



CORTE DEI CONTI

LINEE GUIDA SULLA
PROTEZIONE DEI DATI PERSONALI NELLA
CORTE DEI CONTI

Vers. 1.2022

Sommario

1. PREMESSA	4
1.1 La protezione dei dati personali nel GDPR e nel nuovo Codice della protezione dei dati personali	4
1.2 Scopo delle Linee guida	5
2. I Soggetti, i Ruoli organizzativi e gli Obblighi nel nuovo sistema di protezione dati personali	6
2.1 I Soggetti attivi nel GDPR	6
2.1.1 Il Titolare (<i>Data Controller</i>).....	7
2.1.2 Il Contitolare (<i>Joint Controller</i>).....	7
2.1.3 Il Responsabile del Trattamento dei Dati personali (<i>Data Processor</i>) e gli eventuali Sub-Responsabili (<i>Sub Processor</i>)	7
2.1.4 I Responsabili interni nell'organizzazione: i Designati e gli Autorizzati dal Titolare ...	7
2.1.5 Il Responsabile per la Protezione dei dati (RPD o <i>Data Processor Officer</i> - DPO)	8
2.2 I Soggetti Attivi nell'Organigramma della protezione dati della Corte dei conti.	9
2.3 Gli Obblighi dei soggetti attivi	12
2.3.1 Obblighi del Titolare	12
2.3.2 Obblighi del Responsabile del trattamento dati nel GDPR.....	13
2.3.3 Obblighi del Responsabile della protezione dati (RPD-DPO).....	15
2.4 Gli altri Soggetti della privacy	16
2.4.1 Gli Interessati al trattamento e diritti	16
2.4.1.1 <i>Il Consenso dell'Interessato al trattamento</i>	21
2.4.1.2 <i>Il Trasferimento dei dati dell'Interessato verso Paesi Extra UE</i>	22
2.4.2 Il soggetto Terzo e i Destinatari del trattamento	23
2.4.3 L'Autorità di Controllo italiana: il Garante per la protezione dei dati personali.....	23
2.4.3.1 <i>Le Sanzioni del Garante</i>	24
3. Definizioni e Principi cardine nel GDPR	25
3.1 Dati personali e relative categorie; Trattamento e base giuridica del trattamento dati nel GDPR	25
3.2 Dato Anonimo, Pseudonimizzazione, Profilazione	28
3.3 Larga scala, Violazione, Rischio, Danno.	28

3.3 I Principi del GDPR	30
4. Strumenti di Accountability.....	32
4.1 Il Registro delle attività di trattamento dei dati personali	32
4.2 Le misure di sicurezza	33
4.3 Le attività di monitoraggio	34
4.4 La Valutazione di impatto (VIA o DPIA)	35
5. La Violazione dei dati personali (personal data breach)	37
6. La protezione dei dati personali: casi particolari	40
6.1 Il trattamento dati personali nell'ambito del rapporto di lavoro	40
6.2 Il trattamento dati personali nell'emergenza sanitaria COVID-19.....	42
6.3 Il trattamento dati personali relativo alle condanne penali e in ambito giudiziario .	44
7. Entrata in vigore, pubblicità e revisione.....	46
APPENDICE 1. Formula normativa standard privacy per atti.....	47
APPENDICE 2. Esempi di Informativa	48
APPENDICE 3. Normativa con Link.....	51
Provvedimento 5 giugno 2019 recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101.....	54
Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica - 2 dicembre 2010.....	54
Parere del Garante n. 247 del 24 giugno 2021 su uno schema di regolamento recante l'individuazione dei trattamenti di dati personali relativi a condanne penali e reati e delle relative garanzie appropriate ai sensi dell'articolo 2-octies, comma 2, del Codice - 24 giugno 2021.....	54
APPENDICE 4. Il Responsabile esterno del trattamento dati ex art. 28 GDPR nella fase precontrattuale e contrattuale Raccomandazioni operative e diagramma sintetico delle attività	56
APPENDICE 5. Il Registro delle attività di trattamento	60
APPENDICE 6. Nomina Designati ex art. 2 quaterdecies GDPR - Diagramma di flusso	62
APPENDICE 7. Data Breach: il flusso di notifica - Diagramma di flusso.....	63

1. PREMESSA

1.1 La protezione dei dati personali nel GDPR e nel nuovo Codice della protezione dei dati personali

Il Regolamento generale (UE) 2016/679 sulla protezione dei dati personali (RPD, di seguito Regolamento o *GDPR*), è la realtà normativa e organizzativa con la quale tutti i soggetti, pubblici e privati, a partire dalla sua data di applicazione (25/05/2018) “sono tenuti a confrontarsi nella prassi quotidiana quando vogliono o devono trattare dati personali...imponendo di pensare in anticipo le finalità e le modalità dei trattamenti e di costruirne correttamente e in modo documentabile l’impalcatura giuridica e organizzativa” dei processi interni.

Il GDPR “si inserisce in un solco già aperto dalla direttiva comunitaria del 1995 e, in Italia, dalla legge 675/1996 seguita dal Codice del 2003”¹ (Codice in materia di dati personali – di seguito Codice o Codice privacy) rispetto al quale il legislatore italiano ha pur mantenuto la struttura, ma che ha profondamente rivisto abrogando, modificando e coordinando i contenuti alla luce del Regolamento, con il Dlgs. n. 101/2018.

La nuova disciplina poggia su un diverso approccio metodologico nel quale l’Interessato, persona fisica² i cui dati (personali) sono oggetto di trattamento, è il soggetto da tutelare nel contesto dell’economia digitale.

