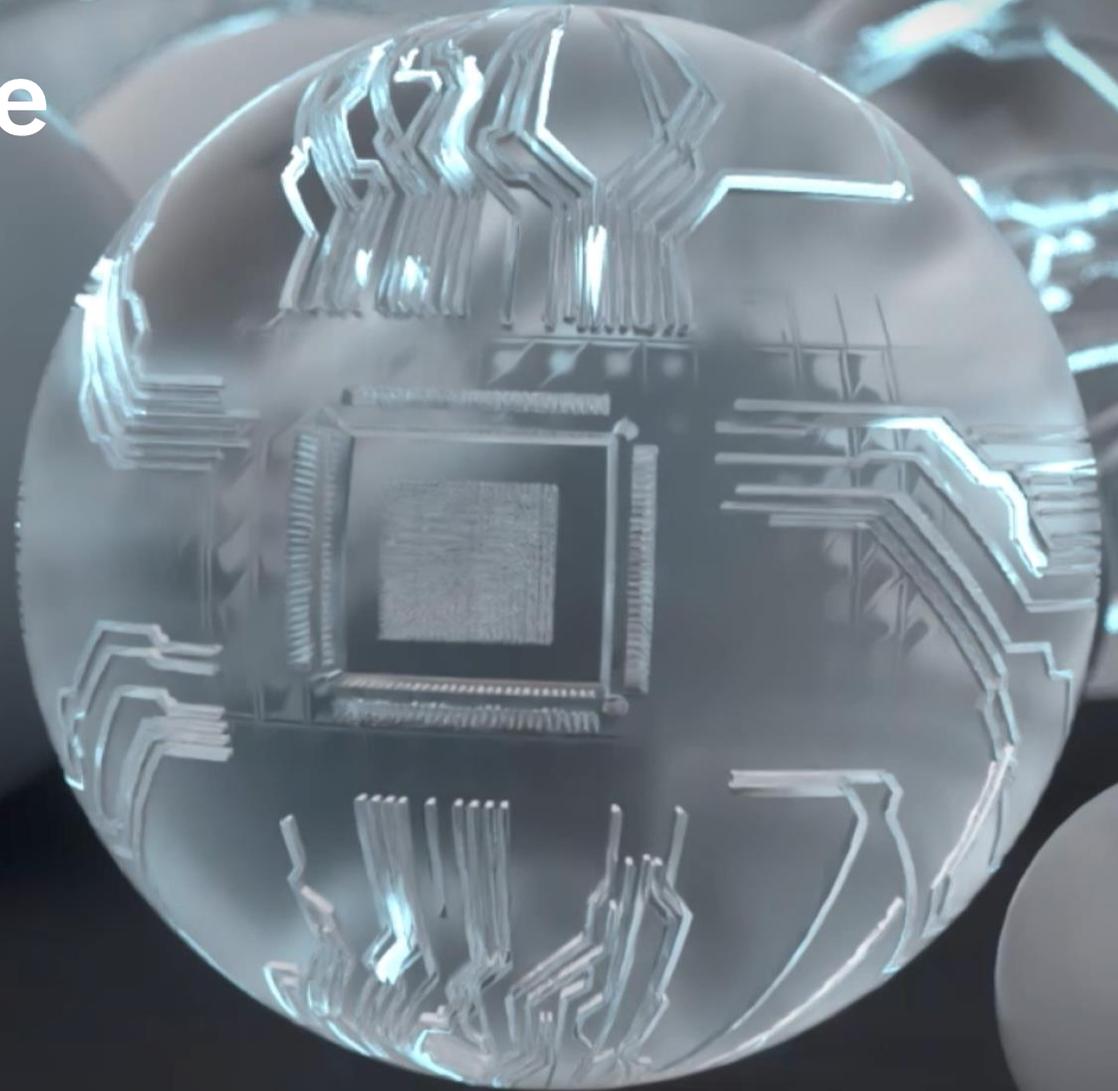


I dati sulla salute e l'approccio del Garante alla loro gestione

23 Novembre 2021



Today's team



Today's team



Edoardo Tedeschi

Partner, TMT and Digital Business

T +39 02 7250 5585

E edoardo.tedeschi@simmons-simmons.com



Eugenia Lopresti

Lawyer, Milan

T +39 02 7250 5440

E eugenia.lopresti@simmons-simmons.com



Mauro Teresi

Of Counsel, Regulatory and Product Liability

T +39 02 7250 5559

E mauro.teresi@simmons-simmons.com

Dati “sensibili”



Art. 4 n. 15 e considerando n. 35 GDPR

«**Dati relativi alla salute**»: i dati personali attinenti alla salute fisica e mentale di una persona fisica compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute

Art. 9 e considerando 51 GDPR

Il trattamento di particolari categorie di dati personali (“dati sensibili”)

L’art. 9 n. 1 GDPR sancisce come principio di carattere generale **il divieto** di trattare dati personali che rivelino l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, nonché **trattare dati genetici, dati biometrici, dati relativi alla salute** o alla vita sessuale o all’orientamento sessuale della persona.

