PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Codice di condotta sulla protezione dei dati per la ricerca e l'innovazione responsabile

Questo progetto ha ricevuto un finanziamento dal programma di ricerca e innovazione Horizon 2020 dell'Unione europea nell'ambito dell'accordo di sovvenzione n. 788039. Questo documento riflette solo il punto di vista dell'autore e l'Agenzia non è responsabile dell'uso che può essere fatto delle informazioni in esso contenute.

Informazioni sul progetto

Titolo del progetto	Approcci partecipativi a un nuovo quadro etico e legale per le TIC
Acronimo del progetto	PANELFIT
Numero della convenzione di sovvenzione	788039
Coordinatore del progetto	UPV/EHU

Informazioni sul documento

Numero del deliverable	D5.4
Titolo del documento	Codice di condotta sulla protezione dei dati per una ricerca e un'innovazione responsabili
Versione del documento	Versione 4.0
Data del documento	2021-08-04
Piombo del documento	ICM-CSIC | < soacha@icm.csic.es>
Licenza di copyright	(Creative Commons Attribution International4.0)
Livello di diffusione	PU (pubblico)

Partner del progetto coinvolti nel documento

N°	Nome dell'organizzazione partecipante	Acronimo
1	Institut de Ciències del Mar (Consejo Superior de Investigaciones Científicas)	ICM-CSIC
2	Università del País Vasco / Euskal Herriko Unibertsitatea	UPV/EHU
3	Rete europea dei comitati etici per la ricerca	EUREC
4	Unabhängiges Landeszentrum für Datenschutz AöR	ULD
5	Oesterreichische Akademie der Wissenschaften	OEAW
6	Fondazione Teknologiradet	DBT

Storia del documento

Stato	Versione	Data	Autore/i	Recensito da
Bozza	v0.5	2020-10-30	Pranesh Prakash (ICM-CSIC)	Karen Soacha (ICM-CSIC), Jaume Piera (ICM-CSIC)
Bozza	v1.0	2020-11-03	Pranesh Prakash	Julia Maria Mönig (EUREC), Johann Cas (OEAW), Bud Bruegger (ULD), Harald Zwingelberg (ULD), Bjørn Bested (DBT)
Bozza	v2.0	2020-12-06	Pranesh Prakash	Iñigo de Miguel Beriain (UPV/EHU), Karen Soacha
Bozza	v3.0	2021-01-23	Pranesh Prakash	Karen Soacha
Finale	v4.0	2021-08-02	Pranesh Prakash	Karen Soacha, MLE (parti interessate, ricercatori), Iñigo de Miguel Beriain

.

1 Preambolo

Questo codice di condotta sulla protezione dei dati per una ricerca e un'innovazione responsabili (CCDP) è un contributo del progetto PANELFIT alla comunità di ricerca.

PANELFIT (Participatory Approaches to a New Ethical and Legal Framework for ICT) è un progetto finanziato da Horizon 2020 che ha prodotto standard operativi e linee guida pratiche per affrontare alcune delle questioni etiche e legali poste dalle tecnologie ICT. Il progetto PANELFIT cerca quindi di fornire chiarezza e guida rispetto alle questioni all'intersezione tra ricerca responsabile e innovazione, [1]etica e protezione dei dati.

Il CCDP mira a fornire un insieme di regole di condotta di facile comprensione che coprono i principi principali previsti dal Regolamento generale sulla protezione dei dati dell'UE (GDPR), così come una serie di pratiche auspicabili, specificamente adattate alla comunità di ricerca.[2] Esistono molteplici codici di condotta relativi alla ricerca responsabile e all'innovazione. Tuttavia, questi codici di condotta esistenti non cercano di fornire una guida sui principi di protezione dei dati, che è una lacuna che questo CCDP cerca di colmare. Il CCDP cerca di essere un testo introduttivo ai principi di protezione dei dati, e non cerca di coprire tutti gli aspetti del GDPR che possono essere di interesse per i ricercatori. Così, per esempio, il CCDP non cerca di coprire tutti gli obblighi che un ricercatore può avere in base alle leggi sulla protezione dei dati, né tutti i diritti delle persone i cui dati personali sono utilizzati dai ricercatori, o i requisiti legali relativi alla condivisione dei dati personali con i colleghi ricercatori al di fuori dell'UE, le leggi nazionali sulla protezione dei dati, e così via. Il progetto PANELFIT ha anche creato le "Linee guida sulla protezione dei dati, questioni etiche e legali nella ricerca e nell'innovazione ICT", che mira ad essere molto più completo a questo proposito.

1.1. RRI e protezione dei dati

L'attività di ricerca, sia che si tratti di impegnarsi nella ricerca o nella diffusione della ricerca, spesso coinvolge i dati personali di altre persone.[3] Quindi, l'etica dei dati è una componente necessaria della ricerca e dell'innovazione responsabile, e questo include la protezione dei dati personali. Nell'UE, la protezione dei dati personali è un diritto fondamentale ai sensi della Carta dei diritti fondamentali dell'Unione europea, e il regolamento generale sulla protezione dei dati fornisce una guida normativa concreta su questo diritto.

Ogni volta che i ricercatori trattano dati personali, sono tenuti a rispettare la legge sulla protezione dei dati e dovrebbero sforzarsi di seguire le migliori pratiche di protezione dei dati.

Il CCDP cerca di aiutare i ricercatori a capire i principi di base che sono alla base della protezione dei dati

[1] La ricerca e l'innovazione responsabile (RRI) è una componente importante del programma "Scienza con e per la società" di Horizon 2020 (H2020) dell'UE. "La RRI è il processo continuo di allineare la ricerca e l'innovazione ai valori, ai bisogni e alle aspettative della società."("Dichiarazione di Roma sulla ricerca e l'innovazione responsabile in Europa"). La Commissione europea nota che "l'RRI è un approccio inclusivo alla ricerca e all'innovazione (R&I), per assicurare che gli attori sociali lavorino insieme durante l'intero processo di ricerca e innovazione... In termini generali, l'RRI implica l'anticipazione e la valutazione delle potenziali implicazioni e delle aspettative della società in relazione alla ricerca e all'innovazione." (Commissione europea, "La scienza con e per la società")

