistica

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

4
RISERVATEZZA

Artt. 24 Responsabilità del titolare

Articolo 24 Responsabilità del Titolare del trattamento

1. Tenuto conto **della natura**, dell'ambito di applicazione, del **contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà** delle persone fisiche, il titolare del trattamento mette in atto misure **tecniche e organizzative** adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure **sono riesaminate** e aggiornate qualora necessario.

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

4.11 Trattamento di dati genetici e campioni biologici per finalità di ricerca scientifica e statistica

Il trattamento di dati genetici e campioni biologici per finalità di ricerca scientifica e statistica, è consentito solo se volto alla tutela della salute dell'interessato, di terzi o della collettività in campo medico, biomedico ed epidemiologico, anche nell'ambito della sperimentazione clinica o ricerca scientifica volta a sviluppare le tecniche di analisi genetica. Il trattamento deve essere svolto sulla base di un progetto redatto conformemente agli standard del pertinente settore disciplinare, anche al fine di documentare che il trattamento dei dati e l'utilizzo dei campioni biologici sia effettuato per idonei ed effettivi scopi scientifici. Il progetto specifica le misure da adottare nel trattamento dei dati personali per garantire il rispetto del presente provvedimento, nonché della normativa sulla protezione dei dati personali, anche per i **profili riguardanti la custodia e la sicurezza dei dati e dei campioni biologici, e individua gli eventuali responsabili del trattamento** (art. 28 Regolamento UE 2016/679). In particolare, laddove la ricerca preveda il prelievo e/o l'utilizzo di campioni biologici, il progetto indica l'origine, la natura e le modalità di prelievo e di conservazione dei campioni, nonché le misure adottate per garantire la volontarietà del conferimento del materiale biologico da parte dell'interessato.

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

4
RISERVATEZZA

4.11 Trattamento di dati genetici e campioni biologici per finalità di ricerca scientifica e statistica

Il progetto è conservato in forma riservata (essendo la consultazione del progetto possibile ai soli fini dell'applicazione della normativa in materia di protezione dei dati personali) per cinque anni dalla conclusione programmata della ricerca. Quando le finalità della ricerca possono essere realizzate soltanto tramite l'identificazione anche temporanea degli interessati, il titolare del trattamento adotta specifiche misure per mantenere separati i dati identificativi dai campioni biologici e dalle informazioni genetiche già al momento della raccolta, salvo che ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o richieda un impiego di mezzi manifestamente sproporzionato.

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

4 RISERVATEZZA

Art. 28 Responsabile del trattamento

Articolo 28 Responsabile del trattamento

1. Qualora un trattamento debba essere effettuato per **conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale** che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. **Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento.** Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

3. **I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

4
RISERVATEZZA

Art. 28 Responsabile del trattamento

a) tratti i dati personali soltanto **su istruzione documentata del titolare del trattamento**,
anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca **che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza**;

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

4 RISERVATEZZA

Art. 28 Responsabile del trattamento

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy
Controlli Privacy

4.11 Trattamento di dati genetici e campioni biologici per finalità di ricerca scientifica e statistica

Esempi controlli documentali e in campo per verificare conformità alle prescrizioni

Progetto: indicazione e misure per trattamento dei dati personali

Effettiva esistenza e adeguatezza delle misure di protezione dei dati personali presenti da progetto

- custodia e sicurezza dei dati personali dei dati e dei campioni biologici
- Termini di conservazione del Progetto

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy
Controlli Privacy

4 RISERVATEZZA

4.11 Trattamento di dati genetici e campioni biologici per finalità di ricerca scientifica e statistica

Esempi controlli documentali e in campo per verificare conformità alle prescrizioni

Progetto: indicazione misure per trattamento dei dati personali

Effettiva esistenza e adeguatezza delle misure di protezione dei dati personali presenti da progetto

Nomine a responsabili del trattamento ,modalità

Procedura per identificazione e archiviazione separata e riservata dati temporanei interessati