Infatti, l’evoluzione tecnologica ha profondamente trasformato e sviluppato le relazioni sociali e la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo, richiedendo inevitabilmente un maggiore elevato livello di protezione e un quadro giuridico più solido sotto il profilo della certezza giuridica e operativa sia per i consumatori-utenti, che per gli operatori economici e le autorità pubbliche, al fine di favorire un clima di maggiore fiducia nelle transazioni e di governo dei dati personali (*Considerando 6-7 GDPR*).

Così nel Regolamento *il diritto alla protezione dei dati personali*, conformemente alla definizione posta da documenti fondanti dell’UE³ è *un diritto fondamentale della persona di rango costituzionale*⁴ (*Considerando 1 GDPR*) ma anche una *prerogativa non assoluta, che va temperata di volta in volta “alla luce della sua funzione*

¹ Applicare il GDPR. Le linee guida Europee. 2019 – Il Garante per la protezione dei dati.

² Il Regolamento disciplina unicamente il trattamento dei dati delle persone fisiche e non di quelle persone giuridiche (*Considerando 14* GDPR).

³ Nella Carta dei diritti fondamentali dell’Unione europea (art. 16, par. 1) e nel Trattato sul funzionamento dell’Unione Europea del 2007.

⁴ In realtà di rango internazionale pattizio in quanto contenuta o richiamata nel Trattato di Lisbona” – F. Pizzetti, “Privacy e diritto europeo alla protezione dei dati personali” – 2016.

sociale...con altri diritti fondamentali, in ossequio al principio di proporzionalità”⁵ e ancora “tali dati non possono dunque essere considerati una merce”⁶.

Con il GDPR si ha un “*approccio sistemico e realistico*”⁷ proattivo e sostanziale. Si tratta dunque di un diritto vivente e non statico, che supera la previgente logica dell’adempimento formale e reattiva che caratterizzava la precedente normativa sulla privacy, e che poggia invece, oggi, su rinnovate responsabilità in capo al Titolare e al Responsabile (esterno) del trattamento, attraverso la positivizzazione del principio di *accountability* (responsabilizzazione e rendicontazione), l’adozione di misure di sicurezza a garanzia della riservatezza e tutela dei dati che agevolano comportamenti e prassi virtuosi nelle organizzazioni, ove la materia va contestualizzata con una *governance* dedicata, che ha impatto trasversale su tutti i settori e i processi gestionali organizzativi interni.

1.2 Scopo delle Linee guida

Le Linee guida sulla protezione dei dati personali della Corte dei conti intendono fornire indicazioni di base per l’acquisizione della consapevolezza:

- Sui presupposti e sui vincoli della normativa europea sui dati personali;
- Sui soggetti, i ruoli, i compiti e le responsabilità di ciascuno nei processi organizzativi interni ed esterni;
- Sugli atti e i documenti in uso, verificando l’esistenza, l’aggiornamento e la coerenza dei relativi contenuti e principi, adeguandoli a quelli del corpus normativo sulla materia, vale a dire al Regolamento, al Codice per la protezione dei dati e alle indicazioni fornite nel tempo dalle Autorità di controllo - Garanti europei e italiano - sotto forma di: Linee Guida, Provvedimenti, Pareri, Chiarimenti anche tramite FAQ, etc.

La pervasività della materia e il suo stretto collegamento con i vari ambiti dell’organizzazione determinano la necessità di valutare la protezione dei dati personali nei vari contesti (ecosistema) che poggiano sul trattamento di dati, quali, ad esempio, la trasformazione digitale, la gestione documentale e lo scambio di flussi documentali anche con altri soggetti pubblici o privati (gestione, conservazione-*storage* documentale-tempo di conservazione - *data retention* - scarto); la trasparenza, l’anticorruzione e il

⁵ Considerando 4 - Altri diritti dell’ordinamento: diritto di difesa - diritto di cronaca - diritto dell’impresa - attività di ricerca - attività di marketing - diritto alla trasparenza -legittimo interesse

⁶ Cit. 24esimo considerando della direttiva 2019/770 del 20 maggio 2019 dal Consiglio di Stato, nella sentenza 29 marzo 2021 n. 2631, che decide su appello contro la sentenza del T.A.R. Lazio, Sez. I, 10 gennaio 2020 n. 260 con la quale è stato parzialmente accolto il ricorso mosso dalla società Facebook Ireland Limited nei confronti del provvedimento dell’Autorità garante della concorrenza e del mercato AGCOM n. 27432 del 29 novembre 2018, confermando la sentenza di primo grado e in parziale accoglimento del ricorso di primo grado.

⁷ Pizzetti F., op. cit.

diritto di accesso ai documenti e ai dati; gli *open data*; le misure di sicurezza dei documenti e dei dati; i contratti di fornitura con impatto sui dati personali; i dati del personale.

I documenti e i dati che li contengono sono patrimonio e beni pubblici tutelati come culturali⁸, di valore inestimabile. Singolarmente, infatti, i dati possono in apparenza non avere significato e valore, ma una volta aggregati possono costituire un potenziale non misurabile, che richiede la maggiore protezione possibile, tenuto conto che i dati costituiscono il principale obiettivo degli attacchi ai sistemi che li contengono.

