PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Linee guida sulle questioni etiche e legali della protezione dei dati nella ricerca e nell'innovazione delle TIC

BIOMETRIA

Questo progetto è stato finanziato dal programma di ricerca e innovazione Horizon 2020 dell'Unione Europea con l'accordo di sovvenzione n. 788039. Il presente documento riflette esclusivamente il punto di vista degli autori e l'Agenzia non può essere ritenuta responsabile per l'uso che può essere fatto delle informazioni in esso contenute.

Dati biometrici nella ricerca e innovazione nelle TIC

Alessandro Ortalda, Carlotta Rigotti, Andrés Chomczyk Penedo, Paul De Hert (VUB)

La presente parte degli Orientamenti è stata rivista da Stefano Leucci (Garante europeo della protezione dei dati), Ernestina Sacchetto (Università di Torino); Catherine Jasserand-Breeman (KU Leuven) e Lydia Belkadi (KU Leaven).

Essa è stata, inoltre, rivista e convalidata dal Prof. Gert Vermuelen (Università di Gent)

1 Introduzione e scopo della sezione degli orientamenti

Le attività di ricerca, a volte, possono includere il trattamento di dati biometrici, il che implica che i ricercatori e le istituzioni di ricerca agiscano come titolari del trattamento dei suddetti dati o responsabili del trattamento per il rispetto dei requisiti di protezione dei dati. Poiché i dati biometrici godono di un regime di protezione speciale nell'ambito del quadro normativo dell'UE, i ricercatori che lavorano con dati biometrici non solo devono rispettare i requisiti generali di protezione dei dati e quelli specifici indicati nell'articolo 89 del Regolamento generale in materia di protezione dei dati (RGPD) relativi alle attività di ricerca[1], ma devono anche implementare misure di garanzia supplementari specifiche per i dati biometrici e/o il trattamento biometrico.

I seguenti orientamenti forniscono una guida su come adempiere agli obblighi di legge sanciti dal regime europeo di protezione dei dati. In particolare, il documento riguarda le attività di ricerca sulle TIC che includono lo sviluppo di sistemi TIC che utilizzano dati biometrici. Gli autori sono consapevoli che al giorno d'oggi è comune, per i suddetti sistemi, l'uso di tecnologie di intelligenza artificiale. In ogni caso, poiché gli orientamenti specifici in materia di intelligenza artificiale possono essere trovati nel documento 'Orientamenti in materia di questioni legali ed etiche relative all'intelligenza artificiale nella ricerca e innovazione nelle TIC', il presente documento non regola l'intelligenza artificiale.

Il presente documento è rivolto alle istituzioni di ricerca nelle TIC che lavorano con una tecnologia biometrica come titolari del trattamento, ivi inclusi non solo i ricercatori, che potrebbero non essere a conoscenza degli obblighi di legge derivanti dalla loro attività di ricerca, ma anche altre parti interessate, come dipartimenti legali o comitati etici, che potrebbero essere più competenti sugli aspetti legali, ma non necessariamente in materia di regimi di protezione di dati speciali applicabili ai dati biometrici e alle attività di ricerca. Per garantire che entrambi i destinatari anzidetti possano facilmente accedere ai contenuti dei presenti orientamenti, il documento cerca di trovare un equilibrio tra i dati tecnici (relativi sia alla tecnologia nelle TIC e biometrica che alla legge per la protezione dei dati) e l'accessibilità generale.

[1] 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such' (2016).

2 Definizioni

2.1 Categorie particolari di dati personali

Prima di definire i dati biometrici, è necessario esaminare le 'categorie particolari di dati personali', comunemente note come 'dati sensibili'. Infatti, l'articolo 9.1 dell'RGPD raggruppa i dati biometrici (o, almeno, alcuni di essi; cfr. 2.2 Dati biometrici) in questo gruppo più ampio:

Categorie particolari di dati personali
Dati che rivelano l'origine razziale o etnica
Dati che rivelano le opinioni politiche
Dati che rivelano le credenze religiose o filosofiche
Dati che rivelano l'appartenenza a un'associazione sindacale
Dati genetici
Dati biometrici (con la finalità di identificare univocamente persone fisiche)
Dati relativi alla salute
Dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica

Per default, l'Articolo 9 dell'RGPD proibisce il trattamento di categorie particolari di dati personali, salvo nei casi di cui alle eccezioni previste dall'articolo 9.2 dell'RGPD. Una di queste eccezioni si verifica quando "il trattamento è necessario per [...] finalità di ricerca scientifica o storica".

È opportuno specificare che, per essere conformi, non è sufficiente, per un trattamento di categorie particolari di dati personali, rientrare in una delle eccezioni elencate nell'articolo 9.2 RGPD. In aggiunta a ciò, prima che inizi il trattamento, il titolare del trattamento deve identificare una base giuridica adeguata per il trattamento dei dati (cfr. sezione 3.2.3 Identificare la base giuridica più adeguata)[2].

I titolari del trattamento dei dati devono, inoltre, essere consapevoli che, ai sensi dell'articolo 9.4 RGPD, gli Stati membri possono introdurre ulteriori condizioni e applicare requisiti e limiti aggiuntivi relativi al trattamento di dati genetici, dati biometrici o dati relativi alla salute. Perciò, i titolari del trattamento che si accingono a trattare queste categorie particolari devono sempre verificare l'eventuale esistenza di requisiti nazionali specifici applicabili. È possibile trovare maggiori informazioni nelle Relazioni Nazionali prodotte dal consorzio Panelfit (accessibili su https://www.panelfit.eu/national-reports/).

Sebbene alcuni dati non si considerino come categorie particolari di dati personali di per sé stessi, quando utilizzati insieme ad altri dati potrebbero essere ricondotti a categorie particolari di dati personali. Ad esempio, l'indirizzo e la lingua materna di una persona non

[2] Cfr. anche Ludmilla Georgieva and Christopher Kuner, 'Article 9. Processing of Special Categories of Personal Data', in *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford, United Kingdom: Oxford University Press, 2019), 376–77.

sono considerate categorie particolari di dati personali. Però, quando il nome, il luogo di nascita e altri dati del soggetto interessato sono allegati a un set di dati, la combinazione potrebbe rivelare informazioni sufficienti a identificare l'origine razziale o etnica dell'interessato con un certo grado di sicurezza. In questo scenario, i dati devono essere soggetti agli stessi requisiti e limiti applicabili alle categorie particolari di dati personali, anche se di per sé stessi non lo sono.

Set di dati 1	**Set di dati 2**
Indirizzo: Washington D.C.	Indirizzo: Washington D.C.
Lingua materna: Francese	Lingua materna: Francese
	Nome: Seydou Kablan Bakayoko
	Luogo di nascita: Abidjan
	Altra lingua conosciuta: Cebaara, Inglese
	Scuola elementare: École Konan Raphael, Abidjan
Il set di dati 1 non fornisce informazioni relative all'origine razziale o etnica del soggetto interessato	*Le informazioni fornite dal Set di dati 2 potrebbero essere considerate sufficienti a rivelare l'origine razziale o etnica dell'interessato (con un ragionevole grado di certezza)*

È necessario specificare nuovamente che i dati devono soddisfare un certo grado di certezza. Questo grado di certezza è contestuale e dev'essere valutato caso per caso.

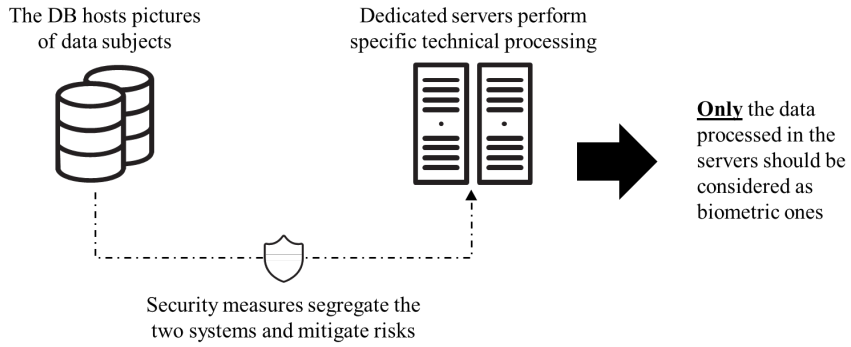
2.2 Dati biometrici

Il termine 'dati biometrici' è definito nell'Articolo 4.14 dell'RGPD. Pertanto, i dati biometrici sono "dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca". La definizione suggerisce che affinché i dati personali siano considerati 'biometrici' devono soddisfare quattro *criteri*[3].

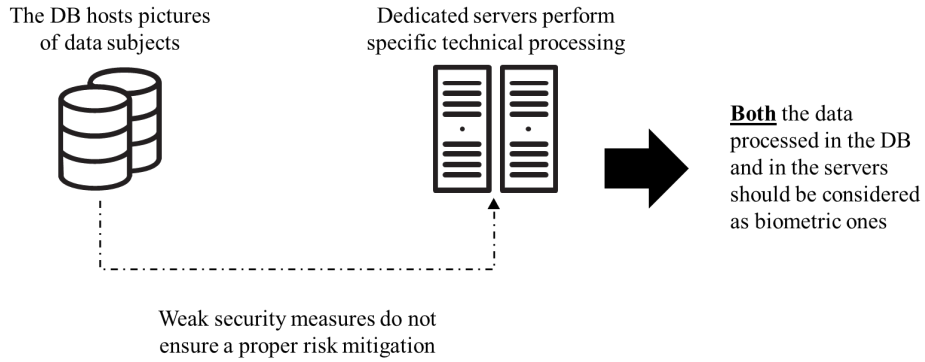
Innanzitutto, devono corrispondere ai ‘dati personali’, definiti nell'Articolo 4.1 dell'RGPD come "informazioni riguardanti una persona fisica identificata o identificabile". In secondo luogo, essi richiedono un 'trattamento tecnico specifico' per l'estrazione delle informazioni dalla fonte di dati grezzi (ad esempio, per estrarre lineamenti del volto da una foto per misurarli). Il considerando 51 dell'RGPD stabilisce che "il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando siano trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica". Quindi, i dati biometrici brevi di un 'trattamento

[3] Sull'analisi della definizione fornita nell'RGPD, cfr. C. Jasserand, ‘Legal Nature of Biometric Data: From “Generic” Personal Data to Sensitive Data’, *European Data Protection Law Review* 2, no. 3 (2016): 297–311, https://doi.org/10.21552/EDPL/2016/3/6.

tecnico specifico' non si annoverano tra i dati biometrici nel contesto dell'RGPD[4]. In ogni caso, anche quando i dati non si considerano come dati biometrici in una determinata fase, essi possono diventare parte di un trattamento di dati che li rende biometrici in una fase successiva. Ad esempio, una base di dati potrebbe contenere immagini che saranno utilizzate per realizzare identificazioni biometriche tramite un trattamento tecnico specifico in una fase successiva (quindi, non considerati ancora come dati biometrici). Immaginiamo uno scenario in cui il suddetto set di dati sia direttamente collegato al sistema che realizza l'identificazione biometrica (cfr. anche la sezione 2.3 Sistema biometrico). In questo caso, soggetti non autorizzati potrebbero utilizzare questo collegamento per accedere a dati biometrici. Ad esempio, essi potrebbero esfiltrare le immagini (non biometriche) contenute nella base di dati e, dopo aver violato il sistema che realizza l'identificazione biometrica, lanciare l'immagine tramite quest'ultimo e realizzare l'identificazione biometrica, ottenendo, quindi, l'accesso ai dati biometrici. In questo scenario, una sicurezza debole garantisce a parti esterne la possibilità di ottenere dati biometrici, anche se questi dati biometrici ancora non esistono. I titolari del trattamento dei dati devono avvicinarsi a quest'ipotesi da una prospettiva di gestione del rischio. Se essi non possono garantire una mitigazione del rischio adeguata ai dati non biometrici (ad esempio, rischi di sfruttamento), questi set di dati devono essere considerati come biometrici e saranno soggetti a tutti i requisiti legali, anche se non rispettano - di per sé stessi - i criteri per essere considerati dati biometrici.