Requisiti ISO 20387 e GDPR

4
RISERVATEZZA

4
RISERVATEZZA

- **4.3.1** proteggere info riservate di donatori, destinatari, utilizzatori
- **4.3.2** accordi riservatezza **- informativa donatore/fornitore**
- **4.3.4** obbligo riservatezza del Personale

GDPR/Autorizzazioni Garante PDP 146/2019

Artt. 13 e 14

4.3.2 2° par. informativa donatore/fornitore

4.11.1 Informazioni agli interessati

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

4 RISERVATEZZA

4.3.2 2° par. informativa donatore/fornitore e accordi

Quando condivide dati o materiale biologico e dati associati, la BBK deve, dove possibile, informare il fornitore/donatore delle modalità con cui la sua privacy e riservatezza sono protette. La BBK deve rilasciare informazioni concernenti il materiale biologico e dati associati secondo accordi e approvazioni pertinenti (es: accordi contrattuali, documenti legalmente vincolanti, approvazioni etiche)

Artt 13 e 14 GDPR

4.11.1 Informazioni agli interessati

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

Disciplina Privacy

4
RISERVATEZZA

Art. 13 GDPR

Articolo 13 Informazioni da fornire qualora i dati siano raccolti presso l'interessato

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) **l'identità e i dati di contatto del titolare del trattamento** e, ove applicabile, del suo rappresentante;

b) i dati di contatto del **responsabile della protezione dei dati**, ove applicabile;

c) **le finalità del trattamento cui sono destinati** i dati personali nonché la base giuridica del trattamento;

d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

e) gli **eventuali destinatari o le eventuali categorie di destinatari** dei dati personali;

f) ove applicabile, **l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo** o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

Disciplina Privacy

4
RISERVATEZZA

Art. 13 GDPR

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, **il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:**

a) il **periodo di conservazione dei dati personali** oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o **la cancellazione degli stessi** o **la limitazione del trattamento** che lo riguardano o di opporsi al loro trattamento, oltre al **diritto alla portabilità dei d**ati;

c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di proporre reclamo a un'autorità di controllo;

e) **se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto**, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

Disciplina Privacy

4 RISERVATEZZA

4.11.1 Informazioni agli interessati trattamenti effettuati per scopi di ricerca scientifica e statistica nelle informazioni fornite agli interessati

In relazione ai trattamenti effettuati per scopi di ricerca scientifica e statistica nelle informazioni fornite agli interessati si evidenziano, altresì: a) gli accorgimenti adottati per consentire l'identificazione degli interessati soltanto per il tempo necessario agli scopi della raccolta o del successivo trattamento (art. 25 Regolamento UE 2016/679); b) le modalità con cui gli interessati, che ne facciano richiesta, possono accedere alle informazioni contenute nel progetto di ricerca. I trattamenti effettuati mediante test genetici, compreso lo screening, a fini di ricerca necessitano del consenso degli interessati; in questi casi agli interessati è richiesto di dichiarare se vogliono conoscere o meno i risultati della ricerca, comprese eventuali notizie inattese che li riguardano, qualora queste ultime rappresentino per gli interessati un beneficio concreto e diretto in termini di terapia o di prevenzione o di consapevolezza delle scelte riproduttive

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

Controlli Privacy

4 RISERVATEZZA

4.11.1 Informazioni agli interessati trattamenti effettuati per scopi di ricerca scientifica e statistica nelle informazioni fornite agli interessati

Esempi controlli documentali e in campo per verificare conformità alle prescrizioni

- **in concreto l'accesso alle informazioni** sia esercitabile per l'interessato
- **acquisizione consenso** per test genetici - screening per fini di ricerca
- se **c'è richiesta di interesse a conoscere o** no risultati della ricerca o notizie inattese che siano un beneficio concreto per terapia
- **riservatezza archivio** consensi