Art. 9.2 GDPR



È possibile trattare i dati “sensibili” quando il trattamento è necessario:



Norme del codice privacy (novellato)



- *Art. 2 quater* «Regole deontologiche»
- *Art. 2 sexies* «Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante»
- *Art. 2 septies* «Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute»

Art. 2 quater codice privacy

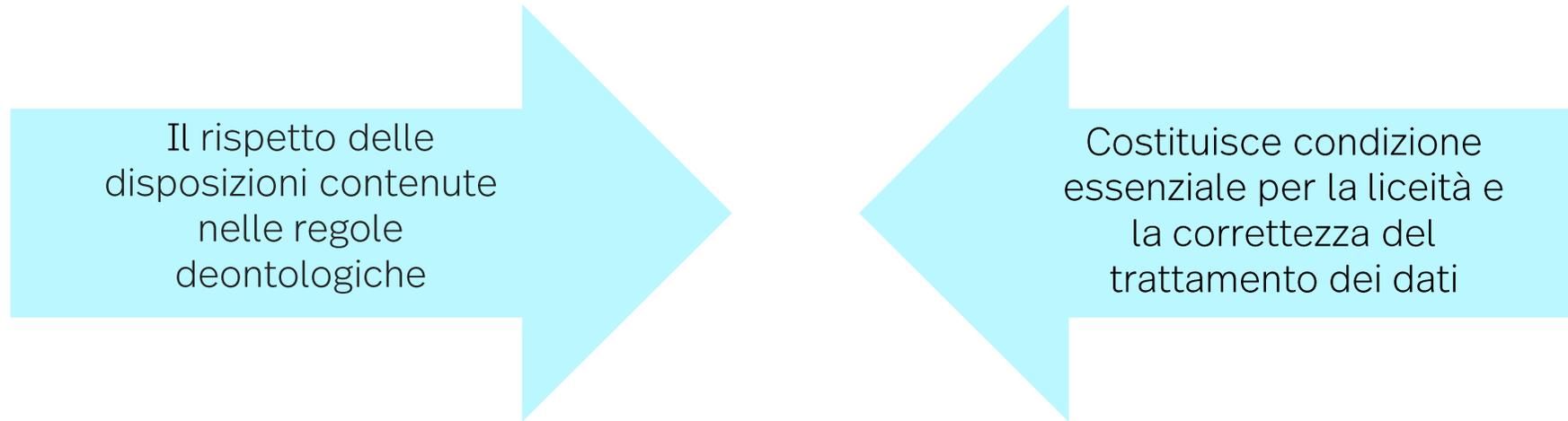


Il Garante promuove l'adozione di regole deontologiche per i trattamenti dati di cui agli articoli:



Lo schema di regole deontologiche è sottoposto a consultazione pubblica per un periodo non inferiore a 60 giorni

Art. 2 *quater* codice privacy



Art. 2 *sexies* codice privacy



Si considerano trattamenti di interesse pubblico rilevante:

- Attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano
- Compiti del Servizio Sanitario Nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica
- Programmazione, gestione, controllo e valutazione dell'assistenza sanitaria
- Tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili

Art. 2 septies codice privacy



Per il trattamento di dati genetici, biometrici e relativi alla salute
con cadenza almeno biennale



Il Garante adotta un provvedimento con **misure di garanzia**, tenendo conto:

- delle linee guida, delle raccomandazioni e delle migliori prassi del Comitato Europeo
- dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure
- dell'interesse alla libera circolazione dei dati personali in UE

Lo schema di provvedimento del Garante con misure di garanzia è sottoposto a consultazione pubblica per un periodo non inferiore a 60 giorni

Art. 2 septies codice privacy



Il Garante adotta misure di garanzia in relazione a ciascuna categoria: misure per dati genetici, biometrici e per dati relativi alla salute



Il Garante detta regole differenziate a seconda delle finalità del trattamento ed inoltre individua ulteriori condizioni sulla base delle quali il trattamento è consentito



Le misure di garanzia individuano le misure di sicurezza, tra le quali: tecniche di cifratura e pseudonimizzazione, misure di minimizzazione, modalità per l'accesso selettivo ai dati, modalità per rendere le informazioni agli interessati

Art. 2 septies codice privacy



Le misure di garanzia che riguardano il trattamento dei dati relativi alla salute per:

- Finalità di prevenzione, diagnosi e cura;
- Profili organizzativi e gestionali in ambito sanitario
- Per definire le modalità di comunicazione all'interessato dei dati relativi alla propria salute
- Per prescrizione di medicinali



Sono adottate sentito il parere del Ministero della Salute, che a tal fine acquisisce il parere del Consiglio Superiore di Sanità.