Dati biometrici scenario 1



Dati biometrici scenario 2

[4] Gli studiosi discutono se ciò debba essere applicato anche al trattamento tecnico che costituisce un requisito previo per l'identificazione, come la semplice memorizzazione nella base di dati. Cfr. ad esempio, Kindt, *Having yes, using no? About the new legal regime for biometric data*, Computer Law and Security Review, 34, 2018, pp. 523-538. Per un'analisi delle questioni relative a un formato diverso da quello fotografico, cfr. Andras Nautsch *et al.*, Preserving privacy in speaker and speech characterisation, Computer Speech & Language, 58, 2018, p. 445

Il terzo criterio riguarda le caratteristiche degli interessati captate tramite il trattamento tecnico specifico anteriormente menzionato. Queste caratteristiche possono essere 'fisiche', 'fisiologiche' o 'comportamentali', e sono diverse da altri elementi accidentali come l'indirizzo dell'interessato, la sua ubicazione in un determinato momento, i dati lavorativi, ecc. Il quarto e ultimo criterio stabilisce che per considerare i dati personali come biometrici, essi devono consentire o confermare l'identificazione univoca di una persona. Infatti, i dati biometrici, non necessariamente individuano univocamente gli individui di per se. Ad esempio, i dati biometrici possono essere utilizzati per distinguere tra umani e animali o tra uomini e donne[5]. Comunque, a differenza di altri identificatori come nomi o codici identificativi, il trattamento di dati biometrici non porta a una chiara identificazione. Piuttosto, consente l'identificazione di soggetti con un certo grado di probabilità. Secondo un'opinione consolidata, i dati devono essere considerati come biometrici "anche se i modelli utilizzati nella pratica per misurarli tecnicamente implicano un certo grado di probabilità"[6].

2.3 Sistema biometrico

Il presente capitolo definisce il 'sistema biometrico' come qualsiasi sistema capace di identificare univocamente le persone fisiche (con un certo grado di probabilità) eseguendo un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali delle persone fisiche[7]. La definizione copre sia i sistemi all-in-one che realizzano tutte queste operazioni (ad esempio, acquisizione dei dati, elaborazione dei dati, memorizzazione dei dati, ecc.) che i cluster di sistemi, ciascuno dei quali realizza singole operazioni (ad esempio, una rete di un modulo per la cattura dei dati basato su una fotocamera, un software di mappatura e un set di dati per la conservazione). Quando un sistema esegue una o più operazioni individuali (d'ora in avanti, "sistema X") non si qualifica di per se stesso come sistema biometrico (secondo la definizione anteriormente data), ma è, comunque, parte di un cluster di sistemi che include quelli biometrici, un sistema X deve essere considerato come un sistema biometrico, a meno che non si possa dimostrare (possibilmente con prova documentale) che non esiste trattamento di dati biometrici e che i rischi sono efficacemente mitigati (ad esempio, il rischio di un uso non autorizzato da parte di terzi del sistema X per ottenere l'accesso a un altro sistema direttamente collegato al sistema X quando sono trattati i dati biometrici).

Spesso, i sistemi biometrici si basano sulla tecnologia dell'intelligenza artificiale. L'uso di questa intelligenza artificiale presenta ulteriori rischi di protezione dei dati che i titolari del trattamento devono considerare. È, perciò, raccomandabile consultare il documento 'Orientamenti su questioni etiche e legali relative all'intelligenza artificiale nella ricerca e innovazione nelle TIC'.

2.4 Tipi di dati biometrici

Come già menzionato, è possibile derivare diversi dati biometrici da una serie di caratteristiche di una persona fisica - fisiche, fisiologiche, comportamentali. La presente sezione illustra questi diversi tipi di dati biometrici. La tassonomia che segue non è stabilita

---

[5] Cfr. ad esempio '14 Misunderstandings with Regard to Identification and Authentication' (Agencia espanola proteccion datos, European Data Protection Supervisor, June 2020), 3.

[6] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data', 2007, 8. Cfr. anche Article 29 Data Protection Working Party, 'Opinion 3/2012 on Developments in Biometric Technologies', 2012, 6.

[7] Anche se l'Organizzazione internazionale per la standardizzazione ha elaborato un vocabolario dettagliato dei termini collegato alla biometria, che include la definizione di 'sistema biometrico', il presente documento preferisce adottare una definizione elaborata sulla base delle disposizioni dell'RGPD. Cfr. International Standardization Organization and International Electrotechnical Commission, 'ISO/IEC 2382-37 - Information Technology - Vocabulary - Part 37: Biometrics', 2017.

come standard e determinati tipi di dati biometrici potrebbero essere categorizzati in modo diverso da esperti diversi. Ad esempio, le tassonomie, a volte, raggruppano dati biometrici fisiologici all'interno di dati biometrici fisici.

2.4.1 Dati biometrici fisici

I dati biometrici fisici possono essere generati captando caratteristiche distintive degli individui. La tipicità di queste caratteristiche può, quindi, essere utilizzata come identificatore. Alcune delle caratteristiche biometriche di tipo fisico più comuni sono le impronte digitali, la forma della mano, i lineamenti del viso (come la rotondità del volto, la distanza tra gli occhi, ecc.), e le caratteristiche dell'iride.

2.4.2 Dati biometrici fisiologici

I dati biometrici fisiologici possono essere generati osservando le funzioni corporali e captando modelli distintivi a esse associati. Alcuni dei più comuni dati biometrici sono generati da elettrocardiogrammi (ECG), modelli di respirazione ed elettroencefalogrammi (EEG).

Nonostante i dati biometrici fisici siano, spesso, utilizzati come sinonimo di dati biometrici fisiologici (e viceversa), gli autori ritengono che una differenza potrebbe essere d'aiuto a definire meglio la discussione, specialmente se si considerano i recenti studi sul rapporto tra tecnologia biometrica e certe funzioni fisiologiche, come quelle neurofisiologiche[8].

2.4.3 Dati biometrici comportamentali

I dati biometrici comportamentali possono essere generati osservando il comportamento dei soggetti, per identificare dei modelli distintivi nel suddetto comportamento. Alcuni comportamenti sono inerenti agli individui (come l'andatura o la voce), mentre altri richiedono l'interazione di un determinato strumento per manifestarsi (come la scrittura, la dinamica del tasto e il movimento del mouse).

A differenza dei dati biometrici fisici, i dati biometrici comportamentali richiedono un'osservazione degli individui che introduce un tempo variabile nella valutazione[9]. Si afferma spesso che, pur essendo più variabili alle fluttuazioni e ai cambiamenti momentanei nel corso della vita, i dati biometrici comportamentali hanno il vantaggio di essere meno intrusivi e meno onerosi[10]. In ogni caso, alcuni alunni hanno osservato che i dati biometrici comportamentali possono introdurre maggiori rischi per la privacy rispetto ad altri tipi di dati biometrici[11], grazie alla loro capacità di rivelare ulteriori informazioni sugli interessati, in alcuni casi estremamente sensibili, come le condizioni di salute[12].

2.5 Attività di ricerca

Il termine 'attività di ricerca' non ha una definizione chiara all'interno del quadro normativo. Ai sensi del Considerando 159 dell'RGPD, "il trattamento di dati personali per finalità di

---

[8] Cfr. ad esempio Patrizio Campisi and Daria La Rocca, 'Brain Waves for Automatic Biometric-Based User Recognition', *IEEE Transactions on Information Forensics and Security* 9, no. 5 (May 2014): 782–800, https://doi.org/10.1109/TIFS.2014.2308640.

[9] Cfr. Roman V. Yampolskiy and Venu Govindaraju, 'Behavioural Biometrics: A Survey and Classification', *International Journal of Biometrics* 1, no. 1 (2008): 81, https://doi.org/10.1504/IJBM.2008.018665.

[10] Cfr. Madeena Sultana, Padma Polash Paul, and Marina Gavrilova, 'A Concept of Social Behavioral Biometrics: Motivation, Current Developments, and Future Trends', in *2014 International Conference on Cyberworlds* (2014 International Conference on Cyberworlds (CW), Santander, Cantabria, Spain: IEEE, 2014), 271–78, https://doi.org/10.1109/CW.2014.44.

[11] Cfr. Günter Schumacher, 'Behavioural Biometrics: Emerging Trends and Ethical Risks', in *Second Generation Biometrics: The Ethical, Legal and Social Context*, ed. Emilio Mordini and Dimitros Tzovaras (Springer, 2012).

[12] Cfr. ad esempio Marcos Faundez-Zanuy et al., 'Handwriting Biometrics: Applications and Future Trends in e-Security and e-Health', *Cognitive Computation* 12, no. 5 (September 2020): 940–53, https://doi.org/10.1007/s12559-020-09755-z.

ricerca scientifica dovrebbe essere interpretato in senso lato e includere, ad esempio, sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati".

Il Garante europeo della protezione dei dati (GEPD) identifica l'obiettivo principale delle attività di ricerca come "una conoscenza e benessere collettivo di una società in crescita, come opposti al servizio in favore prevalentemente di uno o più interessi privati"[13]. Quindi, sembra che la mera ricerca di una tecnologia commerciale non potrebbe essere considerata come 'attività di ricerca' ai sensi dell'attuale quadro giuridico (cfr. la sezione 4.1 'Protezione dei dati e ricerca scientifica' nel documento 'Orientamenti su questioni etiche e legali relative all'intelligenza artificiale nella ricerca e innovazione nelle TIC').

3 Dati biometrici nella ricerca e innovazione nelle TIC. Orientamenti

La sezione che segue fornisce una panoramica delle misure concrete che possono essere adottate durante lo sviluppo di tecnologie biometriche o quando le suddette tecnologie sono utilizzate nel contesto della ricerca e dell'innovazione nelle TIC. Queste misure possono aiutare i ricercatori a rispettare le obbligazioni previste in materia di protezione dei dati. Le raccomandazioni sono applicabili ai sistemi biometrici indipendentemente dai dati biometrici che essi generano e trattano (per maggiori informazioni, cfr. 2.3 'Sistema biometrico').

3.1 Fase di progettazione

Durante la fase di progettazione, i ricercatori preparano il campo identificando gli obiettivi e le necessità dell'attività di ricerca.

3.1.1 Identificare gli obiettivi, se l'attività si qualifica come 'ricerca', e i ruoli degli interessati

I ricercatori dovrebbero, innanzitutto, identificare l'obiettivo della loro attività (ad esempio, realizzare uno studio teorico, sviluppare un sistema biometrico, testare quello esistente, ecc.). Questo è un passo importante non solo per definire le finalità per cui i dati personali saranno raccolti, ma anche per aiutare i ricercatori a stabilire se l'attività si qualifica come 'ricerca' e, di conseguenza, se trovano applicazione le disposizioni legali specifiche per l'attività di ricerca. L'articolo 89.2 dell'RGPD, ad esempio, introduce numerose deroghe al trattamento dei dati personali nel contesto della ricerca. In particolare, l'articolo riconosce che alcuni diritti degli interessati (diritto di accesso, diritto di rettifica, diritto di limitazione, diritto di opposizione. Per maggiori informazioni, cfr. il documento 'Diritti degli interessati') renderebbero più difficile o impossibile il raggiungimento dell'obiettivo in alcuni tipi di ricerca. Quindi, stabilisce deroghe a questi diritti quando sono soddisfatti due criteri. In primo luogo, l'eccezione dev'essere esplicitamente prevista dal diritto degli Stati membri o dell'Unione. Ciò significa che, oltre alle disposizioni dell'RGPD, i ricercatori possono essere esentati dall'obbligo di rispettare i suddetti diritti solo nella misura in cui esistano basi giuridiche specifiche nella normativa nazionale o nel diritto dell'UE diverse dall'RGPD (cfr. sezione 3.2.3 'Identificare la base giuridica più adeguata'). In secondo luogo, i ricercatori devono implementare misure tecniche e organizzative adeguate a salvaguardare i diritti e le libertà degli interessati, come richiesto dall'Articolo 89.1 RGPD. Dato l'impatto potenziale di conformità per l'attività di ricerca, è importante valutare immediatamente se l'attività si qualifica come 'ricerca'.

[13] European Data Protection Supervisor, 'A Preliminary Opinion on Data Protection and Scientific Research' (European Data Protection Supervisor, 6 January 2020).

Una corretta definizione del campo di applicazione delle attività è, inoltre, necessaria ai ricercatori per comprendere i rischi della protezione dei dati collegati alla ricerca. Ad esempio, è probabile che i sistemi che devono essere utilizzati nel campo sanitario o dell'applicazione della legge richiedano dei risultati più accurati rispetto a quelli impiegati per attività di svago (come i servizi di musica in streaming). Poiché la precisione di un sistema può, in alcuni casi, dipendere dalla quantità di dati personali da trattare (ad esempio, durante la formazione di un algoritmo di IA), la necessità di maggiore precisione potrebbe introdurre maggiori rischi per la protezione dei dati. I ricercatori devono identificare con chiarezza che livello di precisione dovrà essere soddisfatto dal sistema e definire strategie per garantire che la suddetta precisione venga raggiunta, introducendo il più basso livello di rischio possibile, ad esempio, limitando la quantità di dati personali trattati (cfr. sezione 3.3. 'Minimizzazione dei dati' nel documento 'Orientamenti su questioni etiche e legali relative all'intelligenza artificiale nella ricerca e innovazione nelle TIC').