2. I Soggetti, i Ruoli organizzativi e gli Obblighi nel nuovo sistema di protezione dati personali

2.1 I Soggetti attivi nel GDPR

Il Regolamento ridisegna il ruolo, i compiti e le responsabilità dei soggetti attivi, con immediato riferimento *in primis* agli obblighi gravanti in capo al Titolare, con implicazioni di responsabilità diretta riferite a tre principali innovazioni⁹:

- 1) *assicurare costantemente di aver messo in atto le misure tecniche ed organizzative adeguate conformi al Regolamento, dimostrandolo e documentandolo (principio di accountability art. 24.1 GDPR) anche sotto il profilo dell'efficacia delle misure intraprese;*
- 2) *notificare all'Autorità di controllo (il Garante italiano per la protezione dei dati) la violazione di dati personali (personal data breach) entro 72 ore dal momento in cui ne è venuto a conoscenza (art. 33 GDPR);*
- 3) *notificare agli interessati al trattamento di dati personali la violazione, solo nel caso in cui questa sia suscettibile di presentare un rischio elevato per i loro diritti e le libertà (art. 34 GDPR).*

Poste queste premesse, derivano a cascata profili di responsabilità nei confronti di altri soggetti attivi previsti dal Regolamento.

Appare rilevante identificare tutti i soggetti attivi coinvolti nella protezione dei dati personali, dapprima analizzandoli in base alla definizione posta dall'attuale

⁸ "La normativa in materia di archivi e documenti pubblici è stata sempre ispirata al principio della salvaguardia della documentazione prodotta dalla pubblica amministrazione, tutelata come bene culturale e individuata come rappresentativa di atti o fatti giuridicamente rilevanti. L'obbligo di conservazione dei documenti d'archivio è inteso a salvaguardare diritti soggettivi, interessi legittimi, il diritto d'accesso, la ricerca a fini storici, culturali e scientifici ed è finalizzato alla fruizione dei documenti per finalità amministrative e per interesse storico" Linee guida sulla conservazione dei documenti informatici 2015 - AGID.

⁹ Pizzetti F., op.cit.

normativa, contestualizzando e identificando nel successivo paragrafo la relativa corrispondenza con i soggetti dell'organigramma privacy della Corte dei conti.

2.1.1 Il Titolare (*Data Controller*)

È *“la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali...”* (art. 4, n. 7)). I relativi obblighi sono dettagliati nel successivo par. 2.3.1.

2.1.2 Il Contitolare (*Joint Controller*)

“Allorché due o più Titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento essi sono contitolari del trattamento e determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dell'Interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14...” (art. 26 GDPR).

2.1.3 Il Responsabile del Trattamento dei Dati personali (*Data Processor*) e gli eventuali Sub-Responsabili (*Sub Processor*)

E' *«la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati per conto del Titolare»* (art. 4, n. 8) GDPR) che presenta *“garanzie sufficienti”* per mettere in atto *“misure tecniche e organizzative adeguate, nonché per garantire la tutela dell'Interessato e che non possa ricorrere ad un altro Sub-Responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare”* (art. 28.1 GDPR). I rapporti fra Titolare e Responsabile del trattamento sono condivisi e sottoscritti dal Responsabile del trattamento per accettazione nell'ambito di *“un contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il Responsabile del trattamento al Titolare e stabilisca la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e diritti del Titolare...”* (art. 28.3 GDPR). I contenuti del contratto o altro accordo scritto, corrispondono agli obblighi del Titolare, come descritti nel successivo par. 2.3.2, tenuto anche conto delle raccomandazioni operative indicate nell'Appendice 4, e del diagramma esplicativo di cui all'Appendice 7.

2.1.4 I Responsabili interni nell'organizzazione: i Designati e gli Autorizzati dal Titolare

*“Il Titolare o il Responsabile del trattamento possono provvedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente **“designate”**, che*

operano sotto la loro autorità” (art. 2-*quaterdecies* Codice Privacy Dlgs. n. 196/2003 novellato dal D.lgs. n. 101/2018). Nella relazione illustrativa al D.lgs. 101/2018, in commento all’art. 2 - *quaterdecies* è indicato che “la norma prevede il potere di Titolare e Responsabile, di delegare compiti e funzioni a persone fisiche che operano sotto la loro autorità e che, a tal fine, dovranno essere espressamente designati. Tale disposizione permette di mantenere le funzioni e i compiti assegnati a figure interne all’organizzazione che, ai sensi del previgente codice in materia di protezione dei dati, ma in contrasto con il Regolamento, potevano essere definiti, a seconda dei casi, Responsabili o Incaricati”. A norma del Regolamento, tutti i soggetti “autorizzati” al trattamento dei dati personali agiscono sotto l’autorità del Titolare o del Responsabile del trattamento e non possono accedere ai dati né li possono trattare se non siano stati istruiti dal Titolare (art. 29 GDPR).

Nella nuova disciplina non viene citato esplicitamente, ma rimane definito nella realtà privacy italiana dal Garante¹⁰ in provvedimenti tuttora vigenti e compatibili con il Regolamento, un ulteriore soggetto nel trattamento non occasionale di dati personali, il c.d. Amministratore di sistema, spesso coincidente con il Titolare del trattamento. Tale figura è concretamente operante nelle organizzazioni a garanzia del rispetto dei principi posti a tutela dei dati attraverso il costante monitoraggio dello stato di sicurezza di tutti i processi di elaborazione dati. L’Amministrazione di sistema può ricondursi ad uno o più soggetti interni all’organizzazione “autorizzati” al trattamento, oppure ad uno o più soggetti esterni nominati in qualità di Responsabili esterni del trattamento ai sensi dell’art. 28 GDPR.

2.1.5 Il Responsabile per la Protezione dei dati (RPD o *Data Processor Officer* - DPO)

È una figura nuova introdotta dal GDPR con un ruolo chiave e centrale nel monitoraggio della *governance* della protezione dei dati personali all’interno dell’organizzazione. Infatti, il DPO controlla per conto del Titolare l’applicazione interna del Regolamento e riveste una importante funzione consultiva e di raccordo tra il Titolare e l’Autorità di controllo da un lato e tra il Titolare e gli Interessati dall’altro. La relativa designazione da parte del Titolare è obbligatoria per tutte le autorità pubbliche e gli organismi pubblici, ivi comprese, per quanto riguarda l’ordinamento interno, le autorità giudiziarie¹¹ e dunque anche per la Corte dei conti.