N.B. Le misure di garanzia **in caso di dati genetici** possono individuare, in caso di particolare ed elevato rischio, il consenso come ulteriore misura di protezione

Periodo transitorio (ancora in corso)



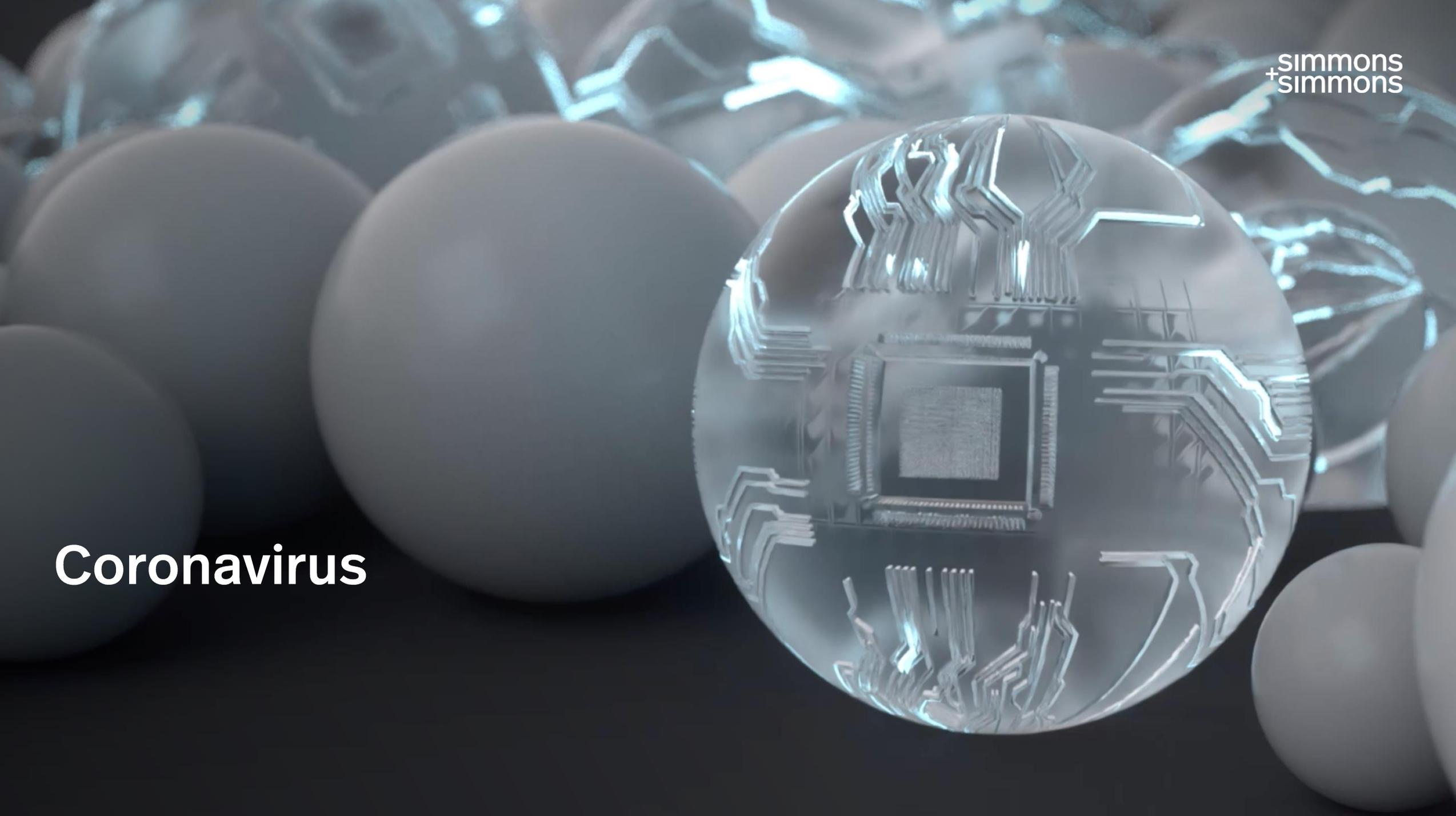
Il Legislatore ha affidato al Garante il compito di :

- Verificare la conformità al GDPR dei Codici deontologici adottati precedentemente
- Individuare e aggiornare le prescrizioni contenute nelle autorizzazioni generali che siano ancora compatibili con il GDPR



- Il Garante ha verificato la conformità delle **regole deontologiche per fini statistici o di ricerca scientifica**
- Con Provvedimento del 13/12/2018 il Garante ha individuato le disposizioni delle Autorizzazioni Generali compatibili tra cui: la **n. 1/2016** (dati sensibili nei rapporti di lavoro, **n. 8/2016** (dati genetici), **n. 9/2016** (ricerca scientifica)

Coronavirus



Disciplina transitoria per i dati sensibili



Fino al termine dello stato di emergenza deliberato dal Consiglio dei Ministri, per motivi di interesse pubblico nel settore della sanità pubblica ed in particolare :

- Per garantire la protezione dall'emergenza sanitaria a carattere transfrontaliero mediante adeguate misure di profilassi
- Per assicurare la diagnosi e l'assistenza sanitaria dei contagi
- Per assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali



I soggetti operanti nella Protezione civile, il Ministero della salute, ISS, le strutture pubbliche e private che operano nell'ambito del SSN e tutti i soggetti deputati a monitorare e garantire l'esecuzione delle misure di contenimento



Possano effettuare trattamenti, ivi inclusa la comunicazione tra loro dei dati personali, anche sensibili, necessari all'espletamento delle funzioni attribuitegli nell'ambito dell'emergenza sanitaria da Covid-19

GDPR

Art. 9.2 :