Infine, ma non meno importante, i ricercatori hanno bisogno di comprendere il loro ruolo e i ruoli degli altri soggetti coinvolti. I ricercatori devono guardare al loro coinvolgimento nel trattamento dei dati previsto per capire se essi (ad esempio, l'ente per cui lavorano) sono gli organismi con le responsabilità principali in materia di trattamento dei dati (titolare del trattamento), se condividono il ruolo di titolari del trattamento con altri organismi (titolare congiunto), o se procedono al trattamento in nome di altri organismi (responsabile del trattamento). I diversi ruoli implicano una distribuzione diversa delle responsabilità. Per maggiori

3.1.2 Confermare la necessità di trattamento dei dati biometrici

Come già accennato, l'RGPD proibisce il trattamento di categorie particolari di dati personali - ivi inclusi quelli biometrici - salvo in presenza di esenzioni specifiche (cfr. la sezione 3.2.3 'Identificare la base giuridica più adeguata'). Quindi, i ricercatori che intendono trattare dati biometrici devono essere certi che il loro trattamento sia necessario per raggiungere l'obiettivo dell'attività di ricerca. Ad esempio, l'obiettivo della ricerca potrebbe essere lo sviluppo e l'esame di un nuovo approccio volto ad aumentare la precisione dei sistemi di rilevamento dei lineamenti del volto. In questo caso, l'obiettivo non è incrementare la precisione dell'identificazione univoca delle persone, ma solo la precisione del rilevamento dei lineamenti del volto. Quindi, i ricercatori potrebbero affidarsi a immagini del viso generate da computer piuttosto che immagini di persone realmente esistenti, rimuovendo la necessità di trattamento di dati personali biometrici. In caso di sviluppo di un sistema, i ricercatori devono, inoltre, considerare il modo in cui il sistema biometrico procederà al trattamento dei dati biometrici dopo il suo sviluppo. Ai ricercatori è richiesto di implementare in anticipo tutte le misure tecniche e organizzative volte a garantire che qualsiasi rischio potenziale sia mitigato e che il trattamento dei dati che si verifica dopo lo spiegamento sia realizzato conformemente al quadro giuridico.

3.2 Fase di preparazione

Durante la fase di preparazione, i ricercatori pongono le basi della ricerca implementando tutto il lavoro di preparazione per l'attività di ricerca.

3.2.1 Nomina di un Responsabile per la protezione dei dati

Il Responsabile per la protezione dei dati (RPD) supporta il titolare del trattamento o il responsabile del trattamento con le norme in materia di protezione dei dati. L'articolo 37 dell'RGPD ordina la nomina di un RPD in cinque casi specifici.

Requisiti per la nomina di un Responsabile per la protezione dei dati (RPD)	
Requisito 1	"Il trattamento è effettuato da un'autorità pubblica o da un organismo

	pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali", Articolo 37.1 RGPD
Requisito 2	"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", Articolo 37.1 RGPD
Requisito 3	"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", Articolo 37.1 RGPD
Requisito 4	"Le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, […] di dati personali relativi a condanne penali e a reati di cui all'articolo 10", Articolo 37.1 RGPD
Requisito 5	"Il titolare 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", Articolo 37.4 RGPD

I requisiti 1 e 3 sono particolarmente rilevanti per il presente documento. Il requisito 1 è rilevante perché non è infrequente che le istituzioni di ricerca siano organismi pubblici, come nel caso degli ospedali pubblici e delle università pubbliche. Qualora si presenti il suddetto scenario, l'Articolo 37.3 RGPD prevede che "un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici". Ad esempio, gli ospedali pubblici potrebbero non aver nominato un RPD, ma potrebbero fare affidamento su un RPD per la fornitura del servizio. Il requisito 3 è rilevante in quanto menziona il trattamento di categorie particolari di dati personali (come i dati biometrici), come uno dei tre criteri per la nomina obbligatoria di un RPD. Gli altri due intervengono quando il trattamento dei dati personali avviene nel contesto di un'attività principale ed è realizzato su larga scala. Il termine 'attività principali' e 'larga scala' non sono espressamente definiti nell'RGPD. Il Gruppo di lavoro dell'Articolo 29 (Article 29 Working Party, WP29), però, fornisce una guida interpretativa nei suoi Orientamenti in materia di Responsabili per la protezione dei dati. In tal senso, le attività principali sono "operazioni chiave per perseguire gli obiettivi del titolare del trattamento e del responsabile del trattamento"[14], con conseguente esclusione delle attività di supporto o accessorie. Nel contesto della ricerca e dell'innovazione nelle TIC, ciò potrebbe essere inteso come qualsiasi attività direttamente collegata all'esecuzione di una ricerca nelle TIC e al raggiungimento di un'innovazione nelle TIC; come nel caso dello sviluppo di un sistema biometrico. Per quanto attiene al criterio di larga scala, il gruppo di lavoro dell'articolo 29 (WP29) lo collega al "numero di soggetti interessati coinvolti (siano essi un numero specifico o una parte della popolazione pertinente), al volume dei dati e/o alla varietà degli elementi di dati da trattare, alla durata o alla permanenza dell'attività di trattamento dei dati [e] all'estensione geografica dell'attività di trattamento"[15].

[14] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Officers ("DPOs")', April 2017, 20.
[15] Article 29 Data Protection Working Party, 21.

Se è richiesta la nomina di un RPD, ciò deve avvenire il prima possibile. Infatti, l'Articolo 39.1 lettera a) RGPD stabilisce che una delle responsabilità dell'RPD è quella di informare e fornire consulenza al titolare del trattamento durante tutte le fasi della ricerca. Quindi, la garanzia della presenza di un RPD il prima possibile garantisce che la ricerca riceva una guida adeguata su come rispettare i requisiti di conformità.

I dati di contatto dell'RPD devono essere pubblicati e resi disponibili ai soggetti interessati.

3.2.2 Identificare l'approccio alla raccolta dei dati

Il passo successivo per i ricercatori è identificare se i dati personali saranno raccolti direttamente dagli interessati o indirettamente (ad esempio, altri ricercatori, basi di dati commerciali, ecc.). Anche se ciò non obbliga necessariamente i ricercatori ad adottare una determinata base giuridica (cfr. la sezione 3.2.3 'Identificare la base giuridica più adeguata'), potrebbe comunque influenzare la suddetta decisione. Ad esempio, se i ricercatori decidono di raccogliere i dati direttamente dagli interessati, essi potrebbero essere più favorevoli all'uso del consenso come base giuridica, in quanto viene comunque instaurato un rapporto diretto con gli interessati. Inoltre, ai sensi degli Articoli 13 e 14 dell'RGPD, la scelta di un approccio diretto o indiretto in materia di raccolta dei dati cambia il tipo di informazioni che i titolari del trattamento hanno bisogno di fornire agli interessati.

Informazioni da fornire agli interessati ai fini della raccolta		
	Direttamente	**Indirettamente**
I dati personali e di contatto del titolare del trattamento	☐	☐
Se del caso, l'identità e i dati di contatto del rappresentante del titolare del trattamento	☐	☐
I dati di contatto del Responsabile per la protezione dei dati	☐	☐
Le finalità del trattamento	☐	☐
Le categorie di dati interessate		☐
La base giuridica per il trattamento	☐	☐
Se del caso, gli interessi legittimi perseguiti dal titolare del trattamento o da terzi	☐	☐
Destinatari o categorie di destinatari dei dati personali	☐	☐
L'intenzione del titolare del trattamento di trasferire i dati personali a un paese terzo o un'organizzazione internazionale	☐	☐
In caso di trasferimento, l'esistenza o meno di una decisione di adeguatezza della Commissione, o, se del caso, un riferimento alle garanzie e alle misure attraverso cui ottenere una copia dei dati	☐	☐
Il periodo di conservazione dei dati personali o, qualora ciò non sia possibile, i criteri utilizzati per definire detto periodo	☐	☐

L'esistenza del diritto di richiedere l'accesso a e la correzione o cancellazione dei dati o la limitazione del trattamento relativo all'interessato o di opporsi al trattamento e il diritto alla portabilità dei dati	☐	☐
In caso di 'consenso esplicito' come base giuridica del trattamento, l'esistenza del diritto alla revoca del consenso in qualsiasi momento	☐	☐
Il diritto a presentare un reclamo dinanzi all'autorità di controllo	☐	☐
La fonte dei dati personali e, se del caso, se essi provengono da fonti pubblicamente accessibili		☐
Se la fornitura dei dati deriva da un requisito normativo o contrattuale, o un requisito per la conclusione di un contratto, e se l'interessato è obbligato a fornire i dati e le conseguenze della mancata fornitura dei suddetti dati	☐	
L'esistenza di un processo decisionale automatizzato, inclusa la profilazione	☐	☐
In caso di processo decisionale automatizzato, le informazioni relative alla logica utilizzata, l'importanza del trattamento e le possibili conseguenze per l'interessato	☐	☐

L'RGPD riconosce che potrebbero esserci casi in cui questo dovere d'informazione potrebbe non essere applicabile ed enumera una serie di eccezioni nell'Articolo 14.5 dell'RGPD. Queste eccezioni sono:

- I soggetti dispongono già delle informazioni;
- La comunicazione di queste informazioni:
    - risulta impossibile;
    - implicherebbe uno sforzo sproporzionato,
    - è probabile che renda impossibile o pregiudichi seriamente il raggiungimento degli obiettivi di quel trattamento.

A questo proposito, è importante chiarire che quest'eccezione si applica soprattutto per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e garanzie previste dall'Articolo 89.1 dell'RGPD.

Inoltre, nei suddetti casi, il titolare del trattamento adotterà le misure adeguate per proteggere i diritti e le libertà degli interessati, così come i loro interessi legittimi, anche rendendo pubbliche le informazioni;

- Il diritto dell'UE o di uno Stato membro richiede al titolare del trattamento di ottenere o rivelare i dati personali; o
- Quando i dati personali devono rimanere confidenziali ai sensi di un obbligo di segreto professionale disciplinato dal diritto dell'Unione o di uno Stato membro, ivi incluso il caso di un obbligo di segretezza previsto per legge.

Indipendentemente dalla forma di raccolta dei dati, il titolare del trattamento realizzerà i passi adeguati a garantire che i dati siano precisi e aggiornati (ad esempio, un audit di precisione

periodico). La raccolta dei dati direttamente dagli interessati potrebbe aiutare a ridurre il rischio di imprecisione (soprattutto nel caso dei dati biometrici comportamentali, che potrebbero cambiare con il tempo). Inoltre, il titolare del trattamento deve garantire la trasparenza in tutte le fasi del processo (cfr. sezione 3.1. 'Legittimità, equità e trasparenza' nel documento 'Orientamenti su questioni etiche e legali relative all'intelligenza artificiale nella ricerca e innovazione nelle TIC'). Per una spiegazione più dettagliata relativa al diritto d'informazione e le sue sfumature, leggere il documento 'Diritti degli interessati'.

3.2.3 Identificare la base giuridica più adeguata

Uno dei passi più importanti dal punto di vista della protezione dei dati è l'identificazione della base giuridica per il trattamento dei dati personali, definita dall'Articolo 6 RGPD. In ogni caso, come già accennato, il trattamento dei dati biometrici è proibito e può avvenire soltanto in caso di applicazione di esenzioni specifiche. Esse sono previste dall'Articolo 9.2 RGPD e sono di due tipi. Quelle immediatamente valide e applicabili, e quelle che richiedono diritto ulteriore dell'Unione o di uno Stato membro prima di poter essere utilizzate per giustificare il trattamento di dati biometrici.

Basi giuridiche disponibili previste dall'RGPD per il trattamento dei dati biometrici	
	Richiede diritto ulteriore dell'UE o di uno SM
Consenso esplicito	
Lavoro, previdenza sociale e assistenza sociale	?
Interessi vitali	
Attività di associazioni e altri enti no-profit	
I dati sono stati pubblicati dall'interessato	
Reclami legali o atti giudiziari	
Interesse pubblico sostanziale	?
Salute o assistenza sanitaria	?
Interesse pubblico alla salute	?
Archivio, ricerca e statistica	?