¹⁰ “Con la definizione di amministratore di sistema si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi” <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1626595>

¹¹ Art. 2-*sexdecies* del D.lgs. n. 51/2018.

Il DPO viene designato: “...in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e della prassi in materia di protezione dei dati personali”. Può essere un dipendente del Titolare o del Responsabile del trattamento, oppure assolvere i compiti dovuti in base ad un contratto di servizi, ma deve avere una profonda conoscenza dell’organizzazione nella quale opera per poter garantire al Titolare un proficuo ed efficace assolvimento dei compiti stessi in conformità al Regolamento. I dati di contatto del DPO sono pubblici e, oltre ad essere comunicati all’atto della nomina all’Autorità Garante per la protezione dei dati personali, sono anche pubblicati sul sito istituzionale del Titolare (art. 37 GDPR). Il DPO agisce in piena indipendenza e autonomia (*Considerando 97* GDPR) e riferisce direttamente ai vertici. Può svolgere altri compiti e funzioni non in conflitto di interessi. Deve poter disporre di risorse necessarie per l’espletamento dei compiti assegnati dal Regolamento (artt. 38-39 GDPR). Gli interessati possono contattarlo per tutte le questioni relative al trattamento dei loro dati personali e all’esercizio dei loro diritti derivanti dal Regolamento (art. 38.4 GDPR). I relativi obblighi sono dettagliati nel successivo par. 2.3.3.

2.2 I Soggetti Attivi nell’Organigramma della protezione dati della Corte dei conti.

L’entrata in vigore del Regolamento ha determinato la necessità di definire una disciplina normativa interna compatibile con la nuova cornice europea: in Italia è stato adottato il d.lgs. n. 101/2018 di modifica del Codice Privacy (d.lgs. 196/2013). Conseguentemente, nelle organizzazioni, compresa la Corte dei conti, si è resa necessaria l’adozione di una articolazione organizzativa ai fini privacy per definire i soggetti attivi del trattamento dei dati personali non più compatibili con i previgenti modelli organizzativi strutturati in deleghe del Titolare a responsabili interni di trattamento ai sensi del previgente Codice privacy.

Nella Corte dei conti l’assetto organizzativo che individua i soggetti attivi del trattamento dati personali è stato definito con il Decreto Presidenziale n. 20 del 1° febbraio 2021, di cui fa parte integrante l’allegato “Organigramma della privacy della Corte dei conti ai sensi del GDPR e del Codice della protezione dei dati personali”.

L’articolazione organizzativa ai fini privacy poggia sulle seguenti premesse:

- La sussistenza di una figura unitaria del **Titolare**, corrispondente alla Corte dei conti nel suo complesso;
- La designazione di un **Responsabile protezione dati - DPO**, intervenuta da ultimo con il D.P. 121 del 17 maggio 2021, che si avvale dell’ufficio di supporto denominato “Nucleo di supporto al Responsabile per la protezione dei dati personali”;

- La designazione di soggetti interni all'organizzazione in qualità di *Designati* ex art. 2-*quaterdecies* del Codice, dei quali il Titolare si avvale per garantire la capillare applicazione della normativa negli ambiti-uffici di rispettiva competenza, individuati in relazione a trattamenti riconducibili alle seguenti funzioni omogenee: Consiglio di Presidenza; Ufficio di Gabinetto e altri uffici di supporto al Presidente; Peculiari funzioni istituzionali; Prevenzione della corruzione e della trasparenza; Sezioni Riunite in sede deliberante e consultiva; Funzioni di controllo; Funzioni requirenti; Funzioni giudicanti; Segretariato e Amministrazione attiva (art. 2, c.1, lett. a) - i) del DP n. 20 del 2021). **Ai fini degli adempimenti correlati all'aggiornamento della nomina dei soggetti designati, l'Ufficio di Segreteria del Consiglio di Presidenza avrà cura di comunicare al DPO i provvedimenti di conferimento di incarico ai magistrati delle funzioni direttive e semidirettive. Analogamente, il Servizio per la disciplina rapporto di lavoro avrà cura di comunicare al DPO i provvedimenti di conferimento di incarico ai dirigenti ed ai funzionari delle funzioni dirigenziali e di preposto (v. [flusso di comunicazione in Appendice 6](#)).**
- L'individuazione da parte dei soggetti *Designati*, mediante specifici provvedimenti, di persone *Autorizzate* ai trattamenti, che effettuano correntemente la gestione delle operazioni di trattamento sui dati personali (art. 3, c. 1, DP n. 20 del 2021), fornendo indicazioni di dettaglio, dandone contestuale informazione al Titolare e al DPO, anche nei casi di successive modifiche e/o integrazioni.

Con riferimento ai ruoli dei soggetti attivi dell'Organigramma, giova evidenziare che:

1. Il **Titolare** (*Data Controller*), corrisponde all'entità organizzativa nel suo complesso e assume le decisioni fondamentali sugli scopi e sulle modalità del trattamento dei dati. Tale impostazione è coerente con la precisazione del Garante¹² sugli enti, le persone giuridiche e le pubbliche amministrazioni articolate in direzioni generali o in sedi centrali, decentrate o periferiche (es. servizi, dipartimenti, aree anche geografiche, etc.), che sono individuate dal Garante quali "Titolari nel loro complesso" dei trattamenti ed è stata confermata in tal senso con apposito parere¹³. **La Corte dei conti ai fini della protezione dei dati personali è considerata come entità complessiva unica e dunque il Titolare è unico.**
2. Eventuali **Contitolari del trattamento** (art. 4, n. 7, e art. 26) sono più Titolari di trattamento che determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali per una data procedura o attività di trattamento, formalizzando

¹² Garante per la protezione dei dati personali, Precisazione 9 dicembre 1997, doc. web. n. 39785, confermato dal successivo del 14 giugno 2007, doc. web n. 1417809.