Lett. g) motivi di interesse pubblico

Lett. h) medicina preventiva

Lett. i) motivi di interesse pubblico nel settore della sanità pubblica

Codice privacy

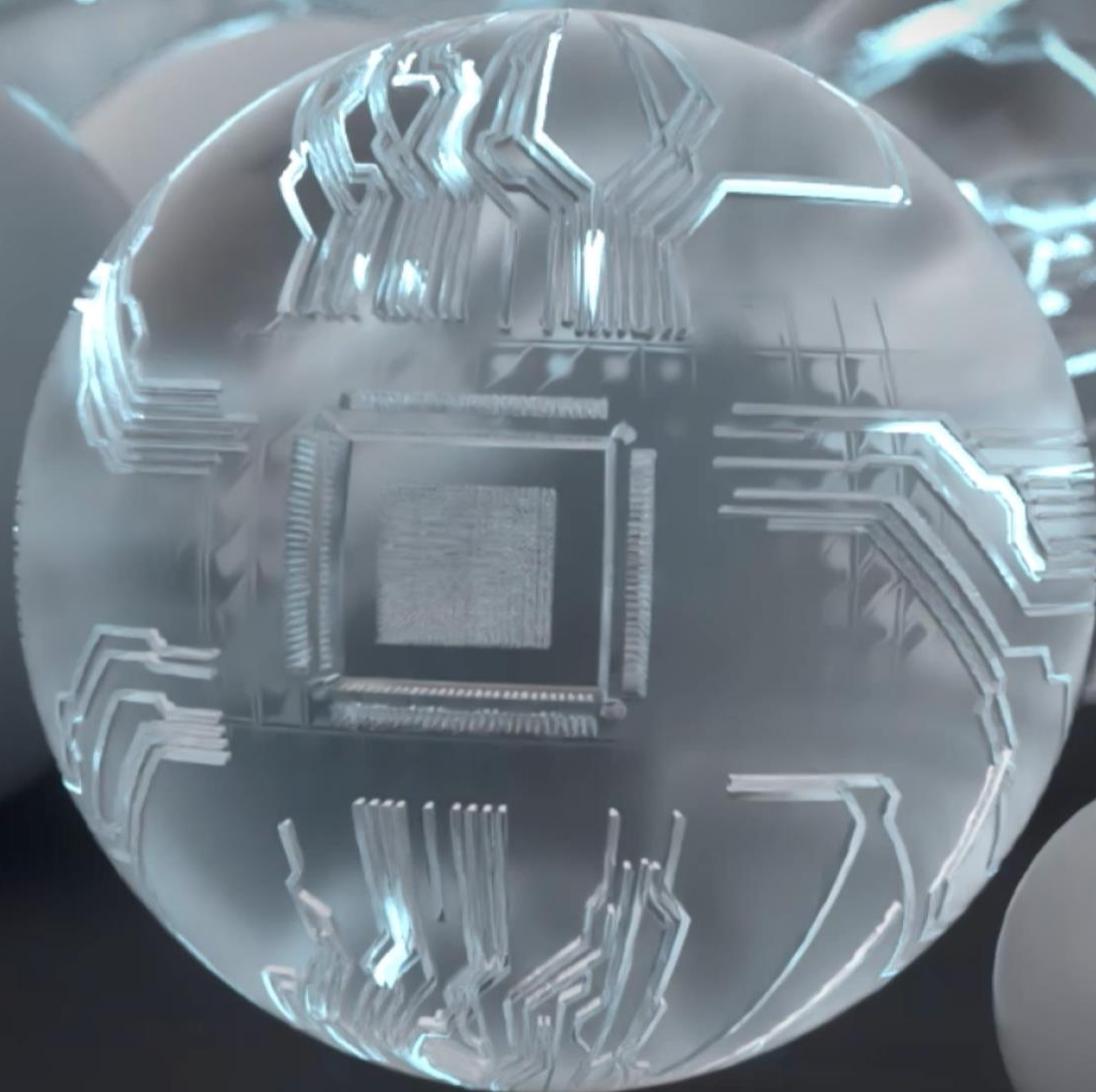
Art. 2 sexies comma 2:

Lett. t) attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale

Lett. u) compiti di servizio sanitario nazionale e dei soggetti operanti nell'ambito sanitario

- D.L. 22 aprile 2021 n. 52 e ss.mm. introduce misure urgenti per contenere e contrastare l'emergenza epidemiologica da Covid-19 prevedendo anche l'impiego delle certificazioni verdi («green pass») nel settore privato.
- I green pass possono essere verificati per accedere in azienda tramite specifica app rilasciata dal Ministero della Salute «verificaC19»
- Il trattamento dei dati dovrà essere preceduto da specifiche istruzioni che il titolare dovrà fornire alle persone autorizzate al trattamento dati che effettueranno i controlli ex art. 29 GDPR e art. 2 *quaterdecies* Codice privacy, nonché da idonea informativa resa agli interessati ex art. 13 GDPR
- Il trattamento dovrà essere effettuato in conformità dei principi sanciti dal GDPR e codice privacy: minimizzazione dei dati, esattezza, trasparenza e limitazione della conservazione dei dati.