[2] Anche se non esiste una definizione unica e universalmente accettata di ricerca, è utile tenere a mente le parole del Garante europeo della protezione dei dati in un recente rapporto: "Definizioni rispettabili di ricerca tendono a sottolineare l'attività sistematica, compresa la raccolta e l'analisi dei dati, che aumenta lo stock di comprensione e conoscenza e la loro applicazione. La Commissione europea ha definito gli obiettivi della ricerca e delle politiche dell'UE come "l'apertura del processo di innovazione a persone con esperienza in campi diversi da quello accademico e scientifico", "la diffusione della conoscenza non appena è disponibile utilizzando la tecnologia digitale e collaborativa" e "la promozione della cooperazione internazionale nella comunità di ricerca"." (Garante europeo della protezione dei dati, "Un parere preliminare sulla protezione dei dati e la ricerca scientifica", 9-10)

[3] I dati personali sono qualsiasi informazione relativa a una persona fisica identificata o identificabile. Il termine è una categoria molto ampia e comprende il nome di una persona, il numero di identificazione, i dati di localizzazione, un identificatore online o fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di quella persona.

in Europa e per dotarli delle conoscenze su come applicare praticamente quei principi come parte della ricerca e dell'innovazione responsabile. La comprensione della ricerca sotto il GDPR è espansiva, coprendo le attività per fornire conoscenze che possono "migliorare la qualità della vita per un certo numero di persone e migliorare l'efficienza dei servizi sociali", e include "lo sviluppo tecnologico, la ricerca fondamentale e applicata e la ricerca finanziata privatamente e gli studi condotti nel pubblico interesse nel settore della salute pubblica"[4]

[4] Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, considerando 159.

2 Principi di protezione dei dati

La protezione dei dati personali secondo il GDPR è costruita intorno a una serie di principi:

- Legalità, equità, trasparenza[1]
- Limitazione dello scopo[2]
- Minimizzazione dei dati[3]
- Precisione[4]
- Limitazione dello stoccaggio[5]
- Integrità e riservatezza[6]
- Responsabilità[7]

2.1. Legalità, equità e trasparenza

Per rispettare i requisiti del principio di legalità, trasparenza ed equità, i ricercatori devono:

- Determinare gli scopi della raccolta e dell'uso dei dati personali.
- Assicurarsi che identifichino un motivo valido (almeno uno dei sei motivi ("basi legali") previsti dal GDPR) per raccogliere e utilizzare i dati.
- Assicurarsi che tutto ciò che fanno con i dati sia legittimo e in conformità con tutte le leggi applicabili e le linee guida etiche, comprese quelle relative agli studi clinici, alla proprietà intellettuale, ai diritti umani, al contratto, ecc.
- Determinare le aspettative degli individui su come i ricercatori potrebbero usare i loro dati e cosa considererebbero ragionevole.
- Determinare i danni potenziali per gli individui i cui dati vengono utilizzati.
- Raccogliere e utilizzare i dati in modo aperto e trasparente.
- Informare gli individui in un linguaggio chiaro su chi sta raccogliendo o ottenendo i dati, in base a quale base legale vengono raccolti/ottenuti, perché vengono raccolti/ottenuti, per quanto tempo verranno conservati, come verranno usati e da chi, e quali diritti hanno.
- Utilizzare i dati in modo equo, in linea con le aspettative delle persone e in modo da non causare loro un danno ingiustificato o ingiusto.
- Verificare se i dati che devono essere raccolti riguardano "categorie speciali di dati personali" (dati sensibili, definiti nel GDPR), nel qual caso una delle basi legittime specifiche elencate nell'art. 9(2) del GDPR deve essere soddisfatta. come avere il consenso esplicito dell'interessato, o essere sulla base di una legge che consente tale raccolta per "scopi di archiviazione nel pubblico interesse, scopi di ricerca scientifica o storica o scopi statistici."

- Verificare se i dati che devono essere raccolti si riferiscono a "condanne penali e reati", nel qual caso si applicano leggi speciali.

---

1 Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, art. 5(1)(a).

2 Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, art. 5(1)(b).

3 Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, art. 5(1)(c).

4 Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, art. 5(1)(d).

5 Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, art. 5(1)(e).

6 Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, art. 5(1)(f).

7 Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, art. 5(2).

Sfondo

Secondo la legge europea, tutti i trattamenti di dati personali devono essere fatti per uno scopo legittimo e con uno scopo legittimo. Mentre gli altri principi forniscono limitazioni su come i dati personali possono essere trattati, questo principio pone restrizioni sugli scopi per cui i dati personali possono essere trattati.

Base legale

Il GDPR stabilisce sei basi[8] giuridiche per le quali i dati personali possono essere trattati legittimamente. Quindi, lo scopo del trattamento dei dati personali deve rientrare in almeno una delle sei categorie:

- Consenso dell'individuo
- Esecuzione di un contratto
- Conformità con un obbligo legale, come autorizzato dalla legge
- Necessario per proteggere gli interessi vitali di una persona
- Necessario per compiti ufficiali o di interesse pubblico legalmente autorizzati, come autorizzato dalla legge
- Interessi legittimi

Va notato che, a differenza delle istituzioni private, le autorità pubbliche non sono autorizzate a utilizzare il "legittimo interesse" come scopo, a meno che il trattamento non esuli dall'ambito dei compiti dell'autorità pubblica. Inoltre, "necessità" e "interesse pubblico" implicano un "bisogno sociale pressante", in contrapposizione a vantaggi prevalentemente privati o commerciali.[9]

Se il "consenso" è usato come base, allora è importante che lo scopo sia specificato in modo chiaro ed esplicito, e che riveli, spieghi o esprima in una forma facilmente comprensibile il motivo per cui i dati vengono raccolti e trattati. Il consenso stesso deve essere dato liberamente, specifico, informato e non ambiguo, e l'individuo ha il diritto di ritirare il consenso in qualsiasi momento.

Il GDPR riconosce che "spesso non è possibile identificare completamente lo scopo del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, gli interessati dovrebbero essere autorizzati a dare il loro consenso a determinate aree di ricerca scientifica, se in linea con gli standard etici riconosciuti per la ricerca scientifica. Gli interessati dovrebbero avere l'opportunità di dare il loro consenso solo a certe aree di ricerca o parti di progetti di ricerca nella misura consentita dallo scopo previsto."[10]

Il Garante europeo della protezione dei dati (GEPD) osserva che, "Il consenso specifico normalmente richiesto dal GDPR può quindi diventare meno appropriato nel caso di dati raccolti e dedotti e soprattutto nel caso di categorie speciali di dati su cui si basa molta ricerca scientifica", e quindi, "quando gli scopi della ricerca non possono essere completamente specificati, ci si aspetta che un controllore faccia di più per garantire l'essenza dei diritti dell'interessato a un valido consenso, anche attraverso la massima trasparenza possibile e altre garanzie."[11]

Equità

Inoltre, il modo in cui il trattamento viene fatto deve essere equo e trasparente. Anche se il trattamento intrapreso ha una base legittima, potrebbe comunque essere ingiusto, e quindi in violazione di questo principio. La correttezza è un concetto ampio: richiede che i ricercatori trattino i dati personali solo in modi che le persone si aspetterebbero ragionevolmente, e che non facciano nulla che possa danneggiare gli interessati.

