



Accountability e registro dei trattamenti

A domanda risponde Prof. Avv. Michele IASELLI

21 maggio 2024 - dalle ore 11.30 alle 12.30

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione
degli Enti Locali

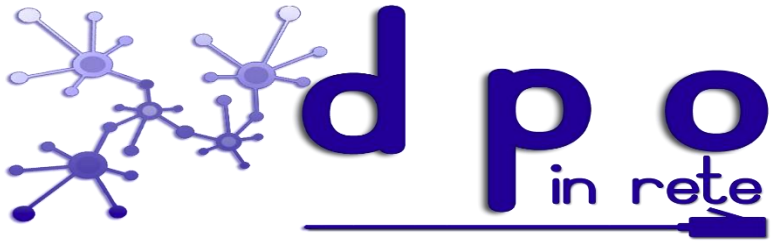
Email info@dpointrete.it

Numero Verde 800.16.56.54

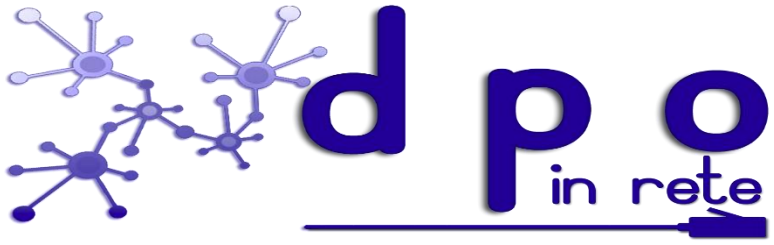
Web: www.dpointrete.it

www.asmel.eu





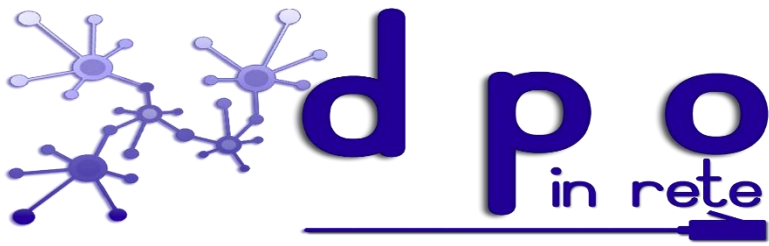
Il principio dell'accountability



Origini e definizione

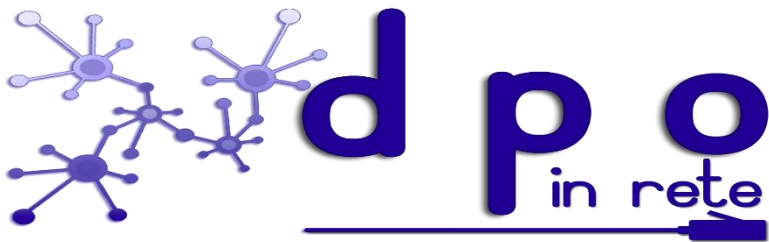


Il termine anglosassone “accountability” non è facilmente traducibile e difatti nella traduzione del regolamento europeo si parla impropriamente di “responsabilità”. Al massimo la traduzione più corretta, anche se poco pratica, potrebbe essere quella di “rendicontazione”.

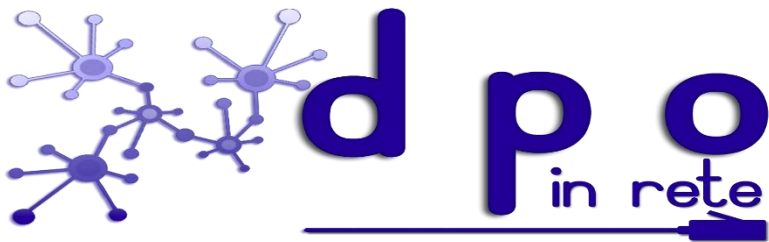


In realtà il termine “accountability” richiama almeno due accezioni o componenti fondamentali:

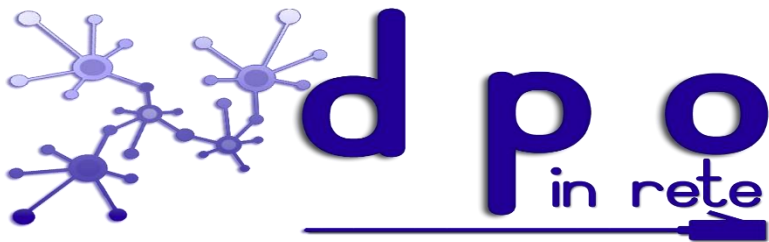
1. da un lato il dar conto all'esterno e in particolare al complesso degli stakeholder, in modo esaustivo e comprensibile, del corretto utilizzo delle risorse e della produzione di risultati in linea con gli scopi istituzionali;
2. dall'altro, l'esigenza di introdurre logiche e meccanismi di maggiore responsabilizzazione interna alle aziende e alle reti di aziende relativamente all'impiego di tali risorse e alla produzione dei correlati risultati.



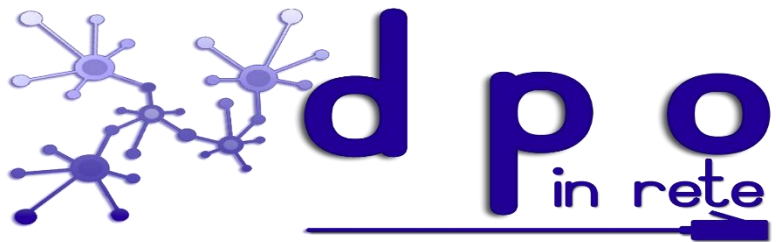
Autore	Commento
Romzek e Dubnick	L'accountability è "un concetto fondamentale ma non sufficientemente approfondito nell'amministrazione pubblica".
Gormley	"L'accountability è divenuto concetto torbido".
Moore e Gates	"I connotati dell'accountability sono in continuo cambiamento".
Kearns	L'accountability è divenuta un "termine omnicomprensivo: dal controllo dei costi all'etica professionale".
Mosher	L'accountability è un "fuoco fatuo".
Sinclair	L'accountability è un concetto "camaleontico", cruciale e ricercato, ma elusivo.
Mulgan	L'accountability è "un concetto in continua espansione".
Uhr	Pochi termini attraggono una tale confusione come quello di accountability.