In caso di applicazione di una di queste esenzioni, è possibile per il titolare del trattamento selezionare una delle basi giuridiche previste dall'Articolo 6 RGPD e procedere di conseguenza al trattamento dei dati personali.

Delle dieci esenzioni previste dall'Articolo 9.2 RGPD, due sono particolarmente rilevanti nel presente documento. La prima è il requisito del 'consenso esplicito'. Nel contesto del trattamento dei dati biometrici, il consenso degli interessati dev'essere 'esplicito', il che significa che dev'essere una dichiarazione chiara, specifica e inequivocabile con cui gli

interessati acconsentano al trattamento dei propri dati biometrici per le finalità specifiche identificate dal titolare del trattamento[16]. Ad esempio, nel caso di trattamento di dati biometrici estratti da immagini, non sarà sufficiente raccogliere il consenso degli interessati al trattamento delle suddette immagini. Gli interessati devono essere informati circa le caratteristiche biometriche che saranno estratte e processate, e si dovrà ottenere un consenso esplicito.

Esempio: Consenso vs. consenso esplicito	
Consenso	**Consenso esplicito**
"Si prega di fornire un'immagine di sé stessi frontale, scattata in un ambiente ben illuminato. L'immagine sarà utilizzata per estrarre elementi biometrici allo scopo di sviluppare un nuovo sistema di riconoscimento biometrico."	"A - Si prega di fornire un'immagine di sé stessi frontale, scattata in un ambiente ben illuminato. B - L'immagine sarà utilizzata per estrarre elementi biometrici allo scopo di sviluppare un nuovo sistema di riconoscimento biometrico. C - Prima di procedere all'invio dell'immagine, si prega di spuntare la seguente casella per indicare che si sta fornendo il proprio consenso come soggetto interessato al trattamento della propria immagine a scopo di estrazione di elementi biometrici da processare per le finalità descritte nel punto B. Spuntare la casella ☐"

Quando si parla di consenso nell'ambito della ricerca, è, inoltre, importante distinguere tra consenso a partecipare a uno studio e consenso al trattamento dei propri dati personali. Si tratta di due diversi tipi di consenso che devono essere raccolti in modo indipendente[17]. Il team di ricerca può utilizzare un unico modulo di consenso, sempre che il modulo distingua chiaramente tra i due tipi di consenso e non li riunisca in un unico accordo (per maggiori informazioni, cfr. il documento 'Analisi delle questioni e delle lacune in materia di consenso informato nel contesto della ricerca e innovazione nelle TIC').

Un'altra esenzione al trattamento di una categoria particolare di dati personali rilevante ai fini del presente documento è l'esenzione per il trattamento necessario alle attività di ricerca. L'esenzione, per essere applicabile, deve soddisfare due criteri. In primo luogo, il trattamento dev'essere soggetto ad adeguate misure tecniche e organizzative ai sensi dell'Articolo 89.1 RGPD. In secondo luogo, deve esistere una norma nel diritto dell'Unione o degli Stati membri

[16] L'RGPD riconosce nel Considerando 33 che potrebbe non essere possibile individuare pienamente la finalità del trattamento dei dati personali al momento della raccolta dei dati e, perciò, dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni "settori della ricerca scientifica". Il punto sollevato dal Considerando 33, così come un certo numero di chiavi d'interpretazione, sono stati oggetto di indagine nel documento 'Analisi delle questioni e delle lacune in materia di consenso informato nel contesto della ricerca e innovazione nelle TIC'.

[17] Cfr. European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679', May 2020, 30; European Data Protection Board, 'Opinion 3/2019 Concerning the Questions and Answers on the Interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation', 2019.

che fornisca una base giuridica per il trattamento nell'ambito di un'attività di ricerca. Quest'ultimo criterio implica che l'esenzione per scopi di ricerca potrebbe non essere applicabile in tutti i casi. Quindi, i ricercatori devono eseguire un riesame della normativa nazionale di tutti gli Stati in cui la ricerca sarà condotta, allo scopo di verificare la presenza o meno di queste norme (cfr. Allegato III 'Studio comparativo dei rapporti nazionali' nel documento 'Orientamenti su questioni etiche e legali relative all'intelligenza artificiale nella ricerca e innovazione nelle TIC').

3.2.4 Creare un deposito per la documentazione giustificativa

L'RGPD richiede che i titolari del trattamento non solo rispettino le obbligazioni in materia di protezione dei dati, ma siano anche capaci di dimostrare la loro conformità con le suddette obbligazioni e con i principi contenuti nella norma. Ciò significa che il titolare dei dati deve mantenere i registri pertinenti e la documentazione relativa al trattamento dei dati e la governance del suddetto trattamento.

A parte una serie limitata di documenti chiaramente obbligatori (come il registro delle attività di trattamento richiesto dall'Articolo 30 RGPD), è dovere del titolare del trattamento identificare quali sono i documenti necessari a dimostrare la suddetta conformità. Le tabelle che seguono presentano la lista dei documenti richiesti dall'RGPD con la relativa ubicazione all'interno del testo. Esse devono essere considerate come una base minima piuttosto che una lista di controllo esaustiva. Infatti, anche se non obbligatori, potrebbero essere necessari ulteriori documenti per dimostrare la conformità (ad esempio, rapporti di consultazioni previe con le autorità di controllo, descrizione delle misure tecniche e organizzative implementate, ecc.)

Documentazione: lista di controllo		
1	Politica in materia di protezione dei dati personali	Articolo 24.2
2	Informativa sulla privacy	Articoli 12, 13, 14
3	Politica di conservazione dei dati	Articoli 5, 13, 17 e 30
4	Schema di conservazione dei dati	Articolo 30
5	Registro delle attività di trattamento (se del caso)	Articolo 30
6	Modulo per il consenso (se del caso)	Articoli 6, 7, 9
7	Accordo di trattamento dei dati con i fornitori	Articoli 28, 32, 82
8	Valutazione d'impatto della protezione dei dati	Articolo 35
9	Nomina di un rappresentante UE (se del caso)	Articolo 27
10	Procedura di risposta e notifica della violazione dei dati	Articoli 4, 33, 34
11	Notifica della violazione dei dati all'Autorità di controllo (se del caso)	Articolo 33
12	Notifica della violazione dei dati agli interessati (se del caso)	Articolo 34

Alcuni documenti sono necessari solo in caso di applicazione di un criterio specifico.

Documentazione essenziale in condizioni specifiche

Registro delle attività di trattamento	In presenza di 250 dipendenti o più, salvo quando il trattamento potrebbe provocare un rischio ai diritti e le libertà degli interessati, non è occasionale o include categorie particolari di dati personali o dati personali relativi a condanne penali e reati
Modulo per il consenso	Se il trattamento si fonda sul consenso come base giuridica e se il trattamento è stato realizzato in forma scritta[18]
Nomina di un rappresentante UE	Se il trattamento riguarda persone stabilite nell'UE ed è realizzato da un titolare del trattamento o da un responsabile del trattamento non stabiliti nell'UE, se non occasionale, non riguarda un trattamento su larga scala o categorie particolari di dati o dati personali relativi a condanne penali o reati ed è improbabile che si verifichi un rischio per i diritti e le libertà delle persone fisiche
Notifica della violazione dei dati all'Autorità di controllo	Solo quando si verifica una violazione dei dati suscettibile di provocare un rischio per i diritti e le libertà delle persone fisiche
Notifica della violazione dei dati agli interessati	Quando si verifica una violazione dei dati suscettibile di provocare un rischio elevato per i diritti e le libertà delle persone fisiche o, quando è improbabile che si verifichi questo rischio elevato, se l'autorità di controllo lo richiede

Al fine di rendere il registro più semplice e coerente, il ricercatore deve preparare dei modelli adeguati per le fasi da documentare o consultare l'RPD o il suo dipartimento legale in sostituzione dell'RPD, per verificare l'esistenza di modelli all'interno dell'organizzazione.

Prima di iniziare con la raccolta e il trattamento di dati personali, i ricercatori devono riunire la documentazione per la protezione dei dati già disponibile nella propria organizzazione, e creare un dossier specifico contenente tutta la documentazione pertinente. I nuovi documenti devono essere aggiunti al dossier subito dopo la loro creazione. Lo scopo del dossier è registrare tutte le fasi e le decisioni adottate dai ricercatori e dagli altri interessati dalla protezione dei dati coinvolti nell'attività di ricerca, così come presentare informazioni sufficienti a dimostrare che è stata mantenuta la conformità durante il processo.

Il team di ricerca deve considerare il dossier non come una mera obbligazione di registro. Il dossier deve agire come la formalizzazione di una fase pratica realizzata dal team di ricerca per garantire la salvaguardia dei dati personali. Ad esempio, disporre di una procedura di risposta e notifica della violazione dei dati non è sufficiente. I ricercatori devono essere in grado di dimostrare che la procedura può essere messa in atto prontamente ed efficacemente, se necessario.

3.2.5 Verificare la necessità di una DPIA

Secondo il gruppo di lavoro dell'Articolo 29, una valutazione d'impatto della protezione dei dati (Data Protection Impact Assessment, DPIA) è "un processo disegnato per descrivere il trattamento (di dati personali), valutarne la necessità e proporzionalità e aiutare a gestire i

[18] Infatti, l'RGPD non obbliga a che il consenso sia raccolto in forma scritta. Per maggiori informazioni, cfr. European Data Protection Board, 'Guidelines 05/2020 on Consent', 16.

rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei dati personali, valutandoli e stabilendo le misure da adottare per farvi fronte"[19].

L'Articolo 35.1 dell'RGPD richiede che i titolari del trattamento realizzino una DPIA quando il trattamento dei dati potrebbe prevedibilmente provocare un elevato rischio per i diritti e le libertà delle persone fisiche. Quindi, una DPIA non è sempre obbligatoria. In ogni caso, si richiede ai titolari del trattamento di eseguire sempre una valutazione preliminare del rischio per stabilire se il trattamento può provocare rischi elevati per i diritti e le libertà delle persone fisiche. Questa valutazione preparatoria è parte integrante del processo della DPIA. Quindi, è possibile dire che alcuni elementi della DPIA sono obbligatori, quantomeno, per determinare se una DPIA è necessaria.

I rischi per i diritti e le libertà degli interessati sono analizzati nel Considerando 75 dell'RGPD. Si tratta dei rischi suscettibili di causare danni fisici, materiali o immateriali all'interessato coinvolto (ad esempio, negandogli l'accesso al servizio a seguito di un'identificazione negativa falsa).

Esempi di rischi per i diritti e le libertà	
Discriminazione	Furto d'identità o frode
Perdita finanziaria	Danno alla reputazione
Perdita della riservatezza del segreto professionale	Annullamento non autorizzato della pseudonimizzazione
Svantaggio economico o sociale	Impossibilità di esercitare controllo sui dati personali

L'RGPD non definisce il concetto di 'rischio elevato'. In ogni caso, il Gruppo di lavoro dell'articolo 29 ha elaborato una lista di nove criteri che i titolari del trattamento possono seguire per comprendere se il trattamento può essere considerato ad alto rischio[20].

Criteri per il trattamento ad alto rischio	
Criterio 1	Valutazione o punteggio (ad esempio, profilazione)
Criterio 2	Processo decisionale automatizzato con efficacia giuridica o simile
Criterio 3	Monitoraggio sistematico
Criterio 4	Dati sensibili o dati altamente confidenziali
Criterio 5	Dati trattati su larga scala
Criterio 6	Corrispondenza o combinazione di set di dati (oltre le aspettative ragionevoli dell'interessato)
Criterio 7	Dati relativi a soggetti vulnerabili

[19] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679', October 2017, 4.

[20] Article 29 Data Protection Working Party, 9–11.

Criterio 8	Uso innovativo o applicazione di nuove tecnologie o soluzioni organizzative
Criterio 9	Quando il trattamento in sé impedisca agli interessati di esercitare un diritto o utilizzare un servizio o contratto

I ricercatori che svolgono la loro attività di ricerca devono considerarli tutti per comprendere se è necessaria una DPIA. Ancora, il criterio quattro e otto sono particolarmente rilevanti ai fini del presente documento. Il criterio quattro è rilevante quando i dati biometrici oggetto di trattamento sono trattati durante l'attività di ricerca. Il criterio otto è importante nell'ambito della ricerca nelle TIC, in quanto quest'attività potrebbe introdurre una nuova tecnologia per il trattamento dei dati (ad esempio, forme innovative di catturare e analizzare campioni vocali).