Trasparenza

La trasparenza richiede che le persone siano informate sugli scopi previsti per la raccolta e l'uso dei dati personali; i motivi legali per il trattamento, ecc. Questo è necessario sia che ci sia un trattamento diretto

---

8 Regolamento generale sulla protezione dei dati, Regolamento UE 2016/679, art. 6.

9 Garante europeo della protezione dei dati, "A Preliminary Opinion on Data Protection and Scientific Research",23 .

10 Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, considerando 33.

11 Garante europeo della protezione dei dati, "A Preliminary Opinion on Data Protection and Scientific Research",19 .

raccolta di dati personali dagli interessati (sia che vengano forniti consapevolmente dall'individuo, sia che vengano raccolti attraverso l'osservazione dell'individuo), o ottenimento di dati personali da qualche altra fonte (come un terzo a cui sono stati affidati i dati, fonti pubbliche, broker di dati, o da altri individui). [12] Le informazioni che dovrebbero essere fornite, come minimo, includono:[13]

- chi è la tua azienda/organizzazione (i tuoi dati di contatto e quelli del tuo DPO, se presente);
- perché la vostra azienda/organizzazione userà i loro dati personali (scopi);
- le categorie di dati personali interessate;
- la giustificazione legale del trattamento dei loro dati;
- per quanto tempo i dati saranno conservati;
- chi altro potrebbe riceverlo;
- se i loro dati personali saranno trasferiti a un destinatario al di fuori dell'UE;
- che hanno diritto a una copia dei dati (diritto di accesso ai dati personali) e altri diritti di base nel campo della protezione dei dati (vedere la lista completa dei diritti);
- il loro diritto di presentare un reclamo a un'autorità di protezione dei dati (DPA);
- il loro diritto di ritirare il consenso in qualsiasi momento;
- se del caso, l'esistenza di un processo decisionale automatizzato e la relativa logica, comprese le conseguenze.

Se avete ottenuto dati personali da una fonte diversa dalle persone interessate, dovete informarle entro un periodo ragionevole, e al massimo entro un mese dall'accesso ai loro dati personali.

Gli obblighi di trasparenza non si applicano se e nella misura in cui la persona interessata dispone già delle informazioni.[14] Per i dati personali raccolti da una fonte terza, ci sono tre ulteriori situazioni in cui gli obblighi di trasparenza non si applicano:[15]

- Quando è impossibile (in particolare per l'archiviazione, la ricerca scientifica/storica o per scopi statistici);
- Dove comporterebbe uno sforzo sproporzionato (in particolare per l'archiviazione, la ricerca scientifica/storica o scopi statistici); o
- Quando fornire le informazioni richieste dall'articolo 14.1renderebbe impossibile o comprometterebbe seriamente il raggiungimento degli obiettivi del trattamento.

Categorie speciali di dati personali / Dati sensibili

Le categorie speciali di dati personali, o dati sensibili, [16]sono dati che rivelano l'identità di una persona:

- origine razziale o etnica,
- opinioni politiche,
- credenze religiose o filosofiche,

- l'appartenenza ad

un sindacato, o sono:

- dati genetici,
- dati biometrici allo scopo di identificare in modo univoco una persona fisica,
- dati relativi alla salute, o
- dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica.

Tali dati sensibili non possono essere raccolti a meno che la raccolta rientri in uno dei dieci motivi legittimi previsti dal GDPR,[17] che include il consenso esplicito, così come quando è necessario per l'archiviazione,

---

12 Regolamento generale sulla protezione dei dati, Regolamento UE 2016/679, art. 12(1), (5), (7), Art. 13, Art. 14, Considerando 58-6239,.

13 Commissione europea, "Quali informazioni devono essere date alle persone i cui dati sono raccolti?

14 Regolamento generale sulla protezione dei dati, Regolamento UE 2016/679, Art. 13(4), Art. 14(5)(a).

15 Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, art. 14(5)(b).

16 Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, art. 9(1), considerando 51-56.

17 Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, art. 9(2)(a).

ricerca scientifica o storica, e le statistiche con le opportune garanzie che sono legalmente richieste dal GDPR e sono previste da una legge appropriata.[18] Date le differenze nazionali nelle leggi che regolano i dati sensibili, e in particolare i dati genetici, biometrici o sanitari, i [19]ricercatori dovrebbero consultare il responsabile della protezione dei dati della loro istituzione, o la loro autorità locale per la protezione dei dati per saperne di più su ciò che è ammissibile e ciò che non lo è.

Inoltre, mentre i dati relativi a condanne penali e reati non sono classificati come "sensibili" sotto il GDPR, il regolamento richiede che tutti gli usi di tali dati da parte dei ricercatori devono essere ulteriormente autorizzati da una legge nazionale o dell'UE, e seguire le garanzie previste da tale legge.[20]

2.2. Limitazione dello scopo

Per rispettare il principio di limitazione dello scopo, i ricercatori dovrebbero:

- Documentare in termini chiari e specifici gli scopi della raccolta e dell'uso dei dati personali.
- Fornire agli individui informazioni sugli scopi della raccolta e dell'uso dei loro dati.
- Limitare il trattamento dei dati personali agli scopi specificati o a scopi compatibili con gli scopi specificati.
- Assicurarsi di informare l'individuo in quelle situazioni in cui il motivo originale per l'uso dei dati personali era qualcosa di diverso dal consenso o da un requisito legale, e ora quei dati vengono messi a un nuovo uso compatibile. Questo dovrebbe essere fatto ragionevolmente prima che il nuovo uso dei dati personali abbia luogo, in modo da consentire all'individuo di opporsi al trattamento.
- Assicurarsi che richiedano un nuovo consenso in quelle situazioni in cui il motivo originale per l'uso dei dati personali era il consenso, e ora quei dati vengono messi a qualsiasi altro uso (indipendentemente dal fatto che il nuovo uso sia un uso "compatibile").
- Assicurarsi di avere il consenso o un chiaro obbligo/funzione previsto nell'interesse pubblico in una legge, se vogliono usare i dati personali per scopi diversi da quelli specificati o compatibili.
- Assicurarsi che il nuovo uso sia equo, legale e trasparente.