¹³ Parere del Garante per la protezione dei dati personali del 23 dicembre 2020 sul quesito formulato dal Presidente della Corte dei conti con nota del 21 novembre 2020.

in un accordo specifico (cd. “accordo di contitolarità”), le rispettive responsabilità ai fini dell’osservanza degli obblighi previsti dal Regolamento. Nella Corte dei conti un esempio di contitolarità è attuato con l’accordo (di contitolarità) per la gestione di alcune procedure concorsuali di reclutamento di personale da assumere presso la Giustizia Amministrativa, tra la Corte dei conti, il Consiglio di Stato e l’Avvocatura dello Stato, in cui la titolarità del trattamento è riconducibile a ciascuna di tali Amministrazioni in ambiti di specifica competenza e, per la Corte dei conti, consistono nella messa a disposizione del *Portale Concorsionline* per la gestione informatica della procedura di gestione delle domande di concorso dei partecipanti.

3. I **Responsabili per il Trattamento dei dati ex art. 28 GDPR** sono soggetti “esterni” all’organizzazione che trattano i dati per conto del Titolare, ricevendo da quest’ultimo istruzioni ad hoc. Questi non vanno confusi con i Responsabili “interni” disciplinati dal previgente Codice della protezione dei dati personali e ora riconducibili alle persone designate dal titolare. In particolare, il Responsabile per il trattamento deve essere nominato con un atto a firma del Titolare del trattamento. Attualmente, la nomina di tali soggetti avviene con un atto presidenziale di designazione del Responsabile del trattamento dati ai sensi dell’art. 28 del GDPR. A tal fine, i soggetti designati ai sensi del D.P. n. 20 del 2021, per consentire l’esatta individuazione dei compiti e delle responsabilità dei Responsabili per il trattamento dati, oltre a verificare con attenzione le eventuali clausole contrattuali che impattano sul trattamento dei dati personali (v. par. 2.3.3), dovranno comunicare i dati e le informazioni al Titolare, per il tramite del DPO, anche al fine dell’aggiornamento del Registro delle attività di trattamento (v. Appendice 5). È necessario considerare che, dalla mancata o inadeguata contrattualizzazione delle rispettive responsabilità, tra Titolare e Responsabile del trattamento, con particolare riferimento all’adozione delle specifiche misure e standard di sicurezza, può scaturire una responsabilità solidale del Titolare con il Responsabile, con eventuale azione di regresso nel caso di pagamento dell’intero risarcimento del danno¹⁴. Qualora il Responsabile del trattamento agisca senza seguire le istruzioni del Titolare, è considerato egli stesso come un Titolare autonomo¹⁵.
4. I soggetti **Designati** dal Titolare, che a loro volta procedono alla individuazione dei soggetti Autorizzati, per mezzo dei quali viene garantita una capillare applicazione del trattamento dei dati personali nell’ambito delle procedure assegnate a ciascuna articolazione organizzativa interna.

¹⁴ GDPR, art. 82.5, c.146.

¹⁵ Id. art. 28 par. 10.

5. Il **Responsabile per la Protezione dei dati personali (DPO)** dal punto di vista organizzativo della governance dei dati personali è collocato in una posizione che gli consente di esercitare, con l'autonomia e le risorse richieste per l'esercizio delle funzioni assegnate dal GDPR¹⁶, per conto del Titolare, il monitoraggio sull'apparato organizzativo tecnico configurato dal Titolare, a tutela del patrimonio informativo dell'Istituto, con particolare riferimento, in primis, ai possibili impatti che i trattamenti dei dati personali possono avere nei confronti dei soggetti Interessati, siano essi dipendenti, clienti, fornitori o altri soggetti. In tal senso, il DPO deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali, per poter supportare il Titolare nella risposta sia alle richieste dell'Autorità garante dei dati personali, sia a quelle degli Interessati anche tramite il rilascio di pareri in materia di dati personali.

Ogni informazione, consultazione e comunicazione sulla materia dei dati personali è indirizzabile al Titolare per il tramite del DPO ai seguenti indirizzi di posta elettronica:

- mail: responsabile.protezione.dati@cor-teconti.it
- pec: responsabile.protezione.dati@cor-teconticert.it .

2.3 Gli Obblighi dei soggetti attivi

Di seguito si elencano i principali obblighi che gravano in capo a ciascun soggetto attivo ai sensi della normativa privacy, la cui conoscenza è rilevante per l'esatta individuazione delle responsabilità e degli adempimenti conseguenti in ottica di responsabilizzazione e di consapevolezza diffusa.

2.3.1 Obblighi del Titolare

- Mettere in atto misure tecniche e organizzative adeguate*** (es: *pseudonimizzazione, minimizzazione*) per garantire ed essere in grado di dimostrare (*accountability-responsabilizzazione*) che il trattamento è effettuato in conformità al Regolamento (art. 24 GDPR), integrandolo delle garanzie idonee a soddisfare i requisiti richiesti da questo, a tutela dei diritti degli interessati sin dal momento della progettazione dei dati (*privacy by design*) e, successivamente, per impostazione predefinita (*privacy by default*) (art. 25 GDPR). Le misure che il Titolare deve mettere in atto devono, pertanto, considerare in via preventiva: la natura, l'ambito di applicazione, il contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche;
- Garantire che siano trattati, per impostazione predefinita solo i dati personali strettamente necessari*** per ogni specifica finalità del trattamento. Tale obbligo vale

¹⁶ GDPR, art. 39.