L'Articolo 35.4 dell'RGPD richiede alle autorità di controllo nazionali di pubblicare la lista delle attività di trattamento dei dati per cui è obbligatoria una DPIA[21]. Ciò potrebbe offrire un'ulteriore guida quanto a ciò che costituisce un trattamento che richieda una DPIA, e i ricercatori dovrebbero prestare attenzione alla posizione delle autorità di controllo pertinenti. Inoltre, i ricercatori devono richiedere il supporto dell'RPD dell'organizzazione, data la complessità della funzione in questione.

Al fine di poter dimostrare la conformità, la valutazione sul se il trattamento sia suscettibile di provocare un rischio elevato per i diritti e le libertà delle persone fisiche dev'essere documentata e conservata.

3.2.6 Eseguire una DPIA (se necessario)

Non esiste una modalità standard di realizzazione di una DPIA. In ogni caso, l'Articolo 35.7 dell'RGPD richiede elementi specifici che devono essere sempre tenuti presenti. Essi sono:

- Una descrizione sistematica dei trattamenti previsti;
- le finalità del trattamento;
- una valutazione della necessità dei trattamenti in relazione alle finalità;
- una valutazione della proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure tecniche e organizzative previste per affrontare i rischi.

I ricercatori possono includere elementi ulteriori per descrivere meglio il trattamento e i rischi sottostanti. Inoltre, se il titolare del trattamento rileva, una volta eseguita la DPIA, che i rischi per i diritti e le libertà degli interessati non sono adeguatamente mitigati dalle misure previste per affrontare i suddetti rischi, il titolare del trattamento deve consultare preventivamente l'autorità di controllo ai sensi di quanto previsto dall'Articolo 36 dell'RGPD.

La legge non stabilisce un formato per la DPIA. Esso può essere liberamente scelto dal titolare del trattamento. Alcune autorità di protezione dei dati, in ogni caso, hanno creato dei modelli che i titolari del trattamento possono adottare[22].

[21] A questo proposito, le autorità di controllo nazionali hanno pubblicato sui loro siti web la lista corrispondente. In alcuni casi, l'EDPB ha già emesso un parere sulla questione relativa alle attività incluse in ciascuna lista. Per maggiori informazioni, cfr. European Data Protection Board, 'Opinion 6/2019 on the Draft List of the Competent Supervisory Authority of Spain Regarding the Processing Operations Subject to the Requirement of a Data Protection Impact Assessment (Article 35.4 GDPR)', March 2019.

[22] Cfr. ad esempio Commision Nationale Informatique & Libertés, 'Privacy Impact Assessment (PIA). Templates', February 2018.

La DPIA non è un'attività sporadica, ma un processo continuo. Perciò, potrebbe essere necessario eseguire più valutazioni nel tempo, ad esempio quando gli elementi contestuali cambiano o quando diventano disponibili nuove informazioni.

I risultati delle DPIA saranno registrati e conservati come parte della documentazione relativa alla protezione dei dati.

3.2.7 Implementare misure di mitigazione del rischio

Ai sensi del Considerando 78 dell'RGPD, "la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento [l'RGPD]". Questa disposizione, che rappresenta la pietra miliare del quadro giuridico, è ulteriormente elaborata per il caso specifico di trattamento per finalità di ricerca. Il Considerando 156 RGPD e l'Articolo 89 RGPD prevedono l'implementazione di 'misure adeguate', sottolineando l'importanza della tutela dei diritti e le libertà delle persone fisiche.

L'RGPD non fornisce una lista esaustiva delle misure tecniche e organizzative, lasciando al titolare del trattamento il compito di identificarle e valutarne l'efficacia per la mitigazione dei rischi per gli interessati. Inoltre, i ricercatori devono considerare l'opportunità di un audit sulla protezione dei dati e sulla sicurezza esterna, per confermare la solidità delle misure di sicurezza e di conformità, e dimostrare l'ulteriore conformità con il principio di responsabilità.

Esempi di misure tecniche e organizzative	
Misure tecniche	**Misure organizzative**
Anonimizzazione dei dati o pseudonimizzazione[23]	Politica in materia di sicurezza
Cifratura della comunicazione	Programmi di gestione dei dati
Protezione dei dati dall'accesso non autorizzato	Programma di formazione per il personale
Valutazione di vulnerabilità / Test di penetrazione	Audit e valutazioni regolari

3.3 Fase di esecuzione

Una volta preparata adeguatamente l'attività di ricerca, i ricercatori possono iniziare il loro lavoro e le relative attività di trattamento dei dati. Questa fase inizia con la raccolta dei dati ai sensi del programma definito durante la fase di preparazione.

3.3.1 Trattamento di dati biometrici

Una volta ottenuti dai ricercatori i dati biometrici necessari, essi possono essere trattati per estrarre caratteristiche biometriche da utilizzare nella ricerca. Sebbene sia teoricamente possibile farlo manualmente (ad esempio, mappatura manuale dei lineamenti del viso nelle immagini, come la distanza tra gli occhi, la forma del viso, l'altezza delle orecchie, ecc.)[24],

[23] Cfr. anche la sezione 3.3.5 Cancellazione o distruzione dei dati per maggiori informazioni sull'anonimizzazione. Per maggiori informazioni tecniche, cfr. la DOCUMENTAZIONE PANELFIT IN MATERIA DI ANONIMIZZAZIONE.

[24] Alcune tecniche di riconoscimento biometrico sono state scoperte come tecniche manuali, e sono addirittura anteriori a un sistema informatico. Cfr. ad esempio Mark Maguire, 'The Birth of Biometric Security', *Anthropology Today* 25, no. 2 (April 2009): 9–14, https://doi.org/10.1111/j.1467-8322.2009.00654.x.

oggi tale tipo di approccio è generalmente considerato impossibile e sostituito da mezzi automatizzati spesso basati su una tecnologia di intelligenza artificiale (per una guida specifica, consultare il documento 'Orientamenti su questioni etiche e legali relative all'intelligenza artificiale nella ricerca e innovazione nelle TIC'). Indipendentemente da questa differenza, qualsiasi attività di trattamento dev'essere condotta adottando tutte le misure e le precauzioni stabilite durante la fase di preparazione.

3.3.2 Sistema biometrico e sviluppo di un'interfaccia utente

Se lo scopo della ricerca è di sviluppare un sistema biometrico, i ricercatori dovranno porre particolare cura nella creazione dell'interfaccia utente, soprattutto se il sistema è destinato al pubblico. L'interfaccia dev'essere disegnata nel modo più fruibile possibile allo scopo di promuovere la trasparenza e semplificare agli interessati l'esercizio del loro diritto d'informazione. Ci sono tre aspetti che i ricercatori devono considerare. Essi sono le informazioni disponibili attraverso l'interfaccia utente, le funzionalità accessibili tramite l'interfaccia utente e la fruibilità generale dell'interfaccia.

Innanzitutto, il titolare del trattamento deve garantire che tutte le informazioni fornite agli interessati ai sensi degli Articoli 13 e 14 dell'RGPD sono disponibili sull'interfaccia utente. Esse devono essere facilmente accessibili e presentate in modo chiaro e comprensibile. Ad esempio, il sistema potrebbe presentare un pulsante visibile che gli interessati possono cliccare per aprire una finestra di pop-up contenente le informazioni. Si consiglia di tenere le informazioni prontamente disponibili nel sistema ed evitare, se possibile, collegamenti a depositi o siti web esterni per ridurre al minimo il rischio d'inaccessibilità dovuto, ad esempio, a problemi di connettività. L'interfaccia utente deve, inoltre, far leva sulle capacità del dispositivo tramite cui si accede alle informazioni. Ad esempio, qualora un sistema funzioni su uno smartphone, dovrebbe fornire l'opzione di chiamare o inviare direttamente un messaggio email all'RPD con un semplice click[25].

In secondo luogo, l'interfaccia utente deve presentare una serie di funzionalità volte a rendere più semplice per gli interessati l'esercizio dei loro diritti (sempre che non sia presente un'esenzione per l'applicazione dei suddetti diritti. Cfr. la sezione 3.2.2Identificare l'approccio alla raccolta dei dati). Ad esempio, l'interfaccia utente deve rendere possibile agli interessati l'accesso ai loro dati personali per rettificarli o cancellarli (in quanto ciò non rende la finalità del trattamento impossibile da raggiungere). Avere delle funzionalità specifiche accessibili agli interessati non solo gli renderà più semplice l'esercizio dei loro diritti, ma alleggerirà anche il peso sui titolari del trattamento, in quanto molte di queste richieste saranno realizzate direttamente dagli interessati. Ad esempio, gli utenti di sistemi di riconoscimento facciale potrebbero dover aggiornare le loro immagini (ad esempio, dopo un intervento chirurgico). Fornire loro un modo diretto per farlo, diverso dal dover contattare il titolare del trattamento, potrebbe incentivarli a mantenere i dati aggiornati e, quindi, a garantire l'aderenza ai principi di precisione. In ogni caso, l'introduzione di queste funzionalità può anche aumentare il rischio per i diritti e delle libertà degli interessati. Ad esempio, in caso di violazione dell'account di un utente, quest'opzione 'self-service' fornisce all'attaccante il pieno controllo sui dati degli interessati. Quindi, il titolare del trattamento deve sempre garantire che qualsiasi rischio aggiuntivo introdotto da funzionalità specifiche è adeguatamente mitigato da adeguate misure di sicurezza (ad esempio, un'autenticazione multi-fattoriale, un aggiornamento obbligatorio della password, ecc.). Qualora i ricercatori non possano mitigare adeguatamente i rischi derivanti dall'introduzione di nuove funzionalità, dovranno consultare preventivamente l'autorità di controllo pertinente o evitare l'introduzione delle funzionalità fino a quando non sia trovato un approccio di mitigazione fattibile.

[25] Ciò nonostante, devono essere visualizzati anche i contatti, e il sistema non deve imporre alcun mezzo specifico di comunicazione.

In terzo luogo, la fruibilità generale dell'interfaccia favorirà la trasparenza ed eviterà di appesantire inutilmente i soggetti interessati nell'esercizio dei loro diritti. Un'interfaccia utente adeguata dovrebbe considerare elementi come le caratteristiche degli interessati (ad esempio, lingua, demografia, ecc.), il modo in cui gli utenti interagiscono con il sistema (ad esempio, su un PC, uno smartphone, un hardware personalizzato, ecc.), il luogo in cui gli utenti interagiscono con il sistema (ad esempio, a casa, in uno spazio pubblico, ecc.), opzioni alternative (ad esempio, quando gli utenti modificano involontariamente alcune impostazioni) e molti altri elementi. Inoltre, gli sviluppatori devono tener presente che il sistema potrebbe essere utilizzato da soggetti vulnerabili, come bambini o persone con disabilità visive. Quindi, l'interfaccia dev'essere disegnata in modo da aiutarli a utilizzare il sistema (ad esempio, voce al testo, ingrandimento del testo, ecc.).