Sfondo

Lo scopo dovrebbe essere "specificato, esplicito e legittimo".[21] Il gruppo di lavoro dell'articolo 29 nota che "uno scopo che è vago o generale, come per esempio ... 'ricerca futura' - senza maggiori dettagli
— di solito non soddisfano i criteri di essere "specifici". Detto questo, il grado di dettaglio con cui uno scopo dovrebbe essere specificato dipende dal particolare contesto in cui i dati sono raccolti e dai dati personali coinvolti. In alcuni casi chiari, un linguaggio semplice sarà sufficiente a fornire una specificazione appropriata, mentre in altri casi potrebbe essere necessario un maggiore dettaglio."[22]

I permessi di elaborazione sono limitati a:

- gli scopi legittimi che sono stati esplicitamente specificati quando i dati sono stati raccolti, o per
- altri scopi che siano compatibili con gli scopi iniziali La compatibilità può essere giudicata utilizzando i seguenti criteri:

a) il legame tra gli scopi iniziali e gli scopi aggiuntivi in esame;
b) il contesto in cui i dati personali sono stati raccolti, in particolare per quanto riguarda la relazione tra gli interessati e il responsabile del trattamento;
c) la natura dei dati personali, in particolare se comprendono categorie speciali di dati personali (cioè, sensibili) o se vengono trattati dati personali relativi a condanne penali e reati
d) le possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

[18] Regolamento generale sulla protezione dei dati, Regolamento UE 2016/679, art. 89.
[19] Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, art. 9(4).
[20] Regolamento generale sulla protezione dei dati, Regolamento UE 2016/679, art. 10.
[21] Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, art. 5(1)(b).
[22] Gruppo di lavoro sulla 29protezione dei dati, "Parere 03/2013 sulla limitazione delle finalità", 15-16.

e) l'esistenza di garanzie adeguate, che possono includere la pseudonimizzazione.

Alcuni scopi che si *presume* siano compatibili, se vengono seguite le appropriate salvaguardie prescritte dalla legge, sono:

- l'archiviazione nell'interesse pubblico,
- ricerca scientifica o storica, e
- statistiche

Tuttavia, come osserva il GEPD, "la presunzione non è un'autorizzazione generale a trattare ulteriormente i dati in tutti i casi per scopi storici, statistici o scientifici. Ogni caso deve essere considerato in base ai propri meriti e alle proprie circostanze. Ma in linea di principio i dati personali raccolti nel contesto commerciale o sanitario, ad esempio, possono essere ulteriormente utilizzati a fini di ricerca scientifica, dal responsabile del trattamento originario o da un nuovo responsabile del trattamento, se sono previste adeguate garanzie... al fine di garantire il rispetto dei diritti della persona interessata, il test di compatibilità di cui all'articolo 6, paragrafo 4, dovrebbe comunque essere considerato prima del riutilizzo dei dati a fini di ricerca scientifica, in particolare quando i dati sono stati originariamente raccolti per scopi molto diversi o al di fuori del settore della ricerca scientifica."[23]

2.3. Minimizzazione dei dati

Per essere in linea con il principio di minimizzazione dei dati, i ricercatori devono:

- Si assicurano di raccogliere dati personali solo se sono adeguati, pertinenti e necessari per lo scopo che hanno specificato.
- Evitare di raccogliere quantità di dati personali maggiori del necessario.
- Astenersi dal raccogliere tipi di dati personali più dettagliati o granulari del necessario.
- Assicurarsi che non conservino i dati personali più a lungo del necessario.
- Rivedere periodicamente i dati personali che conservano per controllare se continuano ad essere in conformità con quanto sopra, e rimuovere i dati personali che non si qualificano.

Sfondo

Adeguatezza, pertinenza e necessità sono tre requisiti per il trattamento dei dati personali secondo il GDPR. Quindi, i dati inadeguati, cioè inadatti allo scopo specificato, non possono essere raccolti o trattati; i dati devono anche essere pertinenti, cioè devono servire allo scopo specificato. E la limitazione della necessità ha tre aspetti:

- quantità di dati;
- granularità dei dati e
- la durata dello stoccaggio (trattata in modo più completo nel principio della "limitazione dello stoccaggio" qui sotto)

Quindi, in termini semplici, i ricercatori dovrebbero cercare di raccogliere, conservare ed elaborare il minor numero di dati personali necessario, per il minor tempo possibile per raggiungere lo scopo specificato. Questo, come per altri principi, si ottiene attraverso misure sia tecniche che organizzative.

La minimizzazione dei dati è elencata come una preoccupazione speciale nel GDPR per coloro che trattano i dati personali per scopi di archiviazione nell'interesse pubblico, scopi di ricerca scientifica o storica, o scopi statistici, poiché questi operano sotto un regime leggermente rilassato quando si tratta del principio di limitazione delle finalità. Le misure che possono essere prese per la minimizzazione dei dati includono la pseudonimizzazione, se questo è fattibile.

2.4. Precisione

Per rispettare il principio di accuratezza, i ricercatori dovrebbero:

- Assicurarsi che i dati personali in loro possesso siano di fatto corretti.
- Assicurarsi che i dati personali in loro possesso siano aggiornati.

---

[23] Garante europeo della protezione dei dati, "Un parere preliminare sulla protezione dei dati e la ricerca scientifica", 22-23.

- Mettere in atto processi per controllare l'accuratezza dei dati, con scadenze per il controllo della valuta.
- Correggere qualsiasi dato di fatto errato o fuorviante non appena viene scoperto.
- Registra tutti gli errori che devono essere conservati come errori, insieme al motivo della conservazione.
- Rispettare qualsiasi richiesta di rettifica da parte degli individui.

Sfondo

Ci sono due aspetti del principio di accuratezza: l'esattezza dei fatti e l'essere aggiornati. È vietato utilizzare dati personali inesatti, poiché potrebbero essere inadatti allo scopo per il quale i dati sono richiesti. Inoltre, i dati inesatti potrebbero danneggiare le persone interessate, e potrebbero quindi violare il principio di equità. Pertanto, i ricercatori hanno l'obbligo di cancellare o correggere i dati personali inesatti.