Requisiti ISO 20387 e GDPR

4
RISERVATEZZA

4
RISERVATEZZA

- **4.3.1** proteggere info riservate di donatori, destinatari, utilizzatori
- **4.3.2** accordi riservatezza - informativa donatore/fornitore
- **4.3.4 obbligo riservatezza del Personale**

GDPR/Autorizzazioni Garante PDP 146/2019

Art. 29 GDPR-Trattamento sotto l'autorità del titolare del trattamento e del responsabile del trattamento-art. 9 art. GDPR - art. 2-sexies del Codice

4.3.4 obbligo riservatezza del Personale -6.2.1.2 e 6.2.1.4 descrizione mansioni

4.6 Comunicazione e diffusione dei dati
Prescrizioni relative al trattamento dei dati genetici (aut. gen. n. 8/2016);

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy
Disciplina Privacy

4
RISERVATEZZA

Art. 29 -Trattamento sotto l'autorità del titolare del trattamento e del responsabile del trattamento e art. 9 GDPR e art. 2-sexies del Codice

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy
Disciplina Privacy

4
RISERVATEZZA

4.6 Comunicazione e diffusione dei dati Prescrizioni relative al trattamento dei dati genetici (aut. gen. n. 8/2016);

Il titolare o il responsabile del trattamento possono autorizzare per iscritto gli esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono designati a trattare dati genetici o campioni biologici, a rendere noti i medesimi dati all'interessato o ai soggetti di cui all'art. 82, comma 2, lettera a) del Codice. Nelle istruzioni alle persone autorizzate al trattamento dei dati sono individuate appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento di dati.

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy
Controlli Privacy

4.6 Comunicazione e diffusione dei dati Prescrizioni relative al trattamento dei dati genetici (aut. gen. n. 8/2016);

Esempi controlli documentali e in campo per verificare conformità alle prescrizioni su autorizzati al trattamento

- esistenza istruzioni alle persone autorizzate al trattamento
- completezza e coerenza delle lettere di autorizzazione rispetto al contesto della attività
- tipologia di controlli svolti

Requisiti ISO 20387 e GDPR

REQUISITI STRUTTURALI

- **5.3** governance della BBK per questioni scientifiche, amministrative, tecniche e altre
- **5.4** BBK responsabile per attività eseguite al proprio interno

Requisiti ISO 20387 e GDPR

5.3 La BBK deve avere un organo di governance/comitato consultivo che guidi e consigli la direzione su questioni scientifiche, tecniche e/o amministrative e altre

5.4 la BBK deve essere responsabile per le attività eseguite nelle proprie strutture/aree dedicate

Artt. 37=>39 GDPR: DPO

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

Disciplina Privacy

5 REQUISITI STRUTTRALI

Artt. 37=>39 GDPR: DPO

Articolo 37 Designazione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento **designano sistematicamente un responsabile** della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da **un'autorità pubblica o** da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) **le attività principali del titolare** del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala**; oppure

c) le **attività principali del** titolare del trattamento o del responsabile del trattamento consistono **nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.**

2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

Disciplina Privacy

5 REQUISITI STRUTTRALI

Artt. 37=>39 GDPR: DPO

3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un **unico responsabile della protezione dei dati può essere designato per più autorità pubbliche** o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

5. Il responsabile della protezione dei dati è **designato in funzione delle qualità professionali**, in particolare della **conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39**.

6. Il **responsabile della protezione** dei dati può essere un **dipendente del titolare** del trattamento o del responsabile del trattamento oppure **assolvere i suoi compiti in base a un contratto di servizi**.

7. **Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto** del responsabile della protezione dei dati e li comunica all'autorità di controllo.