**Trattamento ai fini di
ricerca scientifica**



Trattamenti per finalità di ricerca scientifica e nell'ambito della sperimentazione clinica



- Regolamento UE 2016/679
- Codice Privacy
- Regole deontologiche per trattamenti ai fini statistici o di ricerca scientifica
- Provvedimento del Garante recante le prescrizioni relative al trattamento di particolari categorie di dati ai sensi dell'art. 21, comma 1 del d. lgs. 10 agosto 2018 n. 101
- Chiarimenti del Garante sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario del 7 marzo 2019
- WP29 - parere n. 05/2014 sulle tecniche di anonimizzazione dei dati
- Enisa - Tecniche di pseudonimizzazione e buone pratiche

Regime speciale: art. 89 GDPR



Il trattamento ai fini di ricerca scientifica è soggetto a garanzie adeguate per i diritti e le libertà degli interessati. Tali garanzie devono assicurare misure tecniche e organizzative (ad es. pseudonimizzazione) per garantire il rispetto del principio di minimizzazione.

Il paragrafo 2 dell'art. 89 prevede che nel caso in cui i dati personali siano trattati per la suddetta finalità, il diritto dell'Unione o degli Stati membri possa prevedere deroghe ai diritti di cui agli art. 15 (accesso), 16 (rettifica), 18 (limitazione) e 21 (opposizione), nella misura in cui tali diritti rischiano di rendere impossibile o pregiudicare gravemente il conseguimento di dette finalità specifiche

Regime speciale: secondary use



Il GDPR all'art. 5.1 lett. b) e al considerando 50, qualifica l'ulteriore trattamento per finalità di ricerca scientifica come lecito e compatibile con le finalità per le quali i dati sono stati inizialmente raccolti, consentendo tale trattamento secondo modalità previste dall'art. 89 GDPR (anonimizzazione, pseudonimizzazione, altre misure di minimizzazione)

In tali casi, quindi, non è richiesta la valutazione di compatibilità ex art. 6.4 GDPR né alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati

L'EDPS nella «preliminary opinion on data protection and scientific research» del 6 gennaio 2020 ha precisato che non si tratta di una presunzione assoluta di compatibilità e che la valutazione di compatibilità dovrebbe essere comunque considerata, quando i dati sono stati raccolti per scopi molto diversi

Regime speciale: obbligo di informativa



Di regola, in caso di ulteriore utilizzo per scopo diverso, i partecipanti devono essere informati prima di procedere all'ulteriore trattamento ai sensi dell'art. 13.3 e 14.4 GDPR anche se lo scopo è compatibile e non è necessario fondare il trattamento su una nuova base giuridica

L'obbligo di informare l'interessato viene meno, ai sensi dell'art. 13.4 e 14.5 GDPR solo se:

- l'interessato dispone già delle informazioni,
- risulta impossibile o implicherebbe uno sforzo spropositato in particolare per il trattamento di ricerca scientifica, fatte salve le condizioni di garanzia di cui all'art. 89.1 GDPR (rischia di rendere impossibile il conseguimento delle finalità). In tali casi il titolare deve adottare misure appropriate per tutelare i diritti e le libertà degli interessati, anche rendendo pubbliche le informazioni (art. 14.5 lett. b) GDPR)

Regime speciale: ulteriore conservazione



Il GDPR consente di conservare più a lungo i dati se lo scopo è di ri-utilizzo per fini di ricerca scientifica a condizione che vengano rispettate le misure previste dall'art. 89.1 GDPR

Ciò in deroga al principio di limitazione della conservazione per cui i dati dovrebbero essere «conservati in una forma che consenta l'identificazione delle persone interessate per un periodo di tempo non superiore a quello necessario» (art. 5.1 lett e) GDPR «minimizzazione dei dati»)

Base giuridica dedicata



Il GDPR ha previsto una base giuridica specifica per il trattamento di particolari categorie di dati per finalità di ricerca scientifica (**art. 9.2 lett. j**). Tale base prevede il trattamento di particolari categorie di dati per ricerca scientifica, ma solo sulla base del diritto dell'UE o degli stati membri:

«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»