Autore	Definizione di accountability
M. J. Dubnick	<p>L'accountability è una relazione nella quale un individuo o un ente è tenuto a rispondere della performance connessa a una data attribuzione di autorità di agire.</p> <p>I meccanismi di accountability sono i mezzi con i quali determinare se un compito delegato è stato portato a termine in maniera soddisfacente.</p> <p>L'accountability è costituita da quell'insieme di azioni che svolgono la funzione sociale di "dar conto".</p>
P. Aucoin, R. Heintzman	<p>L'accountability è la pietra angolare della governance e del management pubblico perché costituisce il principio che caratterizza i processi in cui coloro i quali tengono o esercitano un'autorità pubblica sono chiamati a "renderne conto".</p>
R. Mulgan	<p>Il significato del termine accountability sul quale la maggior parte degli autori concorda attiene al processo mediante il quale qualcuno è chiamato a "dar conto" a una qualche autorità per una data azione.</p>
J. Roberts, R. Scapens	<p>Il nucleo fondamentale del processo di accountability consiste "nel fornire e nel richiedere le ragioni per un dato comportamento".</p>
A. Grey, B Jenkins	<p>L'accountability è l'obbligo di dar conto e rispondere per l'esecuzione delle responsabilità a coloro i quali hanno assegnato tali responsabilità.</p>
R. J. Boland, U. Schultze	<p>L'accountability attiene alla "capacità e disponibilità a fornire spiegazioni per un dato comportamento, dimostrando come le responsabilità sono state messe in atto".</p>
A. Scheldler	<p>Si può dire che A è accountable nei confronti di B, quando A è obbligato a informare B circa le proprie azioni e decisioni (passate o future), a giustificarle e ad accettare un'eventuale sanzione nel caso di una cattiva condotta.</p>
OECD	<p>L'accountability è l'obbligo di coloro ai quali è stata affidata una data responsabilità di dar conto di, e di rispondere per, il suo adempimento.</p>
GASB	<p>L'accountability implica che le amministrazioni pubbliche rispondano alla comunità amministrata e giustifichino il prelievo di risorse pubbliche e gli scopi per i quali esse sono state impiegate.</p>



Il Regolamento recepisce tale principio all'art. 24 il quale prevede che tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. Inoltre, se ciò è proporzionato rispetto alle attività di trattamento, le predette misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

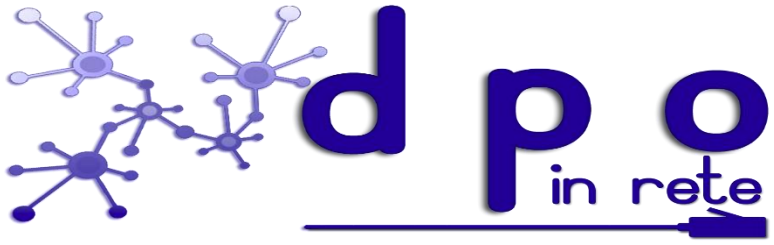


I pilastri dell'accountability

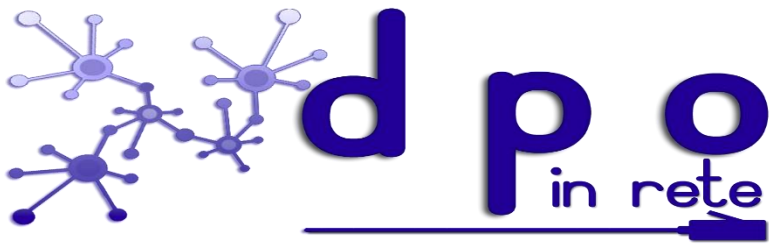


L'accountability si compone di almeno tre elementi:

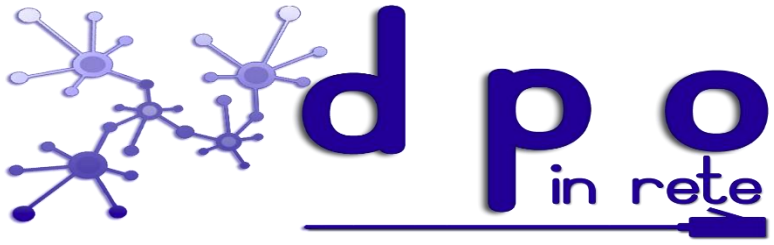
1. La "trasparenza" intesa come garanzia della completa accessibilità alle informazioni, in primo luogo per i cittadini, anche in quanto utenti del servizio.
2. La "responsività" intesa come la capacità di rendere conto di scelte, comportamenti e azioni e di rispondere alle questioni poste dagli stakeholder.
3. La "compliance" intesa come capacità di far rispettare le norme, sia nel senso di finalizzare l'azione pubblica all'obiettivo stabilito nelle leggi, che nel senso di fare osservare le regole di comportamento degli operatori della PA.



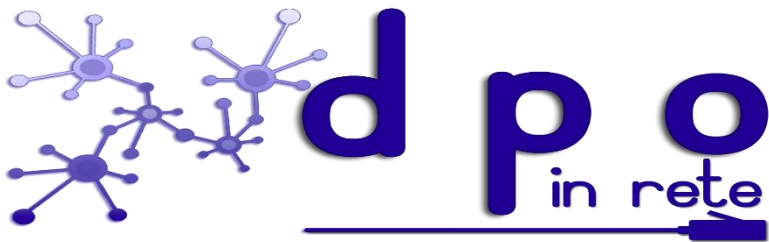
L'Accountability nella pubblica amministrazione



In un ambito pubblicistico il concetto di accountability è sicuramente collegato a quello di trasparenza. Difatti le istituzioni pubbliche compiono (o non compiono) quotidianamente atti rilevanti per la comunità nazionale. Ma proprio una tale responsabilità, mette i cittadini nelle condizioni di formulare domande e osservazioni sul rendimento degli uffici pubblici e dei dirigenti che li guidano. I cittadini chiedono che il potere amministrativo adotti delle decisioni, ma, allo stesso tempo, chiedono che queste decisioni risolvano i loro problemi e che siano comprensibili e trasparenti. In altre parole, chiedono di “rendere conto”.