Al fine di garantire che i loro dati personali siano esatti, agli interessati è stato concesso il diritto di chiedere la rettifica dei dati.

2.5. Limitazione dello stoccaggio

Per garantire il rispetto del principio di limitazione della conservazione, i ricercatori devono:

- Assicurarsi che non conservino i dati personali più a lungo del necessario per lo scopo per cui sono stati raccolti.
- Assicurarsi che cancellino o rendano anonimi i dati personali che non sono più necessari.
- Documentare lo scopo per cui i dati personali sono stati raccolti e per quanto tempo i dati devono essere conservati per raggiungere tale scopo.
- Documentate la giustificazione del periodo di conservazione.
- Rivedere la necessità di conservazione quando il periodo di conservazione predeterminato finisce.
- Identificare e documentare l'archiviazione di interesse pubblico, la ricerca scientifica o storica, o lo scopo statistico per cui i dati vengono conservati per un periodo più lungo di quello strettamente necessario, nel caso in cui i dati vengono conservati sotto l'eccezione per tali ricerche, insieme al rispetto delle garanzie adeguate, come prescritto legalmente dall'Art. 89.

Sfondo

I ricercatori non dovrebbero conservare i dati personali più a lungo di quanto sia necessario per gli scopi specificati per i quali i dati sono stati raccolti. I dati dovrebbero essere distrutti non appena non sono più necessari per gli scopi specificati.

Un modo per realizzare questo è quello di impegnarsi nell'anonimizzazione dei dati ogni volta che è possibile, convertendo così i dati personali in dati che non permettono più l'identificazione diretta o indiretta degli interessati a cui si riferiscono.

I ricercatori sono autorizzati a conservare i dati personali più a lungo di quanto strettamente necessario se i dati personali devono essere utilizzati esclusivamente per scopi di archiviazione nel pubblico interesse, per scopi di ricerca scientifica o storica o per scopi statistici, e se soddisfano inoltre le condizioni stabilite nell'articolo del89 GDPR di avere garanzie adeguate sotto forma di misure tecniche e organizzative appropriate per salvaguardare i diritti dell'individuo. Inoltre, i ricercatori dovrebbero assicurarsi di non utilizzare tali dati personali come base per qualsiasi misura o decisione riguardante un particolare individuo.[24]

2.6. Integrità e riservatezza

Per rispettare il principio di integrità e riservatezza, i ricercatori devono:

---

[24] Articolo Gruppo di lavoro sulla 29protezione dei dati, "Parere 03/2013 sulla limitazione delle finalità",28 .

- Garantire che i dati personali siano conservati in modo sicuro, proteggendoli da elaborazioni non autorizzate o illegali, e da perdite accidentali, distruzione o danni, utilizzando sia misure tecniche che organizzative.
- Documentare le misure tecniche e organizzative messe in atto per garantire la sicurezza.

Sfondo

I ricercatori sono obbligati a garantire che i dati personali siano conservati in modo sicuro, il che significa che assicurano la riservatezza, l'integrità e la disponibilità dei dati, e quindi la protezione contro il trattamento non autorizzato o illegale e contro la perdita accidentale, la distruzione o il danno, utilizzando sia mezzi tecnici che organizzativi.

Quindi, la sicurezza dei dati è una parte fondamentale della protezione dei dati personali. Nell'affrontare se la confidenzialità e l'integrità sono state soddisfatte, è importante guardare dalla prospettiva delle persone interessate e non dalla prospettiva dei ricercatori. In altre parole, anche se i ricercatori non hanno subito alcun danno a causa del trattamento non autorizzato, non si può dire che il trattamento non autorizzato non abbia causato alcun danno.

Questo significa che i ricercatori devono avere ruoli e responsabilità chiaramente designati in modo che sia chiaro chi ha accesso autorizzato ai dati personali per ogni particolare impresa di ricerca.

2.7. Responsabilità

Per il rispetto del principio di responsabilità, i ricercatori devono:

- Assicurarsi che siano proattivi e organizzati nel loro rispetto della legge sulla protezione dei dati.
- Imparare a conoscere gli obblighi imposti loro e i diritti che gli individui hanno secondo la legge.
- Mettere in atto politiche chiare, processi e misure tecniche che garantiscano la conformità ai principi di cui sopra e alla legge.
- Assicurarsi che venga seguito l'approccio "privacy by design e by default".
- Assicurarsi che la loro organizzazione abbia un responsabile della protezione dei dati nel caso in cui siano un'autorità o un organismo pubblico; se si impegnano in un monitoraggio regolare e sistematico degli individui su larga scala; o se trattano una grande quantità di categorie speciali di dati, come i dati sensibili.
- Condurre una valutazione d'impatto sulla protezione dei dati se il tipo di trattamento dei dati che desiderano intraprendere può comportare un rischio elevato, e in particolare se prevedono di utilizzare sistematicamente ed estesamente la profilazione con effetti significativi; elaborare su larga scala dati di categorie speciali o di reati penali; o monitorare sistematicamente su larga scala luoghi accessibili al pubblico.
- Notificare gli individui, di solito attraverso il responsabile della protezione dei dati della vostra istituzione, di una violazione dei dati non più tardi di ore72 se la

violazione può comportare un rischio per i diritti e le libertà degli individui i cui dati personali sono stati violati.
- Rispondere immediatamente a qualsiasi esercizio da parte degli individui dei loro diritti sui loro dati.
- Documentare la loro conformità a tutti i principi di cui sopra e alla legge.

Sfondo

Coloro che raccolgono e utilizzano i dati personali, come i ricercatori, sono responsabili del rispetto dei principi sopra elencati. È importante che siano in grado di dimostrare che sono conformi.

Quindi il rispetto di questi principi deve essere pianificato e documentato. Per esempio, i ricercatori dovrebbero essere in grado di giustificare perché hanno bisogno di certi dati personali alla granularità con cui li stanno raccogliendo e la durata di conservazione dei dati. Molti aspetti della responsabilità trarrebbero vantaggio da misure tecniche automatizzate.

3 Buone pratiche relative ai principi di protezione dei dati

Le buone pratiche per i principi di protezione dei dati riguardano pratiche che vanno oltre il minimo che è legalmente richiesto dal GDPR e dalle leggi nazionali. Anche se non sono legalmente richieste, aiuteranno i ricercatori a rispettare i principi di protezione dei dati già discussi in questo documento.