Possibilità di ottenere un consenso



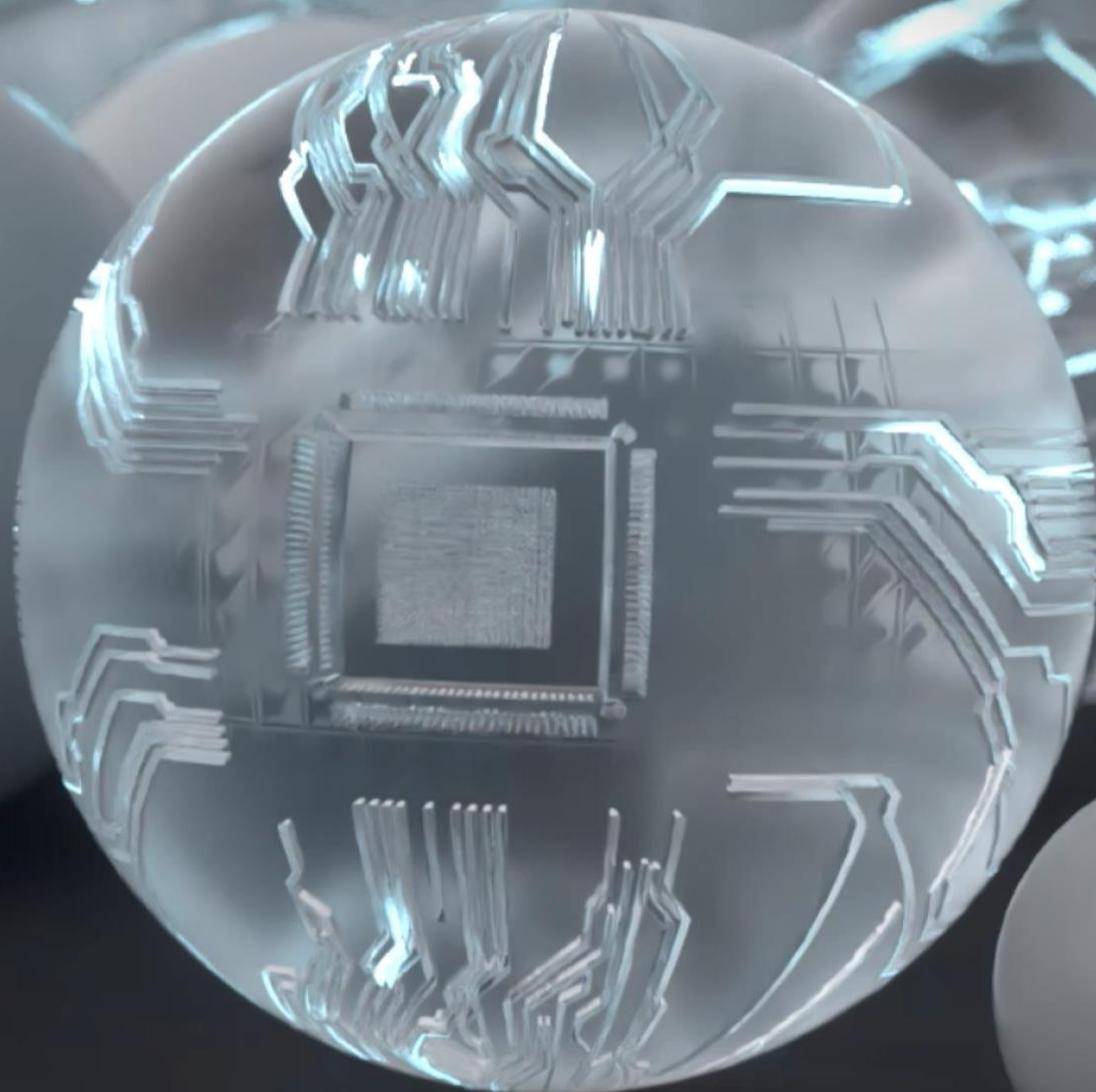
Esiste la possibilità di ottenere un consenso per alcuni settori della ricerca scientifica.

In tutti quei casi in cui il consenso costituisce la base legittima per trattare i dati ma, al momento in cui i dati vengono raccolti, non sia possibile individuare pienamente la finalità, il legislatore europeo ha previsto la possibilità di prestare un consenso a determinati settori della ricerca o a parti di progetti di ricerca; ciò nella misura consentita dalla finalità prevista e nel rispetto delle norme deontologiche riconosciute per la ricerca scientifica (considerando 33)

Come chiarito dai Garanti Europei, il consenso può essere prestato in relazione ad una finalità di ricerca descritta ad un livello più generale (ma non generico). Questa prescrizione accorda flessibilità al grado di specificazione e gradualità del consenso nel contesto della ricerca scientifica, ma non prevale sulle condizioni di consenso previste dal GDPR.

In un'ottica di compensazione il titolare del trattamento deve garantire la massima trasparenza e adottare le garanzie previste dall'art. 89.1 GDPR

Trattamento dei dati nella sperimentazione clinica



Trattamento dati nell'ambito della sperimentazione clinica

Le linee guida emanate per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche medicinali emanate dal Garante il 24/07/2008, individuano prescrizioni riferite ai soggetti coinvolti nel trattamento dei dati dei partecipanti a sperimentazioni cliniche

Le indicazioni contenute in queste linee guida riguardano principalmente le sperimentazioni cliniche di medicinali condotte a scopo di lucro promosse da società farmaceutiche o da altre strutture private per lo sviluppo industriale di un farmaco. Il Garante ha chiarito come tali prescrizioni possono estendersi anche a quelle sui dispositivi medici e a quelle senza scopo di lucro.

Le linee guida rimangono ancora applicabili nella misura in cui le prescrizioni contenute risultano compatibili con il GDPR (art. 22.2 d.lgs. 101/2018)

Ruoli privacy dei soggetti coinvolti



Il Garante esclude il ruolo di Responsabile del trattamento dei dati (art. 28 GDPR) dei centri di sperimentazione in quanto secondo il Garante in ragione delle rispettive attività svolte dal promotore e dai centri di sperimentazione, generalmente, questi soggetti conservano responsabilità distinte e per questo si configurano (tendenzialmente) come Titolari autonomi o contitolari del trattamento a seconda delle specifiche circostanze.