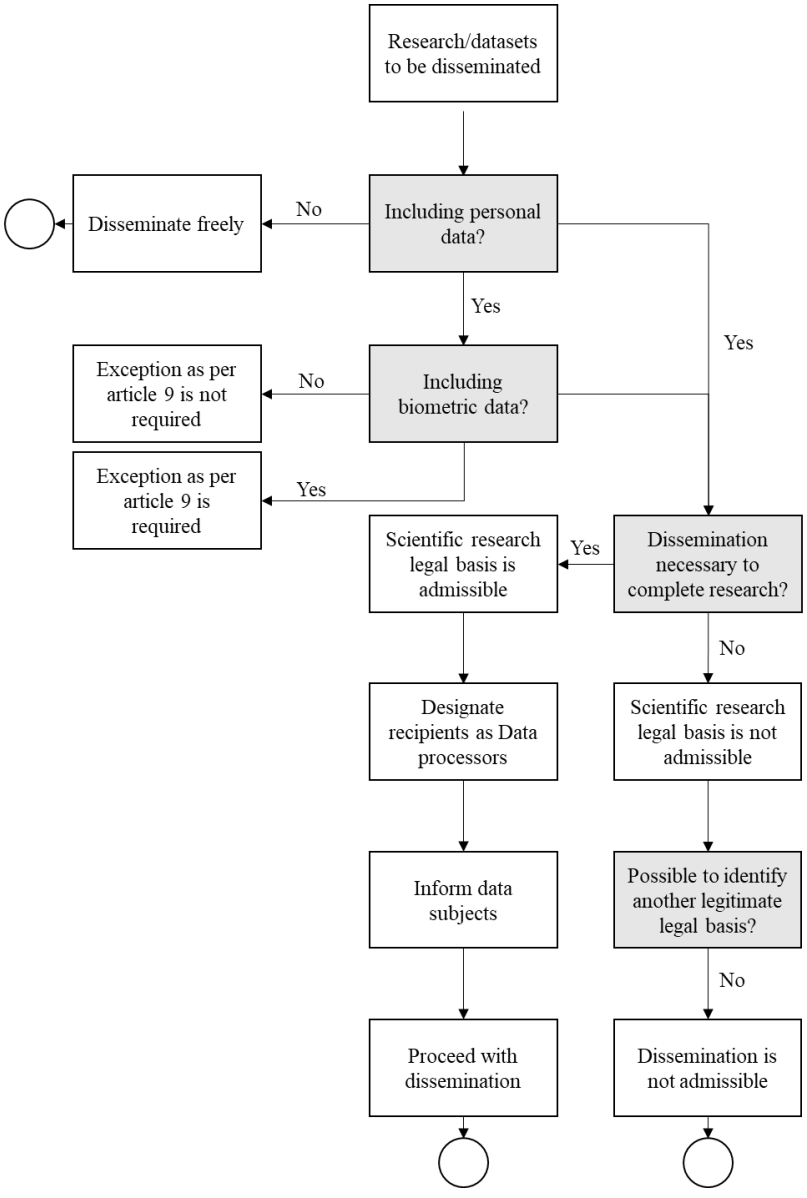
3.3.3 Verifica del Sistema biometrico

Il passo finale prima del dispiegamento del sistema biometrico è quello di testare e convalidarne i risultati. Ci sono due scenari possibili. Nel primo, i nuovi dati devono essere raccolti, mentre, nel secondo, i ricercatori utilizzano gli stessi dati trattati durante la fase di sviluppo. Il primo scenario si verifica quando, ad esempio, i nuovi soggetti sono utilizzati specificamente per testare il sistema. In questo caso, il titolare del trattamento deve eseguire i passi anteriormente menzionati relativamente alla fase di preparazione. Nel secondo scenario, i ricercatori devono considerare se questa ulteriore verifica era compresa tra le finalità iniziali (per maggiori informazioni, cfr. la sezione 3.2). ‘Limitazione delle finalità’ nel documento ‘Orientamenti su questioni etiche e legali relative all'intelligenza artificiale nella ricerca e innovazione nelle TIC’). Infatti, 'la verifica del sistema' configura un trattamento diverso rispetto allo 'sviluppo del sistema' e potrebbe, quindi, richiedere una base giuridica diversa, soprattutto quando i due trattamenti richiedono diversi set di dati. In questi casi, i ricercatori non devono ritenere che, poiché hanno osservato le obbligazioni relative allo sviluppo del sistema, essi hanno automaticamente osservato quelle relative alla verifica. È importante che essi considerino questa fase con un approccio critico e aspirino a minimizzare i rischi per i diritti e le libertà degli interessati come una priorità.

3.3.4 Diffusione dei risultati

Alla fine dell'attività di ricerca, i ricercatori possono decidere di diffondere il loro lavoro. Se la diffusione non include i dati personali trattati durante la ricerca, il lavoro può essere diffuso ad altre parti interessate. Se la diffusione include i dati trattati durante la ricerca (ad esempio, rendere i dati disponibili alla comunità scientifica per una revisione paritaria), allora è necessario realizzare passi ulteriori. La diffusione di dati personali costituisce un'operazione di trattamento ai sensi dell'Articolo 4.2 dell'RGPD e (come descritto anteriormente) qualsiasi operazione di trattamento che implichi dati biometrici dev'essere proibita, salvo l'applicabilità di esenzioni. Quindi, i ricercatori devono ripetere le fasi già descritte nel 3.2.2 prima di procedere alla diffusione. In particolare, se il titolare del trattamento si basa sulle basi giuridiche della 'ricerca scientifica', e se sono soddisfatti tutti i requisiti per l'adozione della suddetta base giuridica (cfr. la sezione 3.2.3 ‘Identificare la base giuridica più adeguata’), è possibile distinguere due ulteriori scenari. Nel primo, il team di ricerca (Team A) ha completato l'attività di ricerca e intende diffondere i dati a vantaggio di altri team di ricerca (Team B). In questo scenario, la diffusione non è un'operazione necessaria per il raggiungimento delle finalità del Team A, ma potrebbe essere necessaria per le finalità di ricerca del Team B. Quindi, il Team A non può fare affidamento sulla base giuridica della 'ricerca scientifica'. Ne consegue che il Team A non ha alcuna base giuridica per condividere i dati con il Team B né con nessun altro destinatario, salvo che si trovi un'altra base giuridica (ad esempio, il Team A può ottenere un consenso esplicito per le finalità di condivisione dei dati con il Team B). Nel secondo scenario, il Team A realizza, dopo la raccolta dei dati personali, di non disporre della capacità (tecnica) adeguata per il trattamento dei dati e la

prosecuzione della ricerca. Quindi, il Team A decide di fare affidamento sulla capacità del Team B per il trattamento dei dati. In questa situazione, la diffusione dei dati al Team B è un passo necessario per raggiungere le finalità di ricerca del Team A, e il Team B ha bisogno di essere nominato 'responsabile del trattamento' ai sensi dell'Articolo 28 RGPD. L'Articolo 4.8 dell'RGPD definisce il responsabile del trattamento come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento". La designazione e le funzioni del responsabile del trattamento devono essere comunicate all'interessato prima del trasferimento e devono essere rette da un contratto o dal diritto dell'Unione o di uno Stato membro, che deve contenere almeno la materia e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e di categorie di soggetti interessati e le obbligazioni e diritti del titolare del trattamento.



Qualora i dati personali debbano essere trasferiti al di fuori dello Spazio Economico Europeo[26], e sempre che il suddetto trasferimento non sia soggetto a una o più deroghe previste nell'Articolo 49 RGPD[27], sarà necessario compiere ulteriori passi. L'RGPD prevede una serie di strumenti per il trasferimento di dati internazionali. In ogni caso, non tutti sono

[26] Che include tutti gli Stati membri dell'UE, insieme a Islanda, Liechtenstein e Norvegia.

[27] Per maggiori informazioni, cfr. European Data Protection Board, 'Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679', May 2018.

attualmente applicabili, in quanto l'autorità pertinente sta ancora lavorando per formalizzare alcuni di essi.

Trasferimento di dati internazionali	
Perseguire una decisione di adeguatezza	Applicabile
Perseguire clausole standard di protezione dei dati	Applicabile
Perseguire norme vincolanti d'impresa	Applicabile
Perseguire codici di condotta	Programmato
Perseguire meccanismi di certificazione	Programmato
Perseguire uno strumento legalmente vincolante tra autorità o organismi pubblici	Programmato[28]

Nel primo caso, (perseguire una decisione di adeguatezza), i dati possono essere trasferiti a stati fuori dall'UE se esiste una decisione di adeguatezza della Commissione. Una decisione di adeguatezza può essere adottata se l'altro stato offre un livello di protezione dei dati adeguato allo Standard europeo29. Nel secondo caso, (perseguire clausole standard di protezione dei dati), i dati possono essere trasferiti se esiste un accordo tra l'esportatore di dati e l'importatore di dati e se i suddetti accordi contengono un certo numero di clausole standard relative alla protezione dei dati, previamente approvate dalla Commissione europea[30]. Nel terzo caso, se il trasferimento extra-territoriale avviene con lo stesso organismo (ad esempio, un trasferimento tra due filiali dello stesso gruppo internazionale), i dati possono essere trasferiti se esistono norme vincolanti d'impresa che offrano misure di protezione dei dati ai sensi dell'Articolo 47 dell'RGPD approvate dalla competente autorità di controllo per la protezione dei dati.

3.3.5 Cancellazione o distruzione dei dati

Alla fine della verifica, il titolare del trattamento deve cancellare il set di dati utilizzato per questa finalità, salvo qualora ci sia una necessità legittima di mantenerli, ad esempio, per il perfezionamento o la valutazione del sistema, o per altre finalità compatibili con quelle per cui essi furono raccolti nel rispetto delle condizioni stabilite dall'Articolo 9.2 RGPD.

L'anonimizzazione costituisce un'alternativa alla cancellazione[31]. Il consorzio ha elaborato un documento specifico in materia (https://www.datenschutzzentrum.de/uploads/projekte/IdentPseudoAnon-320-v1-0-web.pdf).

[28] A luglio 2021, queste tre opzioni di trasferimento internazionale dei dati sono state previste ma non ancora implementate.

[29] La lista dei paesi riconosciuti per tale decisione di adeguatezza può essere consultata all'indirizzo https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[30] La versione più attuale delle clausole standard può essere consultata in European Commission, 'Implementing Decision 2021/914 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council' (2021), https://doi.org/10.5040/9781782258674.

[31] Si noti che, secondo alcuni studiosi, i dati personali, e quelli biometrici in particolare, non possono essere totalmente anonimizzati. Cfr. ad esempio Justin Banda, 'Inherently Identifiable: Is It Possible to Anonymize

4 Dati biometrici nella ricerca e innovazione nelle TIC. Caso di studio

La sezione che segue presenta un'applicazione dei contenuti della sezione 3 'Tecnologia biometrica nella ricerca e innovazione nelle TIC. Orientamenti'. Il caso di studio non si riferisce a nessuna situazione reale.

Un team di sviluppatori TIC decide di disegnare un sistema di riconoscimento della mano per semplificare il processo d'identificazione dei dipendenti all'entrata dei loro luoghi di lavoro. Lo scopo dei ricercatori è proporre un approccio che salvaguardi la privacy, comprendendone la fattibilità, sviluppando la tecnologia corrispondente e pubblicando un documento con i risultati.

Il team di sviluppatori decide di porre l'attenzione su tre aspetti:

- Il sistema rispetta totalmente le norme in materia di protezione dei dati
- Il sistema è sufficientemente efficace per la sua adozione da parte delle organizzazioni
- Il sistema non è considerato dagli utenti (dipendenti) troppo invasivo

Tutti gli sviluppatori lavorano per la stessa azienda privata, Developing Inc., ubicata nello Stato europeo fittizio di Developonia. In questo scenario, Developing Inc. agisce in qualità di titolare del trattamento.

4.1 Fase di progettazione

4.1.1 Identificare gli obiettivi e stabilire se l'attività si qualifica come 'ricerca'

Gli sviluppatori stabiliscono i seguenti obiettivi:

- disegnare un approccio per semplificare l'identificazione dei dipendenti sui luoghi di lavoro
- comprenderne la fattibilità
- sviluppare e testare la tecnologia corrispondente
- pubblicare i risultati.

Con le informazioni dei risultati, gli sviluppatori procedono a valutare se il progetto è una 'ricerca scientifica'. A tal fine, essi considerano la definizione del GEPD (cfr. la sezione 2.5 ‘Attività di ricerca’) e valutano se l'attività aiuta "la conoscenza e il benessere collettivo di una società in crescita, come opposti al servizio in favore prevalentemente di uno o più interessi privati"[32]. Gli sviluppatori concludono che la risposta è positiva, in quanto l'attività non è volta semplicemente a creare una nuova tecnologia commerciale, ma a introdurre un approccio di salvaguardia della privacy per i lavoratori che sarà informativa per le applicazioni a tutela della privacy in altri contesti.

Regime giuridico: ricerca			
L'attività si qualifica come 'ricerca'?	Sì	☒	Si applica il regime speciale sulla ricerca
	No		Non si applica il regime speciale sulla ricerca

Health and Genetic Data?’, *International Association of Privacy Professionals* (blog), November 2019, https://iapp.org/news/a/inherently-identifiable-is-it-possible-to-anonymize-health-and-genetic-data/.

[32] European Data Protection Supervisor, ‘A Preliminary Opinion on Data Protection and Scientific Research’.

4.1.2 Confermare la necessità di trattamento dei dati biometrici

Per la ricerca specifica, gli sviluppatori decidono di non fare affidamento su una base di dati commerciale né di utilizzare immagini generate da un computer. Gli sviluppatori decidono di raccogliere tutti i dati (palmari) necessari a raggiungere gli obiettivi della loro ricerca direttamente da persone fisiche. Gli sviluppatori raccoglieranno le impronte palmari ed estrarranno le caratteristiche fisiche distintive (ad esempio, misurazione della mano) da queste impronte.