3.1. Anonimizzazione, pseudonimizzazione e crittografia

I vari requisiti del GDPR non si applicano se i ricercatori non trattano *dati personali*. Quindi, quando possibile, controllate se i dati necessari per la ricerca richiedono di poter identificare una persona. Ma si noti che il GDPR distingue tra dati pseudonimizzati e dati resi anonimi. La semplice rimozione di tutti gli identificatori personali non rende automaticamente i dati "anonimizzati".

I dati personali pseudonimi si riferiscono a dati personali che non possono più essere attribuiti a un soggetto specifico senza l'uso di informazioni aggiuntive; ma con informazioni aggiuntive, il soggetto dei dati può essere scoperto.

Per i dati resi anonimi, non solo non si deve essere in grado di identificare alcun individuo in particolare sulla base dei dati che si sono raccolti e trattati, ma si devono anche considerare tutti i mezzi che altri possono trovare "ragionevolmente probabile che vengano utilizzati, come l'individuazione ... per identificare la persona fisica direttamente o indirettamente. "Per vedere quali mezzi sono "ragionevolmente utilizzabili per identificare la persona fisica", il GDPR ci informa che "si dovrebbe tener conto di tutti i fattori oggettivi, come i costi e la quantità di tempo necessario per l'identificazione, tenendo conto della tecnologia disponibile al momento del trattamento e gli sviluppi tecnologici. "[1]Così, se è praticamente possibile de-anonimizzare i dati, allora questo non può essere visto come dati anonimizzati - sarebbe allora un dato pseudonimizzato, che conta ancora come dati personali.

Il GDPR suggerisce la pseudonimizzazione e la crittografia come due mezzi per garantire una migliore sicurezza dei dati personali. Entrambe le tecniche aiuterebbero a soddisfare i requisiti del principio di integrità e riservatezza. La pseudonimizzazione aiuterebbe anche a rispettare il principio di minimizzazione dei dati. Nel caso di alcuni tipi di trattamento dei dati per la ricerca scientifica, per i quali i principi di limitazione delle finalità sono leggermente allentati, il GDPR richiede che i ricercatori cerchino di minimizzare i dati, e di farlo utilizzando la pseudonimizzazione quando possibile o di rendere anonimi i dati se questo è fattibile.[2]

3.2. Dati aggregati e grossolani

Quando possibile, preferire i dati aggregati ai dati a livello individuale, e preferire i dati grossolani ai dati granulari. Per esempio, se sono richiesti dati sull'età, scegliete di raccoglierli sotto forma di un numero piuttosto che di una data di nascita. Meglio ancora, se è sufficiente un intervallo di età, scegliete di raccoglierlo invece di un'età precisa. Infine, se la data di più persone può essere aggregata e i dati a livello individuale distrutti, allora scegliete di farlo.

3.3. Trasparenza

Se i dati personali sono raccolti in un contesto online, fornire un link prominente alla dichiarazione o all'avviso sulla privacy, o assicurarsi che l'informazione sia disponibile sulla stessa pagina in cui i dati personali sono

---

1 Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, considerando 26.

2 Regolamento generale sulla protezione dei dati, regolamento UE 2016/679, art. 89(1).

raccolti.[3] Se ci sono cambiamenti nel modo in cui si trattano i dati personali, tutte le informazioni dovrebbero essere fornite di nuovo al soggetto dei dati, rendendo facile dire quali informazioni tra esse sono nuove.[4]

3.4. Molteplici motivi di trattamento

Il GDPR sembra consentire la possibilità di utilizzare più motivi legittimi per il trattamento degli stessi dati personali. Tuttavia, questo potrebbe portare a una situazione in cui due motivi (come il consenso e l'interesse legittimo) sono utilizzati, ma uno dei motivi viene rimosso (come un individuo che revoca il consenso). In tal caso, non è chiaro cosa richiede la legge, e non c'è una chiara opinione unanime tra le autorità legali. È preferibile risolvere questa incertezza attraverso una comprensione conservativa della legge, e cessare di trattare qualsiasi dato quando uno dei motivi scompare. Per evitare questa situazione, può essere preferibile non combinare il consenso con altri motivi. In questi casi, può essere preferibile scegliere di trattare i dati solo in base al motivo più appropriato.

3.5. Il consenso nella protezione dei dati e nell'etica

Il consenso come base legale per il trattamento dei dati secondo la legge sulla protezione dei dati è diverso dal "consenso informato" come principio di etica per la ricerca su soggetti umani.[5] Quindi è sempre preferibile fornire moduli di consenso separati e ottenere ogni tipo di consenso separatamente. Anche se l'istituzione ottiene entrambi utilizzando un unico modulo di consenso, si dovrebbe mantenere una registrazione chiara di ciò che ogni partecipante ha acconsentito per quanto riguarda la ricerca.

Anche nei casi in cui il consenso non è utilizzato come motivo ai sensi del GDPR, "il *consenso informato* come partecipante alla ricerca umana potrebbe ancora servire come "salvaguardia adeguata" dei diritti del soggetto interessato."[6]

3.6. Legittimità, equità e approvazioni etiche

La legittimità della raccolta dei dati sarà a volte determinata da leggi che prescrivono requisiti etici (come per gli studi clinici). Ma anche quando una ricerca specifica non è coperta da requisiti legali di autorizzazione etica, è meglio lavorare sul presupposto che la raccolta o l'uso non etico dei dati sarà anche visto come uno scopo illegittimo per la base del GDPR, oltre a non rispettare il principio di equità. Così, per esempio, i ricercatori dovrebbero astenersi dall'impegnarsi in qualsiasi trattamento di dati che un comitato di revisione etica disapprova.

3.7. Autorità di protezione dei dati e comitati etici

Data la crescente interazione tra le questioni etiche e quelle relative alla privacy e alla protezione dei dati, sarebbe proficuo per le commissioni di revisione etica impegnarsi maggiormente con i responsabili della protezione dei dati e le autorità.[7] Ci sono molti casi (come i dati genetici) in cui l'uso dei dati personali di un individuo

nella ricerca influenzerebbe non solo quell'individuo, ma anche altri. Il quadro della protezione dei dati da solo può essere inadeguato a catturare queste preoccupazioni in un modo che un quadro combinato di etica della ricerca e protezione dei dati potrebbe. Questo richiede una maggiore collaborazione tra coloro che lavorano su questioni etiche e quelli che lavorano su questioni di protezione dei dati.