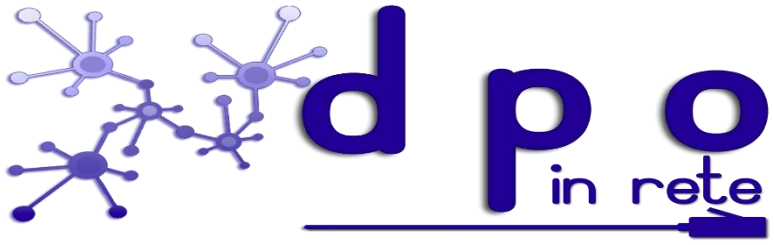


Tendenze europee verso l'accountability

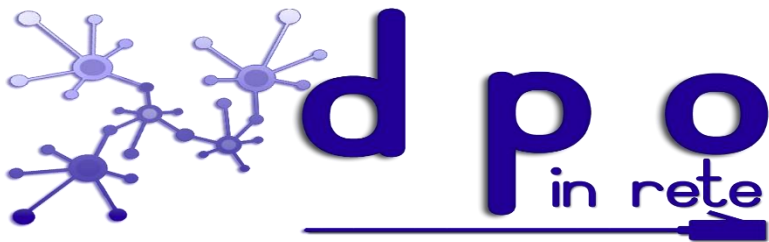


In ambito comunitario, il problema dell'*accountability* si avverte in maniera ancora più evidente, soprattutto se si prendono in conto gli avvenimenti che si sono verificati sotto la Commissione Santer che avevano condotto gli esperti ad affermare che l'Unione Europea si regge su regole tanto complesse che si rende difficile, se non impossibile, la definizione di un sistema efficiente di *accountability*. Di conseguenza non possiamo che rilevare come uno studio sull'*accountability* a livello comunitario richieda uno specifico approccio, che tenga in debito conto le differenze strutturali del sistema europeo rispetto ad altri, sia statuali che internazionali, piuttosto evidenti agli occhi degli analisti.

Una simile analisi comporta che siano compiute due valutazioni preliminari: la prima sulla specificità della struttura istituzionale e del sistema decisionale, la seconda relativa alla descrizione dei concetti di *governance* e, appunto, *accountability*.



Registro delle attività di trattamento



L'art. 30 del Regolamento prevede che ogni titolare del trattamento e il suo eventuale rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.



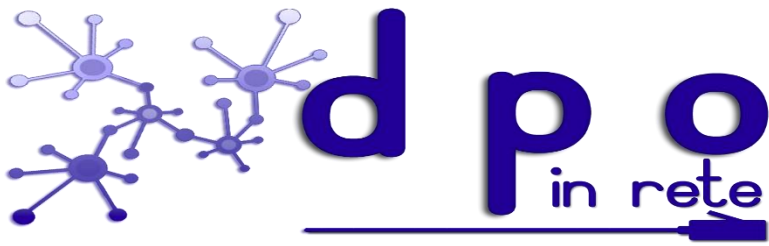
Il registro contiene le seguenti informazioni:

- a) il nome e i dati di contatto del titolare del trattamento e di ogni contitolare del trattamento, del rappresentante del titolare del trattamento e dell'eventuale responsabile della protezione dei dati;
- b) le finalità del trattamento;
- c) una descrizione delle categorie di interessati e delle categorie di dati personali;
- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi;
- e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

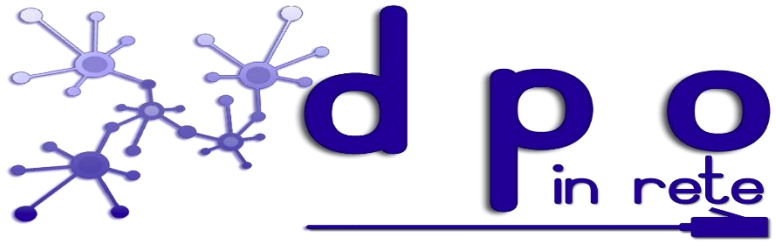


Anche ogni responsabile del trattamento e il suo eventuale rappresentante tengono un registro di tutte le categorie di attività di trattamento dei dati personali svolte per conto di un titolare del trattamento, contenente:

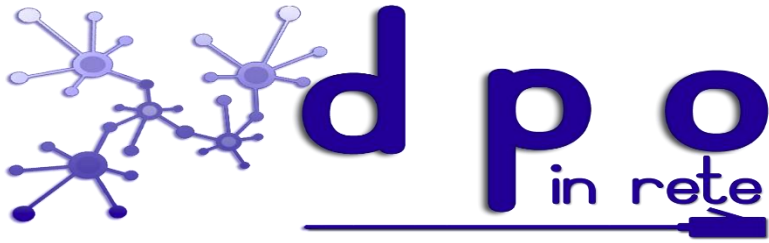
- a) nome e dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e dell'eventuale responsabile della protezione dei dati;
- b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- d) ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative.



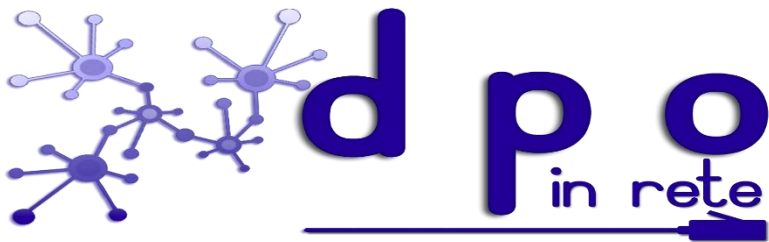
Su richiesta, il titolare del trattamento o il responsabile del trattamento e l'eventuale rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.



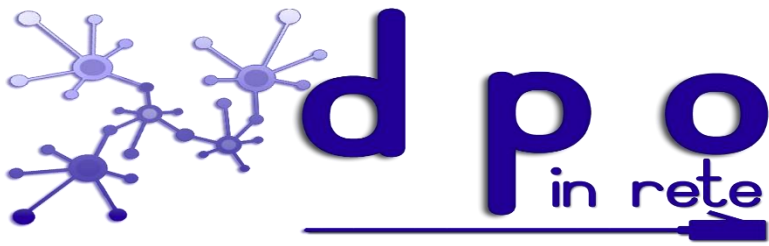
FAQ Garante



Più nello specifico, a seguito anche di quanto consigliato dall'Autorità Garante nelle proprie FAQ datate 8 ottobre 2018, si precisa:



a) nel campo “finalità del trattamento” oltre alla precipua indicazione delle stesse, distinta per tipologie di trattamento (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini), sarebbe opportuno indicare anche la base giuridica dello stesso (v. art. 6 del GDPR; in merito, con particolare riferimento al “legittimo interesse”, si rappresenta che il registro potrebbe riportare la descrizione del legittimo interesse concretamente perseguito, le “garanzie adeguate” eventualmente approntate, nonché, ove effettuata, la preventiva valutazione d’impatto posta in essere dal titolare (v. provv. del Garante del 22 febbraio 2018). Sempre con riferimento alla base giuridica, sarebbe parimenti opportuno: in caso di trattamenti di “categorie particolari di dati”, indicare una delle condizioni di cui all’art. 9, par. 2 del GDPR; in caso di trattamenti di dati relativi a condanne penali e reati, riportare la specifica normativa (nazionale o dell’Unione europea) che ne autorizza il trattamento ai sensi dell’art. 10 del GDPR;