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

Disciplina Privacy

5 REQUISITI STRUTTRALI

Artt. 37=>39 GDPR: DPO

CONTROLLI APPLICAZIONE Artt. 37=>39 GDPR: DPO

Esempi controlli documentali e in campo per verificare conformità alle prescrizioni su requisiti nomina

- conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati
- indipendenza
- informativa, i dati di contatto del DPO

Requisiti ISO 20387 e GDPR

6
REQUISITI RELATIVI ALLE RISORSE

6
REQUISITI RELATIVI ALLE RISORSE

- **6.2.1.2** riservatezza personale
- **6.2.1.4** compiti e responsabilità del personale
- **6.2.3.1 Formazione**
- **6.4.1.2 fornitori selezionati per conformità ai requisiti**
- **6.5.1** accessi controllati
- **6.5.4** attrezzature critiche

Requisiti ISO 20387 Zoom e GDPR

6.2.3.1 formazione

6.4.1.2 fornitori

GDPR Art. 25 - 32

GDPR Art. 28

Requisiti ISO 20387 e GDPR

6
REQUISITI RELATIVI ALLE RISORSE

6
REQUISITI RELATIVI ALLE RISORSE

- **6.2.1.2** riservatezza personale
- **6.2.1.4** compiti e responsabilità del personale
- **6.2.3.1** **formazione**
- **6.4.1.2 fornitori selezionati per conformità ai requisiti**
- **6.5.1** accessi controllati
- **6.5.4** attrezzature critiche

Requisiti ISO 20387 e GDPR

6.2.3.1 Formazione
Il Personale deve ricevere formazione appropriata e pertinente con aggiornamenti regolari per acquisire la necessaria competenza. La formazione deve essere documentata

- **Art. 25 GDPR** - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita
- **Art. 32 GDPR** Sicurezza del trattamento

Requisiti ISO 20387 e GDPR

6
REQUISITI RELATIVI ALLE RISORSE

6
REQUISITI RELATIVI ALLE RISORSE

CONTROLLI APPLICAZIONE 6.2.3.1 e Art. 25 con riferimento alla attività di formazione

Esempi controlli documentali e in campo per verificare conformità alle prescrizioni su requisiti norma

- documenti attestanti di formazione
- Piani di formazione
- Procedura by design e by default per trattamento dati personali collegati a dati genetici e campioni biologici.

Requisiti ISO 20387 e GDPR

6
REQUISITI RELATIVI ALLE RISORSE

6
REQUISITI RELATIVI ALLE RISORSE

- **6.2.1.2** riservatezza personale
- **6.2.1.4** compiti e responsabilità del personale
- **6.2.3.1 formazione**
- **6.4.1.2 fornitori selezionati per conformità ai requisiti**
- **6.5.1** accessi controllati
- **6.5.4** attrezzature critiche

Requisiti ISO 20387 e GDPR

6.4.1.2 Fornitori esterni: valutazione, selezione, monitoraggio e rivalutazione delle prestazioni conformi ai requisiti e **4.3.2 1°Paragrafo** (Informativa fornitore)

Art. 28 GDPR

Requisiti ISO 20387 e GDPR

6
REQUISITI RELATIVI ALLE RISORSE

6
REQUISITI RELATIVI ALLE RISORSE

CONTROLLI APPLICAZIONE Art. 28 responsabile del trattamento

Esempi controlli documentali e in campo per verificare conformità alle prescrizioni su requisiti norma

- stipulato un contratto o altro atto giuridico che rechi i punti dell'art.28
- Attività di audit programmata ed eseguita dal titolare sul responsabile
- monitoraggio sub-responsabili

7
REQUISITI DI PROCESSO

7
REQUISITI DI PROCESSO

- **7.1.1 ciclo di vita materiale biologico e dati associati identificati e processi definiti e verificati**
- **7.2.3.4** principi etici e consenso
- **7.3.2.4 isolamento mat. Biologico e dati associati per verifica conformità legale/etica prima utilizzo**
- **7.4.7** trasferimento dati progettato per assicurare integrità e riservatezza
- **7.7.4** ubicazione della conservazione materiale biologico e dati associati
- **7.7.8** revoca consenso paziente
- **7.11.2 - 3** output non conforme e comunicazione
- **7.13** gestione reclami