Per comprendere se sono coinvolti dati biometrici, gli sviluppatori adottano i criteri di cui all'articolo 4.14 dell'RGPD.

Lista di controllo dati biometrici		
☑	Si considerano come dati personali	Sì, in quanto le impronte palmari fanno riferimento a una 'persona fisica identificata'
☑	Sono basati su un trattamento tecnico specifico	Sì, in quanto le caratteristiche distintive saranno estratte dalle impronte palmari utilizzando un trattamento tecnico
☑	Appartengono alle caratteristiche fisiche, fisiologiche o comportamentali	Sì, poiché le impronte palmari fanno riferimento a caratteristiche fisiche
☑	Consentono o confermano l'identificazione univoca di una persona fisica	Sì, in quanto l'obiettivo del progetto è utilizzare le impronte palmari per identificare le persone fisiche

Regime giuridico: categorie particolari di dati personali			
L'attività coinvolge dati biometrici	Sì	☑	Si applica il regime specifico in materia di categorie particolari di dati personali
	No		Non si applica il regime specifico in materia di categorie particolari di dati personali

4.2 Fase di preparazione

4.2.1 Nomina di un Responsabile per la protezione dei dati (RPD)

Per valutare la necessità di un RPD, gli sviluppatori fanno riferimento ai criteri di cui all'Articolo 37 RGPD. Poiché essi menzionano spesso il criterio della 'larga scala', gli sviluppatori decidono di valutare prima se il trattamento possa essere considerato su larga scala, adottando l'approccio del Gruppo di lavoro dell'articolo 29

Valutazione del criterio di 'larga scala'

Numero di soggetti interessati	tra i 30 e i 50 soggetti interessati previsti
Il volume dei dati e/o il tipo di dati oggetto del trattamento	Saranno trattati dati personali (ad esempio, nome, età, ecc.) e categorie particolari di dati (impronte palmari)
La durata o permanenza dell'attività di trattamento dei dati	Gli sviluppatori prevedono che lo studio duri almeno 1 anno
Estensione geografica dell'attività di trattamento	Gli sviluppatori prevedono che lo studio avrà un'estensione locale (municipalità)

Dopo la valutazione, gli sviluppatori decidono che l'attività di trattamento può essere configurata come 'larga scala'. Anche se non è disponibile un criterio quantitativo e, quindi, i risultati della valutazione non possono essere considerati concludenti, essi decidono per il mantenimento di un approccio più cauto.

Una volta valutato il criterio di 'larga scala', gli sviluppatori procedono a valutare la necessità di un RPD.

Requisiti per la nomina di un Responsabile per la protezione dei dati (RPD)		
"Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali"	?	Non si applica
"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"	?	Non si applica (nessun monitoraggio né periodico né sistematico)
"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"	?	Si applica (trattamento di categorie particolari di dati e 'larga scala')
"Le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, […] di dati personali relativi a condanne penali e a reati di cui all'articolo 10"	?	Non si applica (nessun dato personale relativo a condanne penali o a reati)
In tutti i casi non elencati nei requisiti 1-3, "il titolare 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"	?	Non si applica (nessun diritto specifico dell'UE o di uno SM)

Poiché trova applicazione uno dei requisiti, gli sviluppatori decidono di nominare un RPD. Il titolare del trattamento (Developing Inc.) non ha un RPD nominato. Quindi, gli sviluppatori procedono alla sua nomina.

Regime giuridico: categorie particolari di dati personali			
L'attività soddisfa uno dei requisiti per un RPD	Sì	☑	La nomina di un RPD è obbligatoria
	No		La nomina di un RPD è facoltativa

4.2.2 Identificare l'approccio alla raccolta dei dati

Gli sviluppatori decidono di raccogliere dati personali direttamente dagli interessati. Essi saranno invitati presso il laboratorio di Design Inc., dove saranno prese le impronte palmari.

4.2.3 Identificare la base giuridica più adeguata

Prima di identificare la base giuridica più adeguata, gli sviluppatori devono valutare se trova applicazione una delle esenzioni al trattamento di categorie particolari di dati.

Basi giuridiche disponibili previste dall'RGPD per il trattamento dei dati biometrici		
Consenso esplicito	☑	Si applica
Lavoro, previdenza sociale e assistenza sociale	☑	Non si applica (richiede normativa aggiuntiva; non esiste all'interno dello Stato una valutazione di conformità confermata)
Interessi vitali	☑	Non si applica
Attività di associazioni e altri enti no-profit	☑	Non si applica
I dati sono stati pubblicati dall'interessato	☑	Non si applica
Reclami legali o atti giudiziari	☑	Non si applica
Interesse pubblico sostanziale	☑	Non si applica (richiede normativa aggiuntiva; non esiste all'interno dello Stato una valutazione di conformità confermata)
Salute o assistenza sanitaria	☑	Non si applica (richiede normativa aggiuntiva; non esiste all'interno dello Stato una valutazione di conformità confermata)
Interesse pubblico alla salute	☑	Non si applica (richiede normativa aggiuntiva; non esiste all'interno dello Stato una valutazione di conformità confermata)
Archivio, ricerca e statistica	☑	Non si applica (richiede normativa aggiuntiva; non esiste all'interno dello Stato una valutazione di conformità confermata)

Poiché l'unica esenzione applicabile è quella del 'consenso esplicito', gli sviluppatori decidono anche di adottare il 'consenso' come base giuridica per il trattamento dei dati.

Con riferimento alla base giuridica e considerando che la raccolta avverrà direttamente dall'interessato (cfr. 4.2.2 ‘Identificare l'approccio alla raccolta dei dati’), gli sviluppatori preparano le informazioni che saranno fornite agli interessati nel modulo di consenso.

Informazioni da fornire agli interessati ai fini della raccolta	
I dati personali e di contatto del titolare del trattamento	Developing Inc. (titolare del trattamento) Developers Street, 99, 21010, Developonia +00 – 0123456, info@developinginc.com
Se del caso, l'identità e i dati di contatto del rappresentante del titolare del trattamento	Non applicabile
I dati di contatto del Responsabile per la protezione dei dati	John Doe (RPD di Developing Inc.) Developers Street, 99, 21010 Developonia +00 – 0123457, dpo@developinginc.com
Le finalità del trattamento	Ricerca di un approccio per l'uso di impronte palmari per identificare i lavoratori sul luogo di lavoro, svilupparne e testarne la tecnologia e pubblicare i relativi risultati
Le categorie di dati interessate	Nome, cognome, data di nascita, indirizzo, numero di telefono, email, impronte palmari
La base giuridica per il trattamento	Consenso esplicito
Se del caso, gli interessi legittimi perseguiti dal titolare del trattamento o da terzi	Non applicabile (nessun interesse legittimo perseguito)
Destinatari o categorie di destinatari dei dati personali	Developing Inc. (titolare del trattamento)
L'intenzione del titolare del trattamento di trasferire i dati personali a un paese terzo o un'organizzazione internazionale	Non applicabile (nessun trasferimento)
In caso di trasferimento, l'esistenza o meno di una decisione di adeguatezza o un riferimento alle garanzie e alle misure attraverso cui ottenere una copia dei dati	Non applicabile (nessun trasferimento)
Il periodo di conservazione dei dati personali o, qualora ciò non sia possibile, i criteri utilizzati per definire detto periodo	Durata della ricerca (previsto l'inizio in data 01/01/2022 e per almeno 1 anno), fino allo sviluppo e verifica del sistema
L'esistenza del diritto di accesso, rettifica o cancellazione, limitazione di trattamento, opposizione e portabilità	Gli interessati possono esercitare i loro diritti ai sensi degli Articoli 12-22 RGPD

In caso di 'consenso esplicito' come base giuridica del trattamento, l'esistenza del diritto alla revoca del consenso in qualsiasi momento e senza alcuna conseguenza negativa	I soggetti interessati possono revocare il loro consenso. Se ciò accade, Developing Inc identificherà nuovi interessati
Il diritto a presentare un reclamo dinanzi all'autorità di controllo	I reclami possono essere presentati dinanzi all'RPD di Developonia. Saranno forniti i dati di contatto.
Se la fornitura dei dati deriva da un requisito normativo o contrattuale, o necessario per la conclusione di un contratto, e se l'interessato è obbligato a fornire i dati e le conseguenze della mancata fornitura dei suddetti dati	La fornitura non è un requisito normativo o contrattuale
L'esistenza di un processo decisionale automatizzato, inclusa la profilazione	Il trattamento non include un processo decisionale automatizzato
In caso di processo decisionale automatizzato, le informazioni relative alla logica utilizzata, l'importanza del trattamento e le relative possibili conseguenze per l'interessato	Non applicabile

4.2.4 Creare un deposito per la documentazione giustificativa

L'RPD di Developing Inc. crea un deposito in cui viene conservata la documentazione relativa al trattamento. I documenti sono conservati a livello locale nei server di Developing Inc. La struttura di memorizzazione di Developing Inc. è ridondante per una protezione della continuità operativa e i contenuti dei server sono periodicamente soggetti a back up.

Gli sviluppatori identificano la seguente documentazione obbligatoria:

Documentazione: lista di controllo		
Politica in materia di protezione dei dati personali	☐	Si applica
Informativa sulla privacy	☐	Si applica
Politica di conservazione dei dati	☐	Si applica
Schema di conservazione dei dati	☐	Si applica
Registro delle attività di trattamento (se del caso)	☐	Si applica (vedi di seguito)
Modulo per il consenso (se del caso)	☐	Si applica (consenso come base giuridica)
Accordo di trattamento dei dati con i fornitori	☐	Non si applica (nessun fornitore con accesso ai dati personali)

Valutazione d'impatto della protezione dei dati	?	Si applica (vedi sezione 4.2.5)
Clausole contrattuali per il trasferimento di dati personali (se applicabile)	?	Non si applica (nessun trasferimento)
Nomina di un rappresentante UE (se del caso)	?	Non si applica (Developing Inc. ha sede nell'Unione europea)
Procedura di risposta e notifica della violazione dei dati	?	Si applica
Registro della violazione dei dati	?	Non si applica (non si è verificata alcuna violazione)
Modulo di notifica della violazione dei dati all'autorità di controllo	?	Non si applica (non si è verificata alcuna violazione)
Modulo di notifica della violazione dei dati agli interessati	?	Non si applica (non si è verificata alcuna violazione)

In questo scenario, Design Inc. ha un registro delle attività di trattamento. Infatti, anche se si tratta di una piccola organizzazione con meno di 250 dipendenti, essa realizza regolarmente un trattamento dei dati sui suoi dipendenti (ad esempio, gestione del salario, organizzazione di ritiri aziendali, ecc.). Developing Inc, non ha elaborato un modello proprietario per il registro delle attività di trattamento e ha adottato quello previsto dall'Autorità di controllo francese[33].

4.2.5 Verificare la necessità di una DPIA

L'RGPD richiede una DPIA quando il trattamento dei dati potrebbe prevedibilmente provocare un elevato rischio per i diritti e le libertà delle persone fisiche. Gli sviluppatori, incerti sul se il trattamento implichi i suddetti rischi, decide di valutare il trattamento adottando gli anzidetti nove criteri suggeriti dal Gruppo di lavoro dell'Articolo 29.

Criteri per il trattamento ad alto rischio		
Valutazione o punteggio (ad esempio, profilazione)	?	Non si applica
Processo decisionale automatizzato con efficacia giuridica o simile	?	Non si applica
Monitoraggio sistematico	?	Non si applica
Dati sensibili o dati altamente confidenziali	?	Si applica (vedi di seguito)
Dati trattati su larga scala	?	Si applica (vedi sezione

[33] Il modello può essere consultato su Commision Nationale Informatique & Libertés, 'Record of Processing Activities', August 2019, https://www.cnil.fr/en/record-processing-activities.

		4.2.1)
Corrispondenza o combinazione di set di dati (oltre le aspettative ragionevoli dell'interessato)	☒	Non si applica
Dati relativi a soggetti vulnerabili	☒	Non si applica
Uso innovativo o applicazione di nuove tecnologie o soluzioni organizzative	☒	Non si applica (vedi di seguito)
Quando il trattamento in sé impedisce agli interessati di esercitare un diritto o utilizzare un servizio o contratto	☒	Non si applica

La valutazione rivela che il trattamento soddisfa almeno due criteri. Il primo riguarda il tipo di dati personali che saranno oggetto di trattamento. Poiché, nel contesto di quest'attività di ricerca, le impronte palmari sono state stabilite come dati biometrici, gli sviluppatori concludono che questi dati soddisfano il criterio di essere di natura sensibile e altamente personale. Il secondo criterio riguarda la scala del trattamento. Gli sviluppatori hanno già stabilito che il trattamento si qualifica come su 'larga scala' (cfr. 4.2.1 'Nomina di un responsabile della protezione dei dati (RPD)').