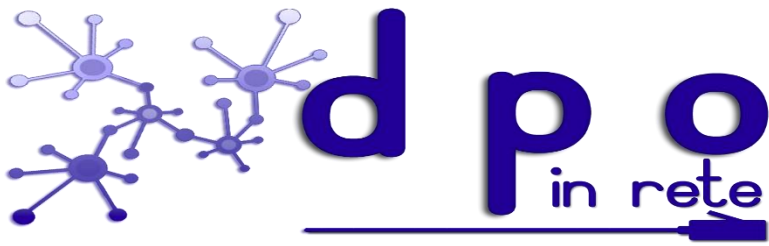
(b) nel campo “descrizione delle categorie di interessati e delle categorie di dati personali” andranno specificate sia le tipologie di interessati (es. clienti, fornitori, dipendenti) sia quelle di dati personali oggetto di trattamento (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.);



(c) nel campo “categorie di destinatari a cui i dati sono stati o saranno comunicati” andranno riportati, anche semplicemente per categoria di appartenenza, gli altri titolari cui siano comunicati i dati (es. enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi). Inoltre, si ritiene opportuno che siano indicati anche gli eventuali altri soggetti ai quali – in qualità di responsabili e sub-responsabili del trattamento– siano trasmessi i dati da parte del titolare (es. soggetto esterno cui sia affidato dal titolare il servizio di elaborazione delle buste paga dei dipendenti o altri soggetti esterni cui siano affidate in tutto o in parte le attività di trattamento). Ciò al fine di consentire al titolare medesimo di avere effettiva contezza del numero e della tipologia dei soggetti esterni cui sono affidate le operazioni di trattamento dei dati personali;



(d) nel campo “trasferimenti di dati personali verso un paese terzo o un’organizzazione internazionale” andrà riportata l’informazione relativa ai suddetti trasferimenti unitamente all’indicazione relativa al Paese/i terzo/i cui i dati sono trasferiti e alle “garanzie” adottate ai sensi del capo V del GDPR (es. decisioni di adeguatezza, norme vincolanti d’impresa, clausole contrattuali tipo, ecc.);



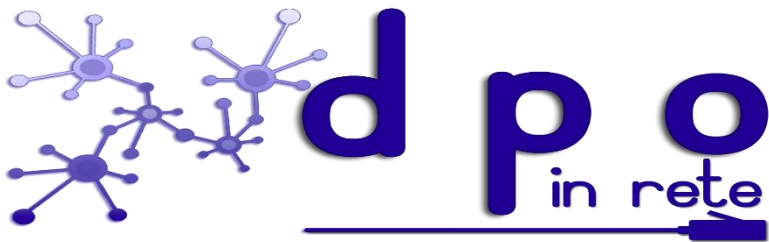
(e) nel campo “termini ultimi previsti per la cancellazione delle diverse categorie di dati” dovranno essere individuati i tempi di cancellazione per tipologia e finalità di trattamento (ad es. “in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall’ultima registrazione – v. art. 2220 del codice civile”). Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri (es. norme di legge, prassi settoriali) indicativi degli stessi (es. “in caso di contenzioso, i dati saranno cancellati al termine dello stesso”);



(f) nel campo “descrizione generale delle misure di sicurezza” andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell’art. 32 del RGDP tenendo presente che l’elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimessa al titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere. Tale lista ha di per sé un carattere dinamico (e non più statico come è stato per l’Allegato B del d. lgs. 196/2003) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l’insorgere di nuovi rischi. Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (es. procedure organizzative interne; security policy ecc.).

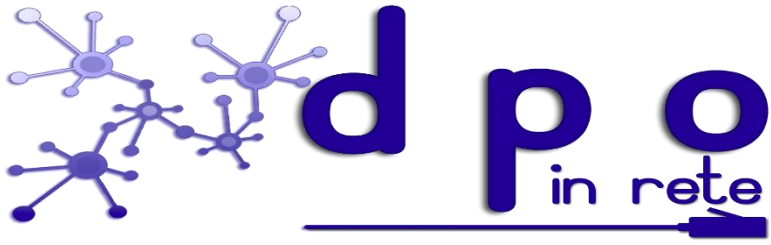


Può essere riportata nel registro qualsiasi altra informazione che il titolare o il responsabile ritengano utile indicare (ad es. le modalità di raccolta del consenso, le eventuali valutazioni di impatto effettuate, l'indicazione di eventuali "referenti interni" individuati dal titolare in merito ad alcune tipologie di trattamento ecc.).

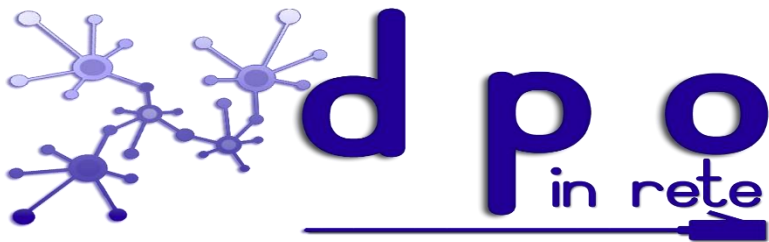


**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

SCHEDA REGISTRO DEI TRATTAMENTI <small>[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]</small>							
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE <small>[inserire la denominazione e i dati di contatto]</small>							
RESPONSABILE DELLA PROTEZIONE DEI DATI <small>[inserire la denominazione e i dati di contatto]</small>							
TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERSSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI <small>[Indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]</small>	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI <small>[Indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]</small>	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE



In merito, poi, al registro del responsabile del trattamento il Garante nelle proprie FAQ ha precisato che:



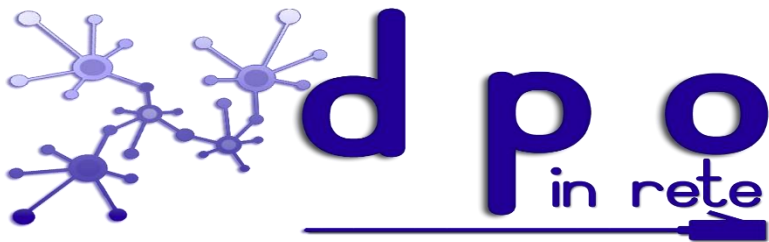
a) nel caso in cui uno stesso soggetto agisca in qualità di responsabile del trattamento per conto di più clienti quali autonomi e distinti titolari (es. società di software house), le informazioni di cui all'art. 30, par. 2 del GDPR dovranno essere riportate nel registro con riferimento a ciascuno dei suddetti titolari. In questi casi il responsabile dovrà suddividere il registro in tante sezioni quanti sono i titolari per conto dei quali agisce; ove, a causa dell'ingente numero di titolari per cui si operi, l'attività di puntuale indicazione e di continuo aggiornamento dei nominativi degli stessi nonché di correlazione delle categorie di trattamenti svolti per ognuno di essi risulti eccessivamente difficoltosa, il registro del responsabile potrebbe riportare il rinvio, ad es., a schede o banche dati anagrafiche dei clienti (titolari del trattamento), contenenti la descrizione dei servizi forniti agli stessi, ferma restando la necessità che comunque tali schede riportino tutte le indicazioni richieste dall'art. 30, par. 2 del GDPR;



b) con riferimento alla “descrizione delle categorie di trattamenti effettuati” (art. 30, par. 2, lett. b) del GDPR) è possibile far riferimento a quanto contenuto nel contratto di designazione a responsabile che, ai sensi dell’art. 28 del GDPR, deve individuare, in particolare, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati oggetto del trattamento, nonché la durata di quest’ultimo;



c) in caso di sub-responsabile, parimenti, il registro delle attività di trattamento svolte da quest'ultimo potrà specificatamente far riferimento ai contenuti del contratto stipulato tra lo stesso e il responsabile ai sensi dell'art. 28, paragrafi 2 e 4 del GDPR.



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

SCHEDA REGISTRO DEI TRATTAMENTI DEL RESPONSABILE/SUB-RESPONSABILE

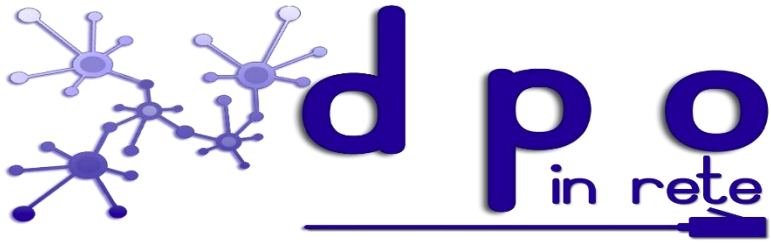
[per i contenuti vedi Faq sul registro delle attività di trattamento: <https://www.garanteprivacy.it/regolamentoue/registro>]

RESPONSABILE *[inserire la denominazione e i dati di contatto]*

TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*

RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*

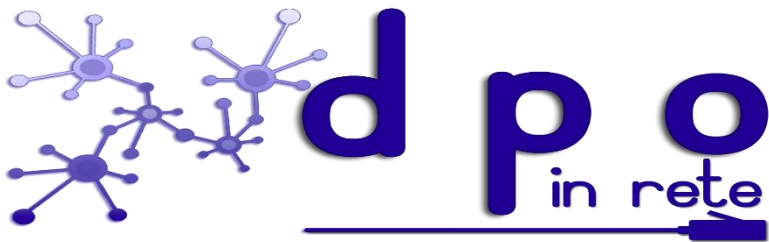
CATEGORIA DI TRATTAMENTO	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI <i>[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]</i>	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE



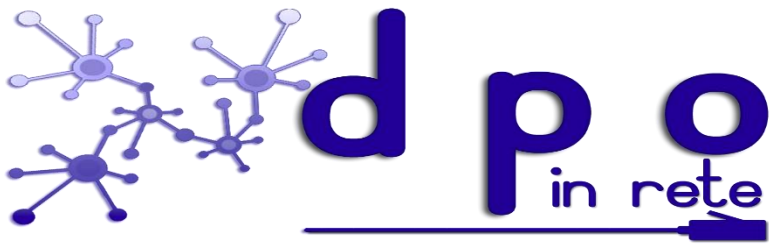
**Chi in concreto deve predisporre il
registro delle attività di trattamento**



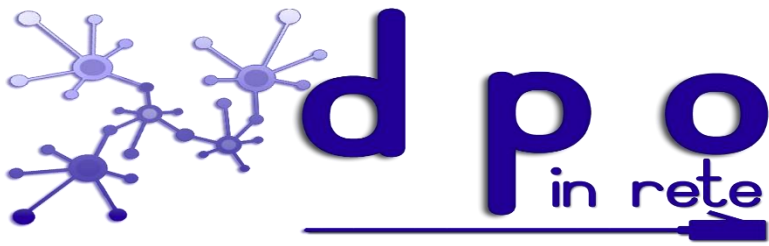
L'art. 30, però, chiarisce che l'obbligo della tenuta di questi registri non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati come quelli di cui all'art. 9 del GDPR (particolari) o all'art. 10 del GDPR (dati relativi a condanne penali, reato o connessi a misure di sicurezza).



In particolare (sulla scorta di quanto evidenziato anche dall'Autorità Garante nelle proprie FAQ datate 8 ottobre 2018), in ambito privato, i soggetti obbligati sono così individuabili:



- imprese o organizzazioni con almeno 250 dipendenti;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare un rischio – anche non elevato – per i diritti e le libertà dell'interessato;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all'articolo 9, paragrafo 1 GDPR, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 GDPR.



Alla luce di quanto detto sopra, sono tenuti all'obbligo di redazione del registro, ad esempio:

- esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);
- liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);
- associazioni, fondazioni e comitati ove trattino "categorie particolari di dati" e/o dati relativi a condanne penali o reati (i.e. organizzazioni di tendenza; associazioni a tutela di soggetti c.d. "vulnerabili" quali ad esempio malati, persone con disabilità, ex detenuti ecc.; associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso ecc.; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);
- il condominio ove tratti "categorie particolari di dati" (es. delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali).



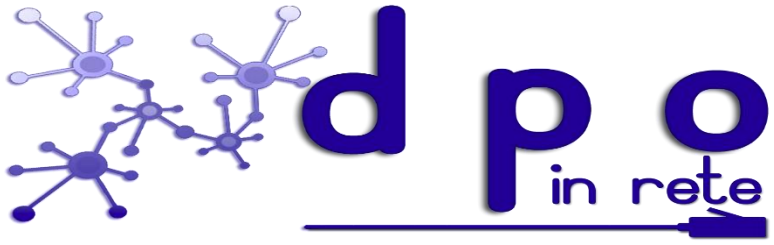
Al di fuori dei casi di tenuta obbligatoria del Registro, anche alla luce del considerando 82 del GDPR, il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso.