Requisiti ISO 20387 e GDPR

7.1.1 le fasi del ciclo di vita del materiale biologico e **dei dati associati** devono essere identificati- Tutte le procedure anche su dati associati devono essere aggiornate

- Art. 30 Registro dei trattamenti

7
REQUISITI DI PROCESSO

CONTROLLI APPLICAZIONE Art. 30 registro trattamenti

Esempi controlli documentali e in campo per verificare conformità alle prescrizioni

- registro dei trattamenti e aderenza dei contenuti al ciclo di vita del materiale biologico e dati associati
- verificare aggiornamento delle procedure del modello di adeguamento privacy

7
REQUISITI DI PROCESSO

7
REQUISITI DI PROCESSO

- **7.1.1** ciclo di vita materiale biologico e dati associati identificati e processi definiti e verificati
- **7.2.3.4** principi etici e consenso
- **7.3.2.4 isolamento mat. Biologico e dati associati per verifica conformità legale/etica prima utilizzo**
- **7.4.7** trasferimento dati progettato per assicurare integrità e riservatezza
- **7.7.4** ubicazione della conservazione materiale biologico e dati associati
- **7.7.8** revoca consenso paziente
- **7.11.2 - 3** output non conforme e comunicazione
- **7.13** gestione reclami

Requisiti ISO 20387 e GDPR

7.3.2.4 il materiale biologico e dati associati devono essere isolati fino a quando la conformità legale, etica della documentazione e della qualità del materiale biologico e dati associati è stata valutata e gestita

Art. 24 -responsabilità del titolare e art. 5 - principi del trattamento

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy
Controlli Privacy

7 REQUISITI DI PROCESSO

CONTROLLI APPLICAZIONE
Art. 24 -responsabilità del titolare e
art. 5 - principi del trattamento
verifica preventiva applicazione principi trattamento dati personali

Esempi controlli documentali e in campo per verificare conformità alle prescrizioni

verifica della qualità ed esattezza dei dati

Finalità del trattamento

Minimizzazione e **limitazione dei dati personali raccolti**

Requisiti ISO 20387 e GDPR

8 REQUISITI SISTEMA DI GESTIONE QUALITÀ

8
Requisiti sistema gestione qualità

- **8.5.1 azioni per affrontare rischi e opportunità**
- **8.5.2** piani di azioni per affrontare rischi/opportunità
- **8.5.3** proporzionalità delle azioni intraprese all'impatto potenziale sul biobanking
- **8.6.1 miglioramento**
- **8.7** azioni correttive output NC
- **8.8 audit interni**
- **8.9.1 riesame direzione SGQ: idoneità, adeguatezza, efficacia**

Requisiti ISO 20387 e GDPR

8.5.1 Azioni per affrontare rischi ed opportunità: La BBK deve considerare i rischi e le opportunità associati alle proprie attività di biobanking

- Art. 32 sicurezza del trattamento
- art. 35 DPIA

8.6.1 Miglioramento: La BBK deve identificare e selezionare opportunità di miglioramento e attuare tutte le azioni necessarie

Requisiti ISO 20387 e GDPR

8 REQUISITI SISTEMA DI GESTIONE QUALITÀ

8
Requisiti sistema gestione qualità

- **8.5.1 azioni per affrontare rischi e opportunità**
- **8.5.2** piani di azioni per affrontare rischi/opportunità
- **8.5.3** proporzionalità delle azioni intraprese all'impatto potenziale sul biobanking
- **8.6.1 miglioramento**
- **8.7** azioni correttive output NC
- **8.8 audit interni**
- **8.9.1 riesame direzione SGQ: idoneità, adeguatezza, efficacia**

Requisiti ISO 20387 e GDPR

8.8 audit interni

8.9 riesame della Direzione

- Art. 32 sicurezza del trattamento
- art. 35 DPIA

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

Controlli Privacy

8 REQUISITI SISTEMA DI GESTIONE QUALITÀ

CONTROLLI APPLICAZIONE requisito

8.5.1 Azioni per affrontare rischi ed opportunità: La BBK deve considerare i rischi e le opportunità associati alle proprie attività di biobanking