- per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità (art. 25 GDPR);
- c) **Tenere il Registro delle attività di trattamento svolte** sotto la propria responsabilità. Il Registro deve essere posto a disposizione dell'Autorità Garante in caso di richiesta e attività ispettive (art. 30 GDPR);
 - d) **Agevolare l'esercizio dei diritti dell'Interessato** ai sensi degli articoli da 15 a 22 GDPR (es. accesso; rettifica; cancellazione-oblio; limitazione; portabilità; opposizione) e fornire all'Interessato l'informativa in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (artt. 13 e 14);
 - e) **Designare il DPO e coinvolgerlo in tutte le questioni connesse alla protezione dei dati personali** (artt. 37-39 GDPR), assicurando che venga «tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali» all'interno dell'organizzazione (art. 38.1 GDPR);
 - f) **Dimostrare l'adozione di misure di compliance al Regolamento** (art. 24.1 GDPR) e **l'adozione misure di sicurezza** (art. 32.3 GDPR);
 - g) **Notificare all'Autorità garante la violazione dei dati personali (personal data breach)**, documentandola e, ulteriormente, comunicandola all'Interessato solo qualora sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche (artt. 33-34 GDPR);
 - h) **Effettuare la valutazione di impatto sulla protezione dei dati personali (DPIA), per i tipi di trattamento da considerare "a rischio elevato"** per i diritti degli Interessati (art. 35 GDPR);
 - i) **Effettuare costantemente un giudizio di bilanciamento** fra: il legittimo interesse del Titolare o del terzo e diritti e libertà dell'Interessato;
 - j) **Consultare l'Autorità di controllo in via preventiva, prima dunque di procedere al trattamento di dati che presentano un rischio elevato**, in assenza di adeguate misure tecniche ed organizzative (art. 36). In tale prospettiva, l'Autorità Garante per la protezione dei dati personali, assume una funzione consultiva, ma il relativo parere non si sostituisce alla valutazione di impatto svolta dal Titolare, ma la presuppone, restando in capo a questo la responsabilità di stabilire se e in che misura intraprendere un trattamento ad elevato grado di rischio nel rispetto del Regolamento.

2.3.2 Obblighi del Responsabile del trattamento dati nel GDPR

Gli obblighi previsti dal GDPR in capo al Responsabile del trattamento devono essere sempre riportati nel contratto o in altro atto giuridico di nomina, ai fini

dell'esatta identificazione delle rispettive responsabilità tra Titolare e Responsabile del trattamento. Tali obblighi consistono nel:

- a) ***Dichiarare e fornire garanzie sufficienti*** in termini di conoscenza specialistica e formazione, affidabilità e risorse sufficienti e idonee per mettere in atto le misure tecniche e organizzative previste dal Regolamento. L'eventuale l'applicazione di un Codice di condotta o di un meccanismo di certificazione approvato può essere utilizzata come elemento atto a dimostrare il rispetto degli obblighi da parte del Titolare (Considerando 81 GDPR);
- b) ***Trattare per conto del Titolare i dati soltanto su sua istruzione documentata;***
- c) ***Garantire che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale alla riservatezza;***
- d) ***Adottare e assicurare le misure di sicurezza del trattamento richieste dal Regolamento,*** con particolare riferimento all'art. 25 (protezione del dato sin falla progettazione e per impostazione predefinita) e all'art. 32 (sicurezza del trattamento). Alcune misure minime di sicurezza da riportare nel contratto quali garanzie offerte dal Titolare sono, ad esempio: la *cifratura dei dati digitali*; la *pseudonimizzazione*; la garanzia della riservatezza e integrità e qualità del dato nel tempo con riferimento ai formati; processi di gestione della struttura e del ciclo dei metadati; le modalità di selezione, di archiviazione e di scarto documentale; la disponibilità dei sistemi; le procedure per testare, verificare e valutare l'efficacia delle misure e relativo aggiornamento e monitoraggio;
- e) ***Rispettare le condizioni per ricorrere ad un Sub-Responsabile del trattamento.*** Può nominare uno o più Sub-Responsabili del trattamento *per specifiche attività di trattamento, nel rispetto dei medesimi obblighi contrattuali che legano il Titolare e il Responsabile primario.* In tali casi, le operazioni di trattamento possono essere effettuate solo da Sub-Responsabili che operano sotto la diretta autorità del Responsabile primario e che si attengono alle istruzioni impartite per iscritto da questo e previa autorizzazione scritta, specifica o generale, del Titolare;
- f) ***Assistere il Titolare in ordine alle richieste degli Interessati*** del trattamento;
- g) ***Cancellare o restituire*** tutti i dati personali trattati e rimuovere eventuali copie;
- h) ***Mettere a disposizione del Titolare e del DPO*** tutte le informazioni necessarie per dimostrare il rispetto degli obblighi e consentire le ispezioni;
- i) ***Tenere il Registro delle attività di trattamento svolte per conto del Titolare*** (art. 30, par. 2 GDPR);
- j) ***Nominare un proprio DPO,*** ove obbligatorio o comunque opportuno (art. 37);
- k) ***Collaborare alla valutazione di impatto*** (DPIA) e cooperare con l'Autorità di controllo (art. 31 GDPR);

- l) **Informare il Titolare senza ingiustificato ritardo** della violazione dei dati personali (Art. 33 GDPR);
- m) **Dichiarare eventuali trasferimenti di dati in paesi extra Ue** o organizzazioni internazionali (ove non si applica il Regolamento);
- n) **Ottemperare alla responsabilità in solido con il Titolare** per il risarcimento dei danni all'Interessato e in caso di violazione degli obblighi del Regolamento o delle istruzioni impartite dal Titolare (art. 82).