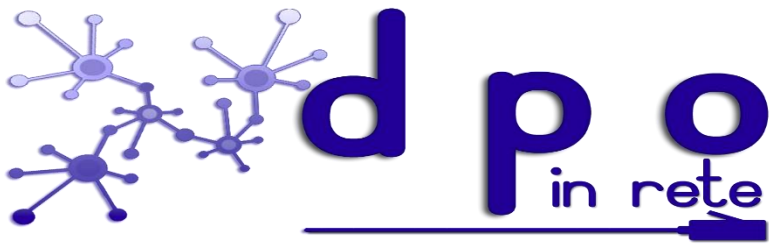
Nella realtà, come sostenuto dai Garanti europei nelle linee guida, sono spesso i DPO a realizzare l'inventario dei trattamenti e tenere un registro di tali trattamenti sulla base delle informazioni fornite loro dai vari uffici o unità che trattano dati personali.

È una prassi consolidata e fondata sulle disposizioni di numerose leggi nazionali nonché sulla normativa in materia di protezione dati applicabile alle istituzioni e agli organismi dell'UE.

Diventa, quindi, un'attività fondamentale dello stesso DPO per monitorare tutti i trattamenti della realtà organizzativa di riferimento.



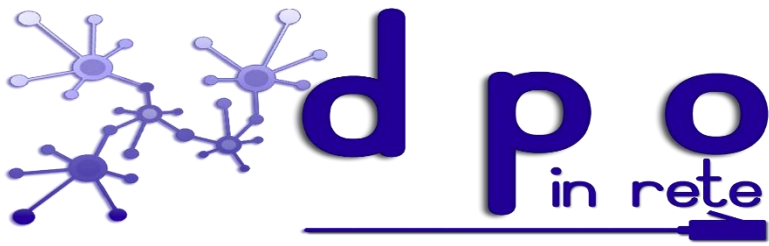
Modalità di compilazione del registro



Lo stesso art. 30 del GDPR prevede che il registro debba rispettare la forma scritta anche in formato elettronico. In realtà l'aspetto formale poco conta (cartaceo, elettronico, struttura schematica, descrittiva, foglio di calcolo, tabella) ciò che rileva è l'esistenza di tutti gli elementi richiesti dall'art. 30 del Regolamento e l'indicazione verificabile della data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella dell'ultimo aggiornamento. In quest'ultimo caso il registro dovrà recare una annotazione del tipo:

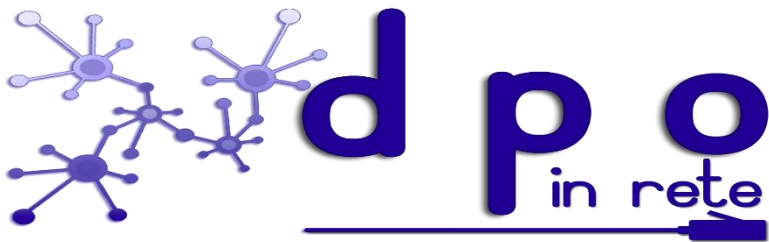
“- scheda creata in data XY”

“- ultimo aggiornamento avvenuto in data XY.



Come precisato dal Garante nelle proprie FAQ il registro dei trattamenti è un documento di censimento e analisi dei trattamenti effettuati dal titolare o responsabile.

In quanto tale, il registro deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Di conseguenza, qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

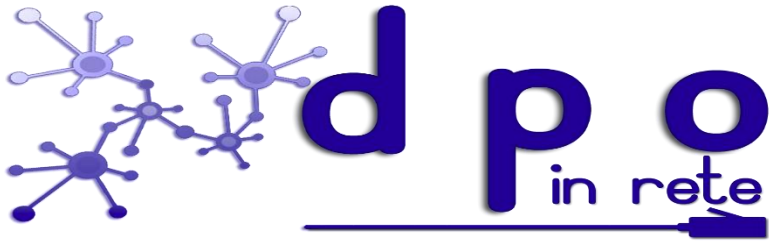


- **Funzione di business/ unità organizzativa/ dipartimento**

- **Denominazione del trattamento (se individuata)**

- **Finalità del trattamento**

- | | | |
|--|---|---|
| <input type="checkbox"/> Amministrazione del personale | <input type="checkbox"/> Albo fornitori | <input type="checkbox"/> Customer Care |
| <input type="checkbox"/> Gestione del personale | <input type="checkbox"/> Gestione Clienti | <input type="checkbox"/> Marketing |
| <input type="checkbox"/> Gestione di assicurazione sanitaria | <input type="checkbox"/> Anagrafica Clienti | <input type="checkbox"/> Direct Marketing |
| <input type="checkbox"/> Gestione di assicurazione sanitaria | <input type="checkbox"/> Contabilità | <input type="checkbox"/> Informazioni commerciali |
| <input type="checkbox"/> Gestione l. 81/2008 | <input type="checkbox"/> Gestione Crediti | <input type="checkbox"/> Analisi generale clientela |
| <input type="checkbox"/> Controllo accessi | <input type="checkbox"/> Insurance management | <input type="checkbox"/> Ricerca Storica |
| <input type="checkbox"/> Sicurezza fisica | <input type="checkbox"/> fuoco, incidenti e rischi vari | <input type="checkbox"/> Ricerca statistica |
| <input type="checkbox"/> Gestione fornitori | <input type="checkbox"/> Pianificazione delle attività | <input type="checkbox"/> Ricerche di mercato |
| | <input type="checkbox"/> Pubbliche relazioni | <input type="checkbox"/> Gestione del contenzioso |
| | | <input type="checkbox"/> Prevenzione frodi |
| | | <input type="checkbox"/> Altro_____ |



- **Software, database e manutenzione**

- Software XXX in cloud e cartelle su NAS, manutenzione da remoto
- Software Fidelity XXX, gestito da agenzia YYY

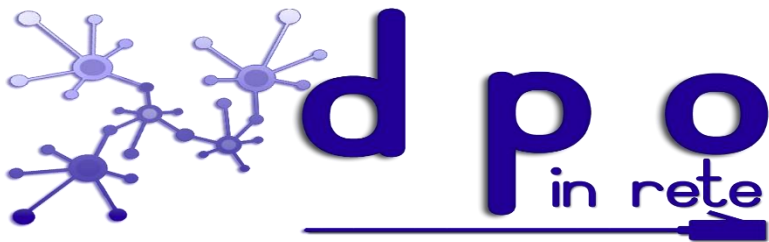
- **Denominazione e dati di contatto del contitolare (se presente)**