---

[3] Articolo Gruppo di lavoro sulla 29protezione dei dati, "Linee guida sulla trasparenza ai sensi del regolamento 2016/679",8 .

[4] Articolo Gruppo di lavoro sulla 29protezione dei dati, 27-28.

[5] Garante europeo della protezione dei dati, "Un parere preliminare sulla protezione dei dati e la ricerca scientifica", 19-20.

[6] Garante europeo della protezione dei dati,20 .

[7] Garante europeo della protezione dei dati,25 .

3.8. Linee guida sulla protezione dei dati e DPO

Molte istituzioni di ricerca hanno emesso linee guida per la protezione dei dati, oltre alle linee guida etiche. I ricercatori dovrebbero familiarizzare con le linee guida della loro istituzione. Molte volte, anche i finanziatori hanno requisiti speciali sulla protezione dei dati. Tutti i progetti finanziati da Horizon 2020, per esempio, richiedono il coinvolgimento di un responsabile della protezione dei dati (DPO) se è stato nominato, e anche nei casi in cui un DPO non è legalmente richiesto,[8] deve essere elaborata una politica di protezione dei dati.

Ci sono alcune questioni su cui si applicano le leggi degli stati membri, piuttosto che il solo GDPR. Importante per i ricercatori, il regime speciale di protezione dei dati per l'elaborazione ai fini dell'archiviazione nel pubblico interesse, della ricerca scientifica o storica, o a fini statistici, può avere allentamenti nei diritti dell'individuo e i conseguenti obblighi del ricercatore, se le leggi nazionali lo permettono. Per il trattamento dei dati personali per uno di questi scopi sono necessarie adeguate garanzie. I ricercatori devono attenersi ai principi discussi sopra, e devono prestare particolare attenzione alle misure tecniche e organizzative per garantire la minimizzazione dei dati.[9] Dato che le specifiche degli obblighi dei ricercatori secondo la legge non sono quindi uniformi, i ricercatori dovrebbero consultare il responsabile della protezione dei dati della loro istituzione e le linee guida sulla protezione dei dati, se possibile, in quanto sarebbero in grado di aiutare a guidare i ricercatori sugli standard legali ed extra-legali applicabili.

3.9. Valutazione d'impatto sulla protezione dei dati

Se un progetto tratterà una grande quantità di dati personali, o i dati personali di persone vulnerabili, allora discutere tale progetto con l'RPD e istituire una valutazione d'impatto sulla protezione dei dati (DPIA) sarebbe utile, anche quando non è legalmente obbligatorio farlo. Il GEPD nota che una "DPIA è obbligatoria per le operazioni di trattamento dei dati che presentano rischi elevati per gli interessati, come quando si applicano due dei seguenti criteri": [10]1. Valutazione/profilazione sistematica Processo decisionale automatizzato2. Monitoraggio sistematico3. Trattamento di dati sensibili4. Trattamento su larga 5.scala Abbinare/combinare6. serie di dati con finalità diverse Interessati vulnerabili7. Nuove 8.tecnologie Impedire9. alle persone di esercitare i propri diritti o di stipulare un servizio/contratto

[8] Regolamento generale sulla protezione dei dati, Regolamento UE 2016/679, art. 38.

[9] Regolamento generale sulla protezione dei dati, Regolamento UE 2016/679, art. 89.

[10] Garante europeo della protezione dei dati, "Decisione del Garante europeo della protezione dei dati di luglio16 sugli elenchi 2019DPIA rilasciati ai sensi dell'articolo 39, paragrafi 4 e 5, del regolamento (UE) 2018/1725", allegato 1.

4 Allegati

4.1. Allegato 1: Risorse chiave

Il progetto PANELFIT ha messo insieme una serie dettagliata di linee guida sulla protezione dei dati, etica e legale nella ricerca e innovazione ICT, così come un'analisi critica del quadro normativo sulla protezione dei dati ICT. Il CCDP è ampiamente basato su questi due documenti. Coloro che desiderano capire di più sulle questioni sollevate nel CCDP o desiderano capire gli aspetti della protezione dei dati che non sono stati coperti nel CCDP sono invitati a consultare le linee guida, che forniscono molti più dettagli.

Saranno entrambi disponibili su https://www.panelfit.eu/deliverables/.

Qui ci sono altre importanti risorse per i ricercatori che cercano di saperne di più sulla protezione dei dati e sulla ricerca e l'innovazione responsabile.

- Garante europeo della protezione dei dati. "A Preliminary Opinion on Data Protection and Scientific Research", gennaio https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_ 2020.research_en.pdf.
- Articolo Gruppo di lavoro sulla 29protezione dei dati. "Parere 03/2013 sulla limitazione delle finalità", aprile2,2013. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/ wp203_it.pdf.
- Articolo Gruppo di lavoro sulla 29protezione dei dati. "Parere 05/2014 sulle tecniche di anonimizzazione", aprile https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/ 10,2014/wp216_it2014..pdf *.
- Articolo Gruppo di lavoro sulla 29protezione dei dati. "Linee guida sulla trasparenza ai sensi del regolamento 2016/679", novembre h29,2017.ttps://ec.europa.eu/newsroom/article29/items/622227.
- Comitato europeo per la protezione dei dati. "Linee guida 03/2020 sul trattamento dei dati relativi alla salute ai fini della ricerca scientifica nel contesto dell'epidemia di COVID-19. "Linee guida, aprile30, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines__ 2020.healthdatascientificresearchcovid19_it202003.pdf.
- Comitato europeo per la protezione dei dati. "Linee guida 4/2019 sull'articolo Protezione dei dati25 per progettazione e per impostazione predefinita. "Linee guida, novembre https://edpb.europa.eu/sites/edpb/files/consultation/ 13,edpb_guidelines_201904_dataprotection_by_design_and_by_default2019.. pdf.
- Comitato europeo per la protezione dei dati. "Linee guida 04/2019 sull'articolo 25: Protezione dei dati per progettazione e per impostazione predefinita. "Linee guida, ottobre https://edpb.europa.eu/sites/edpb/files/files/file1/

20,edpb_guidelines_201904_dataprotection_by_design_and_by_default_v22020..0_en.pdf.