Gli sviluppatori si interrogano anche sul criterio di un 'Uso innovativo o applicazione di nuove soluzioni tecniche o organizzative'. Esso non si applica in quanto l'attività si concentra sulla ricerca e l'applicazione concreta a un contesto organizzativo non è prevista nell'attività attuale.

Valutazione d'impatto della protezione dei dati			
Il trattamento è ad 'alto rischio'	Sì	☒	Una valutazione d'impatto in materia di protezione dei dati è obbligatoria
	No		Una valutazione d'impatto in materia di protezione dei dati è facoltativa

4.2.6 Eseguire una DPIA

Poiché l'autorità di controllo di Developonia non ha elaborato una guida su come realizzare una DPIA, e seguendo il consiglio dell'RPD, gli sviluppatori realizzano la DPIA utilizzando la guida del Gruppo di lavoro dell'Articolo 29, come avallato dall'EDPB (Comitato europeo per la protezione dei dati), e il modello fornito dall'Autorità di controllo francese[34]. Il risultato della DPIA mostra che tutti i rischi per i diritti e le libertà degli interessati sono mitigati a un livello accettabile, che non è mai alto per tutti i rischi identificati.

Il risultato della DPIA viene conservato nel deposito per la documentazione di sostegno.

[34] Commision Nationale Informatique & Libertés, 'Privacy Impact Assessment (PIA). Templates'.

4.2.7 Implementare misure di mitigazione del rischio

Dopo l'esecuzione della DPIA, gli sviluppatori stabiliscono che le misure tecniche e di sicurezza sono adeguate alla protezione dei diritti e le libertà dell'interessato e possono essere considerate misure adeguate ai sensi dell'articolo 89 RGPD.

4.3 Fase di esecuzione

4.3.1 Trattamento di dati biometrici

Il team di ricercatori, una volta distribuite tutte le informazioni all'interessato e ottenuto il loro consenso esplicito, procedono alla raccolta dei dati biometrici dei soggetti. I ricercatori ricevono impressioni dai partecipanti e le trasmettono a un sistema di intelligenza artificiale per estrarre le caratteristiche biometriche (ad esempio, forme libere, creste e valli, ecc.). Tutti i componenti del sistema di intelligenza artificiale, ivi incluso l'algoritmo sottostante, sono sviluppati e mantenuti in loco dai ricercatori e nessun altro soggetto viene coinvolto o accede ai dati trattati dal sistema di intelligenza artificiale. I componenti di intelligenza artificiale del sistema sono sviluppati seguendo i passi descritti nel documento 'Orientamenti su questioni etiche e legali relative all'intelligenza artificiale nella ricerca e innovazione nelle TIC'.

4.3.2 Sviluppo di un'interfaccia utente di un sistema biometrico

Il team di ricerca decide quale interazione con il sistema biometrico avverrà mediante un chiosco dedicato. Durante la ricerca, i chioschi saranno collocati nel laboratorio degli sviluppatori. I chioschi raccoglieranno i dati e li memorizzeranno a livello locale, e gli utenti interagiranno con i chioschi in presenza del team di ricerca. L'uso dei chioschi nell'ambiente controllato del laboratorio informerà gli sviluppatori della fattibilità della tecnologia e funzioneranno come test pilota per sviluppi futuri sui luoghi di lavoro attuali.

Uno degli obiettivi della ricerca è semplificare l'autenticazione dei lavoratori. Per raggiungere quest'obiettivo, i ricercatori tendono a rendere il processo di autenticazione più veloce, aumentandone la semplicità d'uso e, quindi, riducendo al minimo il tempo impiegato da ciascun utente nel chiosco. Per questa ragione, essi decidono di dividere le funzionalità in due diversi tipi di chiosco: uno dedicato all'autenticazione (chiosco di autenticazione), e l'altro dedicato ad altre funzionalità, come l'accesso alle informazioni e l'aggiornamento dei dati personali (chiosco extra). In questo modo, i lavoratori che devono realizzare azioni diverse dall'autenticazione non rallenteranno l'autenticazione degli altri lavoratori.

Il chiosco di autenticazione ha due componenti principali: uno scanner per la mano e un monitor. Se l'autenticazione riesce, viene visualizzata una spunta verde, la porta si apre e il lavoratore può procedere. L'autenticazione non viene registrata (in quanto l'obiettivo non è misurare le ore lavorative dei soggetti) e il monitor non mostra alcuna informazione sulla persona.

Il chiosco extra ha gli stessi elementi del chiosco di autenticazione, con la differenza che il monitor è tattile per garantire agli utenti di poter interagire con il sistema. Inoltre, il chiosco extra è inscatolato per evitare lo shoulder surfing. L'utente può attivare il chiosco extra semplicemente effettuando la scansione delle sue mani. Quando ciò accade, il monitor mostra un menù con tre opzioni:

- Mostrare le informazioni sul trattamento dei dati: quest'opzione apre una finestra di pop-up in cui sono fornite tutte le informazioni elencate in 4.2.3 'Identifica la base giuridica più adeguata';

- Accedere e rettificare i dati personali: quest'opzione apre una finestra di pop-up in cui sono visualizzati tutti i dati personali di un soggetto, e in cui l'utente può modificare i suddetti dati, ivi inclusa la registrazione di nuove impronte palmari;
- Esercitare il diritto di rettifica, limitazione, portabilità dei dati o opposizione: quest'opzione è attualmente disattivata nel chiosco di prototipo della ricerca. Se un utente la seleziona, i membri del team di ricerca riceveranno un avviso sui loro dispositivi mobili e gli sarà richiesto di verificare con gli interessati se intendono esercitare uno dei loro diritti.

4.3.3 Verifica del Sistema biometrico

Una volta sviluppato il sistema, i ricercatori possono testarlo e verificarne le prestazioni (ad esempio, tasso di errore, velocità di autenticazione, consumo di energia, ecc.). A tal fine, essi riuniscono gli interessati per simulare l'uso del sistema.

Poiché la verifica del sistema è una delle attività principali della ricerca, in quanto gli interessati hanno già fornito il loro consenso esplicito alla verifica, e visto che non sono trattati ulteriori dati personali, il team di ricerca conclude che i rischi per i diritti e delle libertà degli interessati sono adeguatamente affrontati e procede con la verifica.

4.3.4 Diffusione dei risultati

Una volta completata l'attività di verifica e raccolti tutti i dati per la verifica, il team di ricerca può finalmente elaborare un progetto in cui sia descritta la tecnologia e siano presentati i risultati. Fiduciosi che il sistema svolgerà le prestazioni in modo coerente, essi decidono di rendere la tecnologia open source per garantire che altri ricercatori possano realizzare le loro verifiche e convalidarne i risultati. Seguendo questa decisione, i ricercatori decidono di cancellare tutti i dati personali dei soggetti che hanno preso parte all'attività di ricerca.

4.3.5 Cancellazione o distruzione dei dati

Tutti i dati personali sono stati totalmente cancellati.

CHECKLISTS

Le seguenti indicazioni non sono state oggetto di validazione esterna. Nonostante ciò, PANELFIT le reputa adeguate a perseguire gli obiettivi espressi dalle Linee Guida.

Fase di design

Passaggio	Sezione di riferimento
☐ Identificare gli obiettivi dell'attività	3.1.1
☐ Valutare se l'attività costituisca una "ricerca"	3.1.1
☐ Identificare il ruolo dei ricercatori e delle altre parti coinvolte	3.1.1
☐ Confermare che il trattamento di dati biometrici sia necessario per il raggiungimento degli obiettivi dell'attività	3.1.2

Fase di preparazione

Passaggio	Sezione di riferimento
☐ Valutare se almeno uno dei requisiti per il RPD sia applicabile	3.2.1
☐ In caso di autorità pubblica, controllare che il RPD possa essere nominato da un'altra autorità pubblica	3.2.1
☐ Pubblicare i contatti del RPD	3.2.1
☐ Identificare se i dati verranno raccolti presso il soggetto interessato	3.2.2
☐ Valutare se sia applicabile una esenzione all'obbligo di informare il soggetto interessato	3.2.2
☐ Registrare e archiviare i risultati della valutazione di applicabilità di esenzione all'obbligo di informare	3.2.2
☐ Definire un processo interno per garantire l'accuratezza dei dati trattati	3.2.2
☐ Identificare se almeno una delle eccezioni al divieto di trattamento per categorie speciali di dati persoali sia applicabile	3.2.3

☐ In caso di eccezione che richieda ulteriori strumenti normativi, verificarne l'esistenza o valutare una diversa eccezione	3.2.3
☐ In caso di conferma di eccezione, identificare una base legale per il trattamento coerente con l'articolo 6 RGPD	3.2.3
☐ Se la base legale identificate è il consenso, assicurarsi che si tratti di consenso esplicito	3.2.3
☐ Registrare e archiviare i moduli di racconta del consenso esplicito	3.2.3 / 3.2.4
☐ Creare un archivio che contenga almeno il set minimo di documenti richiesto dal RGPD	3.2.4
☐ Valutare se il trattamento non introduca rischi elevati per i diritti e le libertà degli interessati	3.2.5
☐ Registrare e archiviare i risultati della valutazione preliminare di rischio	3.2.5
☐ Se il trattamento introduce rischi elevati per i diritti e le libertà degli interessati, eseguire una valutazione di impatto	3.2.6
☐ Se i rischi non sono mitigati dalle misure previste, implementare misure addizionali adeguate alla mitigazione	3.2.7
☐ Se i rischi non sono mitigati e non è possibile imlementare misure addizionali, consultarsi con l'autorità garante	3.2.7
☐ Registrare e archiviare i risultati della valutazione di impatto	3.2.4 / 3.2.6 / 3.2.7

Fase di esecuzione

Passaggio	**Sezione di riferimento**
☐ Trattare i dati personali applicando le misure e precauazione approntate durante la fase di preparazione	3.3.1
☐ In caso di sviluppo di sistemi ICT, assicurarsi che gli interessati possano accedere ai dati tramite interfacce appropriate	3.3.2
☐ In caso di sviluppo di sistemi ICT, valutare i rischi per gli interessati in relazione ad ogni funzionalità del sistema ICT	3.3.2
☐ Registrare e archiviare i risultati della valutazione dei rischi connessi alle funzionalità del sistema ICT	3.2.4 / 3.3.2
☐ Se i rischi non risultano mitigabili, consultarsi con l'autorità garante o interrompere l'implementazione delle funzionalità	3.3.2
☐ Prevedere l'utilizzo del sistema, attraverso specifici casi d'uso, anche da parte di soggetti vulnerabili	3.3.2

☐ In caso di verifica del sistema ICT, valutare se la verifica si configuri come un trattamento differente rispetto allo sviluppo	3.3.3
☐ Registrare e archiviare i risultati della valutazione delle verifica come diverso trattamento rispetto allo sviluppo	3.2.4 / 3.3.3
☐ Se la verifica si configura come un diverso trattamento, valutare la compatibilità delle finalità	3.3.3
☐ Regsitrare e archiviare i risultati della valutazione di compativilità delle finalità	3.2.4 / 3.3.3
☐ Valutare se la disseminazione dei risultati debba coinvolgere anche le categorie speciali di dati personali trattati	3.3.4
☐ Identificare se almeno una delle eccezioni al divieto di trattamento per categorie speciali di dati persoali sia applicabile	3.3.4
☐ Identificare la base legale più appropriata prima di procedere alla disseminazione	3.3.4
☐ Nominare le parti riceventi i risultati come Responsabile del trattamento	3.3.4
☐ Informare i soggetti interessati del trasferimento	3.3.4
☐ Valutare se il trasferimento dati sia internazionale	3.3.4
☐ In caso di trasferimento internazione non soggetto a deroghe, itendificare uno strumento adeguato per il trasferimento	3.3.4
☐ Valutare liceità del mantenimento dei dati personali	3.3.5
☐ Regsitrare e archiviare i risultati della valutazione di liceità sul mantenimento dei dati personali	3.2.4 / 3.3.5
☐ Qualora sia illecito mantenere i dati, procedere alla cancellazione o anonimizzazione	3.3.5