- **Categorie di interessati**

- | | | |
|---|---|---|
| <input type="checkbox"/> Dipendenti | <input type="checkbox"/> Controparti | <input type="checkbox"/> membri di organismi di controllo |
| <input type="checkbox"/> Clienti | <input type="checkbox"/> Professionisti | <input type="checkbox"/> revisori |
| <input type="checkbox"/> Fornitori | <input type="checkbox"/> Associati | <input type="checkbox"/> iscritti in albi ed elenchi |
| <input type="checkbox"/> Prospect | <input type="checkbox"/> Appartenenti all'organizzazione | <input type="checkbox"/> soci |
| <input type="checkbox"/> Pazienti | <input type="checkbox"/> Membri di organismo di amministrazione | <input type="checkbox"/> appartenenti a PA |
| <input type="checkbox"/> Cittadini | | |
| <input type="checkbox"/> Utenti | | |
| <input type="checkbox"/> Amministratori | | |
| <input type="checkbox"/> Altro _____ | | |

- **Categorie di dati personali**

- | | | |
|---|---|---|
| <input type="checkbox"/> Dati personali di identificazione | <input type="checkbox"/> Contatti sociali | <input type="checkbox"/> Dati di noleggio/locazione |
| <input type="checkbox"/> Dati di identificazione rilasciati dai servizi pubblici, diversi dal numero di identificazione nazionale | <input type="checkbox"/> Patrimonio | <input type="checkbox"/> Caratteristiche abitative |
| <input type="checkbox"/> Dati di identificazione elettronica | <input type="checkbox"/> Mandati pubblici | <input type="checkbox"/> Dati sulla salute fisica |
| <input type="checkbox"/> Dati di identificazione biometrica | <input type="checkbox"/> Incidenti | <input type="checkbox"/> Dati sulla salute mentale |
| <input type="checkbox"/> Dati di identificazione finanziaria | <input type="checkbox"/> Uso de media | <input type="checkbox"/> Dati relativi a situazioni e comportamenti a rischio |
| <input type="checkbox"/> Mezzi finanziari | <input type="checkbox"/> Descrizioni psichiche | <input type="checkbox"/> Dati genetici |
| <input type="checkbox"/> Debiti, spese, solvibilità | <input type="checkbox"/> Matrimonio o forma attuale di convivenza | <input type="checkbox"/> Curriculum accademico |
| <input type="checkbox"/> Prestiti mutui e crediti | <input type="checkbox"/> Storia civile | <input type="checkbox"/> Qualifiche professionali |
| <input type="checkbox"/> Aiuto finanziario | <input type="checkbox"/> Dettagli di altri membri della famiglia | <input type="checkbox"/> Esperienze professionali |
| <input type="checkbox"/> Dettagli assicurativi | <input type="checkbox"/> Attività ricreative e interessi | <input type="checkbox"/> Affiliazione/partecipazione a organizzazioni professionali |
| <input type="checkbox"/> Dettagli sulla pensione | <input type="checkbox"/> Affiliazioni (diverse da quelle professionali, politiche o sindacali) | <input type="checkbox"/> Pubblicazioni |
| <input type="checkbox"/> Transazioni finanziarie | <input type="checkbox"/> Dati giudiziari | <input type="checkbox"/> Lavoro attuale |
| | <input type="checkbox"/> Dati giudiziari su condanne e sentenze | <input type="checkbox"/> Curriculum vitae |
| | <input type="checkbox"/> Dati giudiziari relativi a misure giudiziarie | <input type="checkbox"/> Presenza e disciplina |
| | | <input type="checkbox"/> Medicina del lavoro |
| | | <input type="checkbox"/> Pagamenti |
| | | <input type="checkbox"/> Allenamento funzionale |
| | | <input type="checkbox"/> Sicurezza |
| | | <input type="checkbox"/> Uso di risorse del computer |
| | | <input type="checkbox"/> Numero di identificazione nazionale |
| | | <input type="checkbox"/> Dati razziali o etnici |
| | | <input type="checkbox"/> Dati sul comportamento sessuale |
| | | <input type="checkbox"/> Opinioni politiche |



- **Particolari categorie di dati**

- Dati genetici per l'identificazione univoca di una persona
- Dati biometrici per l'identificazione univoca di una persona
- Dati sulla salute
- Dati che rivelano l'origine razziale o etnica
- Dati che rivelano opinioni politiche
- Dati di geolocalizzazione
- Dati finanziari
- Dati che rivelano convinzioni religiose o filosofiche
- Dati che rivelano l'appartenenza sindacale
- Dati sulla vita sessuale o sull'orientamento sessuale
- Dati di comunicazione elettronica
- Trattamento di dati personali relativi a condanne penali e reati, articolo 10 GDPR
- Dati personali protetti dal segreto professionale
- Dati che, in generale, possono aumentare il rischio potenziale per i diritti e le libertà delle persone

- **Categorie di destinatari a cui i dati sono o possono essere comunicati**

- L'interessato
- Coloro che hanno rapporti con l'interessato
- Consulenti professionisti dell'interessato
- Datore di lavoro
- Amministrazioni pubbliche
- Altro _____
- Imprese private
- Servizi pubblici
- Servizi di giustizia e polizia
- Previdenza sociale
- Banche e compagnie assicurative
- Società di marketing
- Fornitori di servizi informatici
- Fornitori di servizi amministrativi e contabili
- Piattaforme di elaborazione

- **Denominazione dei responsabili esterni se presenti**

- **Paesi terzi o organizzazioni internazionali verso cui i dati possono essere trasferiti**



- **Indicazione garanzie adottate per il trasferimento internazionale (se applicabile)**

- | | | |
|---|---|---|
| <input type="checkbox"/> Decisione di adeguatezza | <input type="checkbox"/> Trasferimento sulla base della condizione della sezione 49.2 GDPR | <input type="checkbox"/> Trasferimento basato su esigenze giudiziarie |
| <input type="checkbox"/> Consenso dell'interessato | <input type="checkbox"/> Motivi di interesse pubblico | <input type="checkbox"/> Tutela interesse dell'interessato o di altre persone |
| <input type="checkbox"/> Regole aziendali vincolanti | <input type="checkbox"/> Conclusione o esecuzione di un contratto a favore dell'interessato | <input type="checkbox"/> Trasferimento da registro pubblico |
| <input type="checkbox"/> Clausole standard | | |
| <input type="checkbox"/> Trasferimento basato su una deroga per situazioni specifiche | | |
| <input type="checkbox"/> Altro_____ | | |