- Garante europeo della protezione dei dati. "Orientamenti del GEPD sulla valutazione della proporzionalità delle misure che limitano i diritti fondamentali alla privacy e alla protezione dei dati personali", dicembre https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_ 19,proportionality_guidelines2_en2019..pdf.
- Garante europeo della protezione dei dati. "Diagrammi di flusso e liste di controllo sulla protezione dei dati."2020.https://doi.org/10.2804/823679.
- Commissione europea (Direzione generale per la ricerca e l'innovazione). "Etica e protezione dei dati", novembre 2018.https://ec.europa.eu/research/participants/data/ref/h2020/grants_ manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf.
- ALLEA. *Il Codice europeo di condotta per l'integrità della ricerca*. 2a ed., 2017.https://ec.europa.eu/

research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf.

- Progetto RESPECT. "Codice di pratica di RESPECT per la ricerca socioeconomica. " Istituto per gli studi sull'occupazione, 2004.http://www.respectproject.org/code/respect_code.pdf
- EFAMRO e ESOMAR. "Guidance Note for the Research Sector:Appropriate Use of Different Legal Bases under the GDPR. " Giugno https://www.esomar.org/uploads/public/government- 2017.affairs/position-papers/EFAMRO-ESOMAR_GDPR-Guidance-Note_Legal-Choice.pdf.
- Wilford, Sara, Malcolm Fisk, e Bernd Stahl. "Linee guida per una ricerca e un'innovazione responsabili. " GREAT Project, 2016. https://www.great-project.eu/Deliverables10.
- Il Comitato europeo per la protezione dei dati ha dichiarato che "intende emettere una guida sulle condizioni "orizzontali e complesse" per l'applicabilità della "presunzione di compatibilità" dell'ulteriore trattamento per scopi di archiviazione nel pubblico interesse, ricerca scientifica, storica o statistica, come previsto dall'articolo 5(1)(b) del GDPR. "'Questo sarà utile per i ricercatori quando sarà emesso.

4.2. Allegato 2: Bibliografia

Articolo Gruppo di lavoro sulla 29protezione dei dati. "Linee guida sulla trasparenza ai sensi del regolamento 2016/679"29, novembre h2017.ttps://ec.europa.eu/newsroom/article29/items/622227.

---. 'Opinion 03/2013 on Purpose Limitation'2, aprile 2013.https://ec.europa.eu/justice/article- 29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Commissione Europea. Scienza con e per la società'. Horizon November2020,112013. https:// ec.europa.eu/programmes/horizon2020/en/h2020-section/science-and-society.

---. Quali informazioni devono essere date alle persone i cui dati sono raccolti? '. Testo. Principio del GDPR - Quali informazioni devono essere date alle persone i cui dati sono raccolti?, gennaio https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/ 82018.principles-gdpr/what-information-must-be-given-individuals-whose-data-collected_en.

Comitato europeo per la protezione dei dati. Parere del comitato (art. 70.I.b)". Parere, gennaio 23h2019.ttps://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf.

Garante europeo della protezione dei dati. 'A Preliminary Opinion on Data Protection and Scientific Research', gennaio h2020.ttps://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

---. "Decisione del Garante europeo della protezione dei dati di luglio 16sugli elenchi 2019DPIA rilasciati ai sensi dell'articolo 39, paragrafi 4 e 5, del regolamento (UE)

2018/1725", luglio https://edps.europa.eu/ 162019.sites/default/files/publication/19-07-16_edps_dpia_list_en.pdf.
General Data Protection Regulation, Regolamento UE 2016/679 (2016). https://eur-lex.europa.eu/legal- content/EN/TXT/? uri=CELEX%3A02016R0679-20160504.
'Dichiarazione di Roma sulla ricerca responsabile e l'innovazione in Europa', novembre 212014.https:// ec.europa.eu/research/swafs/pdf/rome_declaration_RRI_final_21_November.pdf.

4.3. Allegato 3: Processo per la creazione del codice di condotta sulla protezione dei dati per la ricerca e l'innovazione responsabile

Abbiamo cercato di coinvolgere più parti interessate nella revisione del CCDP e di ottenere più feedback possibile. Il processo di consultazione è descritto di seguito.

La prima bozza del CCDP è stata fatta circolare in ottobre e2020 la versione finale è stata consolidata in agosto Sono state generate cinque2021. versioni in diverse fasi del processo, incorporando il feedback ad ogni passo. Le seguenti sezioni riassumono il processo di feedback del CCDP, catturano i commenti più significativi ricevuti e i passi fatti per rispondere in ogni caso.

La portata di ciascuna delle fasi di feedback è descritta di seguito:

[1] Comitato europeo per la protezione dei dati, "Parere del Comitato (art. 70.I.b)".

- Consultazione di esperti interni (PANELFIT): la prima versione del CCDP generata in ottobre è stata 2020esaminata dal consorzio del progetto PANELFIT che comprende esperti in cybersecurity, governance, privacy, protezione dei dati, tra gli altri.

- Consultazione di esperti esterni (stakeholder): questa consultazione è stata effettuata attraverso il Mutual Learning Encounter per gli stakeholder organizzato dal progetto. In questo evento online tenutosi in aprile si sono incontrate persone202021,13 delle seguenti organizzazioni: ALLEA, European Group on Ethics (EGE) alla Commissione Europea, Università di Vilnius, NEC Laboratories Europe, Tech Uni Cluj-Napoca, Museum for Naturkunde, COCIR, Babes-Bolyai University, Research Centre for Data Science e Senior Lecturer, School of Computing, Electronics and Mathematics at Coventry University, Uni Babes Bolyai, Commissione Europea, Open Science (DG RTD), Tilburg University, School of Computing, Electronics and Mathematics at Coventry University, University of Copenhagen.

- Consultazione di ricercatori esterni: ricercatori di varie discipline hanno partecipato al Mutual Learning Encounter per ricercatori organizzato dal progetto. L'evento online si è tenuto a giugno 242021.

- Consultazione pubblica: il CCDP è stato pubblicato sul sito web PANELFIT con un modulo disponibile per ricevere feedback da qualsiasi persona interessata. La partecipazione al feedback è stata promossa attraverso i social network e le mailing list. Il documento è stato disponibile da marzo ad agosto al2021 seguente link: https://www.panelfit.eu/a-code-of-conduct-on-data-protection-for-responsible-research- and-innovation-ccdp/

- Sondaggio dei ricercatori: il sondaggio faceva parte del processo di chiusura del feedback del CCDP. È stato fatto circolare prima, durante e dopo il MLE per i ricercatori. Il feedback ha contribuito al miglioramento della sezione sulle buone pratiche.