2.3.3 Obblighi del Responsabile della protezione dati (RPD-DPO)

È importante ricordare che **il Responsabile per la protezione dei dati (DPO) è una figura distinta e diversa dal Responsabile esterno del trattamento dati** esaminato nel precedente paragrafo. È obbligatoria la relativa designazione da parte del Titolare per le autorità pubbliche anche giudiziarie. Come già evidenziato, si tratta di un nuovo soggetto introdotto dal Regolamento europeo (art. 37), che gli attribuisce il ruolo sia di monitoraggio e verifica, che consultivo di supporto al Titolare o al Responsabile del trattamento nel sistema di *governance* della protezione dei dati personali, sancendone compiti e funzioni e posizione nell'organigramma privacy (artt. 38-39). Il DPO riceve direttamente dal Titolare le istruzioni in merito all'espletamento delle attività di trattamento, posto che è il Titolare, ai sensi del GDPR (art. 24) il soggetto tenuto ad *"adottare misure tecniche e organizzative per garantire e per essere in grado di dimostrare che il trattamento viene eseguito in conformità del presente regolamento"*.

Tra gli obblighi del DPO previsti dal GDPR (art. 39) sono ricompresi quelli di:

- a) **Informare e fornire consulenza** al Titolare o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- b) **Sorvegliare l'osservanza del Regolamento europeo**, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- c) **Fornire, se richiesto, un parere in merito alla valutazione d'impatto** sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
- d) **Cooperare** con l'Autorità di controllo;
- e) **Fungere da punto di contatto per l'Autorità** di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

- f) Poter *ricevere dal Titolare il compito di tenere il Registro delle attività di trattamento* di questo, che è uno degli strumenti che consentono di poter adempiere alle funzioni assegnate da questo e dal Regolamento¹⁷;
- g) Nell'eseguire i propri compiti il DPO considera debitamente *i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle relative finalità*. A tal fine, il Titolare ne assicura il tempestivo e adeguato coinvolgimento in tutte le questioni riguardanti la protezione dei dati personali (art. 38.1 GDPR).

2.4 Gli altri Soggetti della privacy

2.4.1 Gli Interessati al trattamento e diritti

«**Interessato**» è la persona fisica vivente alla quale si riferiscono i dati personali. Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, direttamente dal Regolamento (artt. 11 e 12).

Il termine per la risposta all'Interessato è, per tutti i diritti (compreso il diritto di accesso), un mese (estensibili fino a tre mesi in casi di particolare complessità), anche in caso di diniego. La risposta deve essere concisa, trasparente e facilmente accessibile e formulata utilizzando un linguaggio semplice e chiaro. Spetta al Titolare valutare la complessità del riscontro e stabilire l'ammontare dell'eventuale contributo da chiedere all'Interessato in caso di richieste manifestamente infondate o eccessive (anche ripetitive), ovvero se sono chieste più copie dei dati personali nel caso del diritto di accesso (art. 15. 3), in relazione ai costi amministrativi sostenuti. Il riscontro di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'Interessato stesso (art. 12, par. 1; art. 15, par. 3). L'Interessato che si ritenga leso nel trattamento dei propri dati personali può alternativamente ricorrere al Garante (mediante Reclamo), che decide entro 9 mesi, oppure all'autorità giudiziaria ordinaria (mediante Ricorso giurisdizionale), qualora ritenga che i diritti riconosciuti dalla normativa sulla protezione dei dati personali siano stati violati (art. 140-bis Codice protezione dati personali).

Tipologie di diritti dell'interessato:

- a) **Diritto all'informativa** (artt. 13 e 14). L'informativa è una comunicazione rivolta all'Interessato che ha lo scopo di informare il cittadino, anche prima che diventi interessato (prima che inizi il trattamento), sulle finalità e le modalità dei trattamenti svolti dal Titolare. Oltre ad essere un diritto individuale ad essere informato per

¹⁷ Linee guida del Gruppo di lavoro WP 29 sul *Data Protection Officer* adottate il 5.4.2017.

L'Interessato, corrisponde ad un dovere del di assicurare la *trasparenza e la correttezza* dei trattamenti fin dalla loro progettazione, e di essere in grado di provarlo in qualunque momento (principio di *accountability*). I contenuti dell'informativa sono elencati in modo tassativo nel Regolamento. In particolare, il Titolare deve sempre specificare i dati di contatto del DPO, la base giuridica del trattamento, qual è il suo interesse legittimo e se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferirà i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (es.: si tratta di un Paese terzo giudicato *adeguato* dalla Commissione europea; sono state inserite specifiche clausole contrattuali modello, ecc.). Ulteriori informazioni sono poi rese in quanto "*necessarie per garantire un trattamento corretto e trasparente*", come nel caso della precisazione del periodo di conservazione dei dati o, in mancanza, dei criteri seguiti per stabilire tale periodo; il diritto di presentare un reclamo all'autorità di controllo. Qualora i dati non siano stati raccolti presso l'Interessato, il Titolare deve anche precisare se sussiste un processo automatizzato ed eventuali trattamenti per finalità ulteriori, informando l'Interessato circa la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico. Il termine entro il quale il Titolare informa l'Interessato in tali ipotesi è un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati; nel caso in cui i dati personali siano destinati alla comunicazione con l'Interessato, al più tardi al momento della prima comunicazione all'Interessato. oppure, nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

b) **Diritto di accesso** (art. 15): L'Interessato ha il diritto di ottenere dal Titolare la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, l'accesso ai dati personali e alle seguenti informazioni: finalità del trattamento; categorie di dati personali; destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato; diritto di essere informato dell'esistenza di garanzie adeguate, nel caso in cui i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato

elettronico di uso comune. Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui. I Titolari possono anche consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali (Considerando 63).