In caso di contitolarità (art. 26 GDPR) andranno definite in modo trasparente le rispettive responsabilità in merito all'osservanza del GDPR con particolare riferimento all'esercizio dei diritti degli interessati e le rispettive funzioni di comunicazione delle informazioni ai sensi degli art. 13 e 14 GDPR. Il contenuto dell'accordo deve poi essere messo a disposizione dell'interessato.

Ruoli privacy e soggetti coinvolti



Per l'esecuzione di alcune attività es. analisi statistiche, farmacovigilanza, ecc.. Il **promotore** può avvalersi di soggetti esterni quali laboratori analisi, professionisti, ecc..

Tali soggetti trattano i dati personali dai partecipanti in nome e per conto del promotore e, pertanto, si qualificano come Responsabili del trattamento ai sensi dell'art. 28 GDPR.

Anche il **centro di sperimentazione** può avvalersi di responsabili esterni se esternalizza attività correlate alla ricerca che implicano il trattamento dei dati personali dei partecipanti.

Nell'ambito della sperimentazione clinica, **le autorità regolatorie** di settore, nazionali, europee e internazionali (tra cui AIFA e EMA), possono accedere ai dati per lo svolgimento di attività ispettive.

Le persone fisiche preposte al trattamento dei dati e che operano sotto la diretta autorità del Promotore o dello sperimentatore o dei relativi responsabili devono essere adeguatamente selezionate, informate, istruite ed autorizzate.

Il Garante, nelle linee guida, fornisce un modello di informativa che i promotori/sperimentatori possono scegliere di utilizzare e prevede alcune semplificazioni.

Tra le informazioni previste è necessario specificare:

- La natura dei dati,
- I ruoli svolti dal promotore e dagli altri soggetti di cui si avvalga per il trattamento dati,
- La possibilità di esercitare i diritti privacy anche nei confronti del promotore,
- L'eventuale comunicazione dati a terzi nel caso in cui il promotore e lo sperimentatore non siano contitolari. Sul punto il Garante suggerisce di indicare in modo specifico il promotore che riceve i dati.

Consenso al trattamento



L'art. 110 Cod. privacy «Ricerca medica, biomedica ed epidemiologica»

Regola: consenso ex art. 9.1 lett a) GDPR

Deroghe:

- Se il trattamento avviene sulla base di legge/regolamento in conformità con l'art. 9.2 lett. j) GDP, ivi incluso il caso della ricerca biomedica o sanitaria, il titolare deve procedere alla DPIA ai sensi dell'art. 35 e 36 GDPR
- Se a causa di particolari ragioni risulta impossibile informare l'interessato o implica uno sforzo «sproporzionato», il Titolare deve: adottare misure appropriate per tutelare i diritti e le libertà degli interessati, sottoporre il programma di ricerca al motivato parere favorevole del competente Comitato Etico a livello territoriale, svolgere la consultazione preventiva ex art. 36 GDPR

Ci si interroga oggi se il consenso semplificato previsto nelle linee guida del Garante sia ancora compatibile con il nuovo quadro normativo stante l'abrogazione dell'art. 2.2 cod. privacy (principi di semplificazione)

Consenso al trattamento



Sul consenso come base giuridica del trattamento, l'EDPS nella recente opinione preliminare in materia di ricerca scientifica, segnala come sia possibile il consenso come un'adeguata salvaguardia dei diritti della persona interessata.

Per l'EDPS il consenso potrebbe rappresentare, dunque, non solo una potenziale base giuridica ma anche un mezzo per concedere agli individui più controllo e scelta per sostenere la fiducia della società nella scienza.

Esercizio dei diritti di rettifica



Nel caso di esercizio dei diritti previsti dall'art. 16 GDPR, la rettifica e l'integrazione dei dati sono annotate senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca.

Questa previsione può considerarsi conforme al GDPR in quanto espressamente prevista dall'art. 110 comma 2 Cod. Privacy che si applica alla ricerca in ambito medico, biomedico ed epidemiologico.

Conservazione dei dati



La disciplina di settore prevede che la documentazione essenziale relativa allo studio debba essere conservata per almeno 7 anni dal completamento della ricerca ovvero per un periodo di tempo più lungo nel caso in cui ciò sia richiesto da altre norme applicabili.