- **Periodo di conservazione dei dati (se applicabile)**

- **Descrizione generale delle misure di sicurezza organizzative adottate**

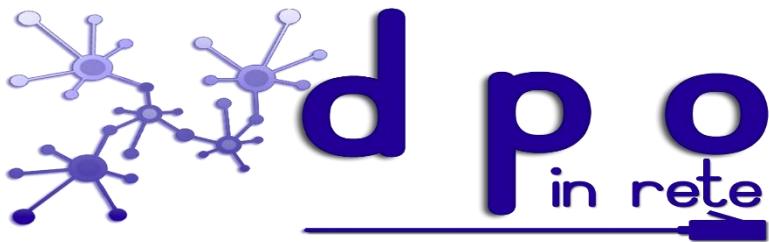
- | | |
|--|---|
| <input type="checkbox"/> Nomina per iscritto personale | <input type="checkbox"/> Procedura modifica credenziali |
| <input type="checkbox"/> Istruzioni per il trattamento | <input type="checkbox"/> Policy aziendali |
| <input type="checkbox"/> Accesso controllato | <input type="checkbox"/> Formazione |
| <input type="checkbox"/> Armadi chiusi | <input type="checkbox"/> Nomina per iscritto responsabili esterni |

- **Descrizione generale delle misure di sicurezza tecniche adottate**

- | | |
|---|--|
| <input type="checkbox"/> Autenticazione | <input type="checkbox"/> antivirus |
| <input type="checkbox"/> Autorizzazione | <input type="checkbox"/> business continuity |
| <input type="checkbox"/> Cifratura dei dati | <input type="checkbox"/> disaster recovery |
| <input type="checkbox"/> Separazione | <input type="checkbox"/> intrusion detection |
| <input type="checkbox"/> firewall | <input type="checkbox"/> vulnerability assessment/penetration test |

- **Articolo 6 (base giuridica su cui si fonda il trattamento)**

- | | |
|---|---|
| <input type="checkbox"/> Consenso dell'interessato | <input type="checkbox"/> Salvaguardia interessi vitali dell'interessato |
| <input type="checkbox"/> Esecuzione di un contratto | <input type="checkbox"/> Esecuzione compiti di interesse generale |
| <input type="checkbox"/> Esecuzione di misure precontrattuali | <input type="checkbox"/> Esercizio di pubblici poteri |
| <input type="checkbox"/> Obbligo legale | <input type="checkbox"/> Legittimo interesse del Titolare |



- **Articolo 9 (base giuridica per il trattamento di particolari categorie di dati)**

- Consenso dell'interessato
- Esercizio di obblighi in materia di diritto del lavoro
- Esercizio di obblighi in materia di protezione sociale
- Tutela interesse vitale dell'interessato
- Trattamento ex art. 9 lett d) GDPR
- Dati personali resi pubblici dall'interessato
- Trattamento in sede giudiziaria
- Trattamento per interesse pubblico rilevante
- Finalità di medicina
- Interesse pubblico per sanità pubblica
- Archiviazione nel pubblico interesse
- Ricerca storica o statistica
- Esistenza del segreto professionale

- **Tipologia d trattamento**

- Normale – nessuno dei tipi seguenti
- Processi valutativi automatizzati e sistematici o profilazione
- Decisioni automatizzate con conseguenze giuridiche
- Sorveglianza sistematica
- Elaborazione di dati su larga scala che ha conseguenze per un gran numero di parti interessate
- Monitoraggio sistematico su larga scala di un'area accessibile al pubblico
- Altro _____
- Interconnessione di raccolte di dati che le persone interessate non possono ragionevolmente prevedere
- Il trattamento di dati implica che gli interessati non possono esercitare un diritto, non possono utilizzare un servizio o non possono stipulare un contratto
- Uso di nuove tecnologie o applicazione di mezzi tecnici ed organizzativi

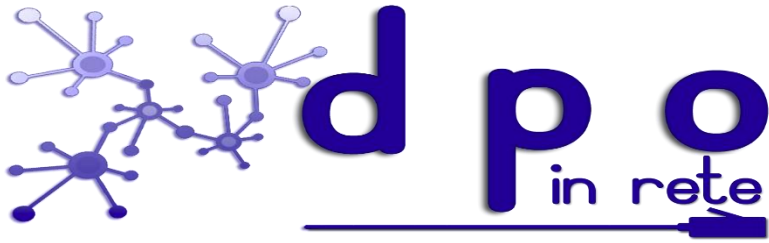
- **Fonte dei dati personali (se applicabile)**

- **Consenso degli interessati**

- Comportamentale
- Espresso
- Altro _____
- per iscritto
- documentato

- **modalità di conservazione dei dati**

- analogico
- digitale
- analogico e digitale



Il trattamento dei dati presenta un rischio elevato in quanto rientra tra le seguenti fattispecie:

- 1) Valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche

<input type="checkbox"/> Si	<input type="checkbox"/> No
-----------------------------	-----------------------------

- 2) Trattamento, su larga scala, di categorie particolari di dati personali quali l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

<input type="checkbox"/> Si	<input type="checkbox"/> No
-----------------------------	-----------------------------

- 3) Trattamento, su larga scala, di categorie particolari di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza

<input type="checkbox"/> Si	<input type="checkbox"/> No
-----------------------------	-----------------------------

- 4) Sorveglianza sistematica su larga scala di una zona accessibile al pubblico

<input type="checkbox"/> Si	<input type="checkbox"/> No
-----------------------------	-----------------------------

- 5) Altro rischio

<input type="checkbox"/> Si	<input type="checkbox"/> No
-----------------------------	-----------------------------

In seguito a quanto emerso dallo svolgimento di un pre-accertamento (pre-assessment) di impatto sulla protezione dei dati personali:

- Non si ritiene necessario provvedere ad eseguire una valutazione d'impatto sulla protezione dei dati eseguita (art. 35 GDPR)

Si ritiene necessario provvedere ad eseguire una valutazione d'impatto sulla protezione dei dati personali eseguita seguendo quanto disposto dall'art. 35 RGDP e quanto definito dalle linee guida concernenti la valutazione di impatto sulla protezione dei dati