Esempi controlli documentali e in campo per verificare conformità alle prescrizioni

- Valutazione del documento di valutazione del rischio del trattamento
- PIA: valutazione di impatto
- Consapevolezza del rischio da parte del personale della struttura operativa

Art. 32 e 35 GDPR Misure di sicurezza e valutazione di impatto

UNI EN ISO 20387:2020 - RT 38 e Disciplina Privacy

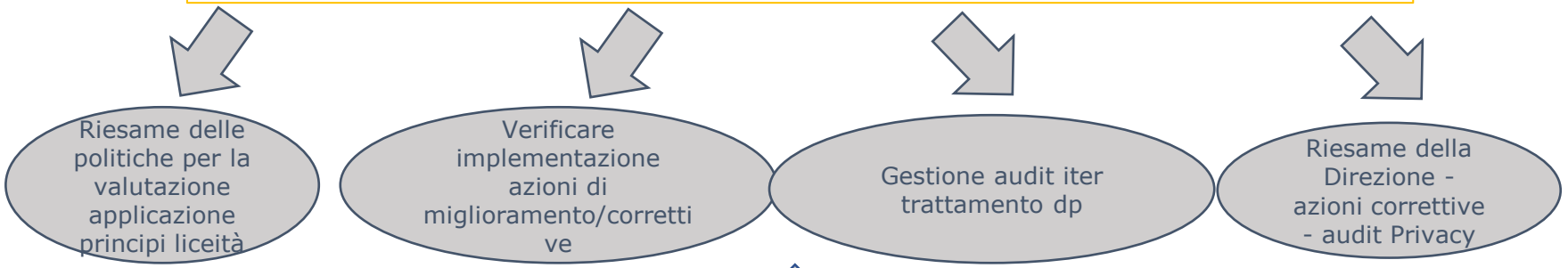
Controlli Privacy

8 REQUISITI SISTEMA DI GESTIONE QUALITÀ

CONTROLLI APPLICAZIONE requisito

8.6.1 Miglioramento: La BBK deve identificare e selezionare opportunità di miglioramento e attuare tutte le azioni necessarie
8.8 audit interni
8.9 riesame della Direzione

Esempi controlli documentali e in campo per verificare conformità alle prescrizioni



Art. 24 GDPR Responsabilità del titolare

CONCLUSIONI

La ISO 20387 rimanda sistematicamente alla conformità alla disciplina della protezione dei dati personali associati ai trattamenti, prevedendola in tutto il percorso del ciclo dei trattamenti dei campioni biologici e dei dati genetici

Le Biobanche sono chiamate ad adottare un sistema di accountability molto solido per dimostrare la compliance Privacy applicata ai requisiti ISO 20387, dalla acquisizione alla distruzione dei campioni biologici e dei dati correlati, nonché dei dati genetici

La attività di verifica della compliance al GDPR e ai Provvedimenti del GPD del biobanking è pervasiva, articolata e multidisciplinare

ACCREDIA

L'ENTE ITALIANO DI ACCREDITAMENTO

ACCREDIA
Via Guglielmo Saliceto, 7/9 - 00161 Roma
T +39 06 8440991 / F +39 06 8841199
info@accredia.it

Dipartimento Certificazione e Ispezione
Via Tonale, 26 - 20125 Milano
T +39 02 2100961 / F +39 02 21009637
milano@accredia.it

Dipartimento Laboratori di prova
Via Guglielmo Saliceto, 7/9 - 00161 Roma
T +39 06 8440991 / F +39 06 8841199
info@accredia.it

Dipartimento Laboratori di taratura
Strada delle Cacce, 91 - 10135 Torino
T +39 011 32846.1 / F +39 011 3284630
segreteriadt@accredia.it