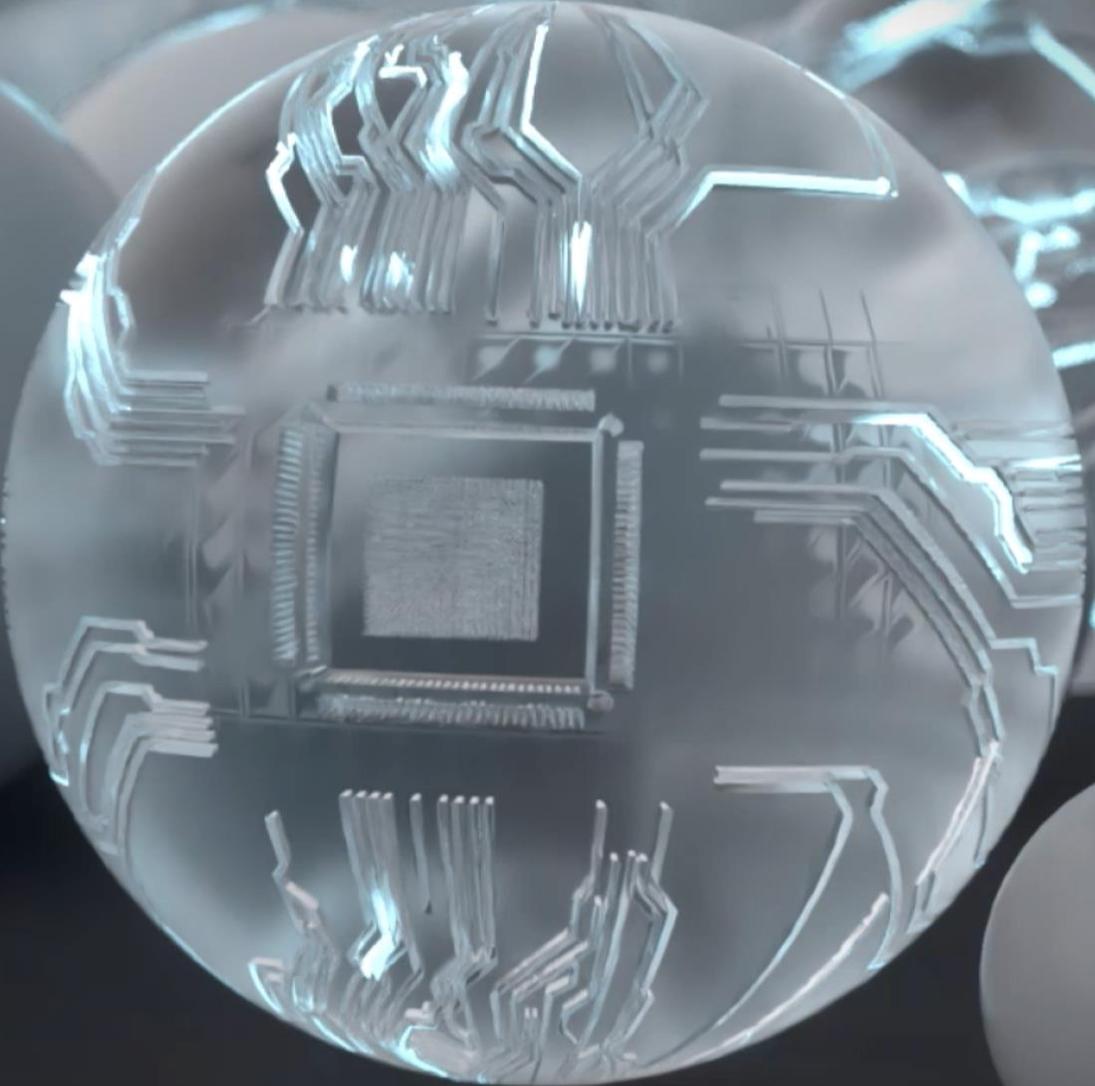
Il Garante chiarisce come l'opportunità di conservare la documentazione per un periodo più lungo potrebbe essere valutata considerando anche la durata dell'autorizzazione d'immissione del farmaco in sperimentazione o eventuali ulteriori esigenze di analisi dei dati, connesse a nuove domande di immissione in commercio o di estensione dell'autorizzazione o al manifestarsi di evidenze significative per la sicurezza dei pazienti.

- Applicazione parziale o integrale di tecnologie crittografate o l'adozione di altre misure di informatiche che rendano intellegibili i dati ai soggetti non autorizzati.
- Uso di protocolli di comunicazione sicuri basati sull'utilizzo di standard crittografici per il trasferimento in via telematica dei dati dei partecipanti verso il database unico presso il promotore
- Idonei sistemi di autenticazione e di autorizzazione per gli autorizzati al trattamento in funzione dei ruoli ricoperti dagli stessi e delle esigenze di accesso e trattamento al database centralizzato, nonché procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati
- Sistemi di *audit log* per il controllo degli accessi al database e rilevamento anomalie

Grazie.

simmons
+
simmons



A large, semi-transparent sphere in the foreground contains a detailed microchip with intricate circuitry. The background is filled with several other similar spheres, some of which are slightly out of focus, creating a sense of depth. The overall color palette is a cool, monochromatic blue and grey.

simmons-simmons.com

STRICTLY PRIVATE AND CONFIDENTIAL

© Simmons & Simmons LLP and its licensors. All rights asserted and reserved. This document is for general guidance only. It does not contain definitive advice. Simmons & Simmons LLP is a limited liability partnership registered in England & Wales with number OC352713 and with its registered office at CityPoint, One Ropemaker Street, London EC2Y 9SS, United Kingdom. It is authorised and regulated by the Solicitors Regulation Authority and its SRA ID number is 533587. The word "partner" refers to a member of Simmons & Simmons LLP or one of its affiliates, or an employee or consultant with equivalent standing and qualifications. A list of members and other partners together with their professional qualifications is available for inspection at the above address.