c) **Diritto alla comunicazione di una violazione di dati** senza ingiustificato ritardo (art. 34). Quando la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

d) **Diritto di rettifica e di integrazione** (art. 16): L'Interessato ha il diritto di ottenere dal Titolare la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e, tenuto conto delle finalità del trattamento, il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa;

e) **Diritto di cancellazione o "oblio"** (art. 17). L'Interessato ha il diritto di ottenere dal Titolare la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il Titolare ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se: 1) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; 2) l'Interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per lo stesso; 3) l'Interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento; 4) i dati personali sono stati trattati illecitamente; 5) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare; 6) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione. Se il Titolare ha reso pubblici dati personali ed è obbligato a cancellarli per una delle ipotesi di cui sopra, adotta le misure ragionevoli, anche tecniche, tenendo conto della tecnologia disponibile e dei costi di attuazione, per informare altri Titolari che stanno trattando i dati personali della richiesta dell'Interessato di cancellare qualsiasi link, copia o riproduzione dei dati personali medesimi. Il diritto di cancellazione *non* si applica per l'Interessato nella misura in cui il trattamento sia necessario: 1) per l'esercizio del diritto alla libertà di espressione e di informazione; 2) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare; 3) per motivi di interesse pubblico nel settore della sanità pubblica; 4) per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici nella misura in cui il diritto di cancellazione rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; 5) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Il diritto all'oblio

era già¹⁸ riconosciuto dalla giurisprudenza europea quale diritto inviolabile e poi codificato nel GDPR quale diritto all'oblio generalizzato mediante cancellazione dei propri dati personali, da valutare tuttavia caso per caso, anche sulla base dei criteri, pareri e linee guida delle Autorità Garanti (europeo ed italiano). Il Garante privacy italiano è intervenuto nel tempo sul tema svolgendo alcune considerazioni in ordine, ad esempio, all'attualità delle informazioni poste su motori di ricerca¹⁹e precisando che, sebbene il trascorrere del tempo sia la componente essenziale del diritto²⁰, questo elemento incontra un limite quando le informazioni di cui si chiede la deindicizzazione siano riferite a reati gravi. A tal riguardo, la giurisprudenza ha sottolineato la necessità di valutare l'interesse pubblico, concreto ed attuale, alla menzione degli elementi identificativi delle persone protagoniste dei fatti e delle vicende oggetto di valutazione ²¹. Le fattispecie pervenute alla Corte dei conti hanno riguardato prevalentemente istanze di cancellazione dai dati in relazione a sentenze in materia di responsabilità per danno erariale. Con l'occasione sono stati ribaditi i principi giurisprudenziali sopra richiamati. In particolare, con riferimento ad una fattispecie concernente una ipotesi di responsabilità per danno all'immagine, è stato ribadito che il diritto all'oblio, secondo la giurisprudenza europea, non è un diritto assoluto, dovendo essere messo a confronto non solo con altri diritti ma anche con eventuali obblighi informativi (v. anche il comma 3 dell'art. 17 del GDPR). Sicché, nella specie, occorre confrontare il diritto all'oblio con l'obbligo generalizzato di pubblicazione delle sentenze del giudice contabile nel sistema informativo interno e sul sito istituzionale, previsto dall'art. 56 ²². E' stato quindi affermato che se ciò in generale postula che le finalità informative vadano temperate con il diritto dell'interessato ad evitare che l'indefinita permanenza su Internet di dati e informazioni risalenti nel tempo determini una lesione proprio di quei diritti che la disciplina della privacy complessivamente protegge, un corretto giudizio di bilanciamento non può prescindere nella specie da una valutazione, caso per caso, delle diverse declinazioni

¹⁸ Corte di Giustizia UE Sentenza C-131/12 del 13 maggio 2014).

¹⁹ Garante per la protezione dei dati personali, Provvedimento del 29 ottobre 2020.

²⁰ Garante per la protezione dei dati personali, Provvedimento del 6 ottobre 2016.

²¹ Corte Di Cassazione, Sezioni Unite - Sentenza 22 luglio 2019, n. 19681.

²² Art. 56 del Codice dell'Amministrazione Digitale (CAD) di cui al D.lgs. n. 82/2005 e ss.mm.ii. *Dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria di ogni ordine e grado.*"1. I dati identificativi delle questioni pendenti dinanzi al giudice amministrativo e contabile sono resi accessibili a chi vi abbia interesse mediante pubblicazione sul sistema informativo interno e sul sito istituzionale delle autorità emananti. 2. Le sentenze e le altre decisioni del giudice amministrativo e contabile, rese pubbliche mediante deposito in segreteria, sono contestualmente inserite nel sistema informativo interno e sul sito istituzionale, osservando le cautele previste dalla normativa in materia di tutela dei dati personali. 2-bis. I dati identificativi delle questioni pendenti, le sentenze e le altre decisioni depositate in cancelleria o segreteria dell'autorità giudiziaria di ogni ordine e grado sono, comunque, rese accessibili ai sensi dell'articolo 51 del codice in materia di protezione dei dati personali approvato con decreto legislativo n. 196 del 2003".

delle condotte illecite causa di responsabilità amministrativa, considerato tra l'altro l'atipicità dell'illecito amministrativo ²³;

f) **Diritto di limitazione del trattamento** (art. 18): Si tratta di un diritto esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), ma anche qualora l'Interessato chieda la rettifica dei dati (in attesa di tale rettifica da parte del Titolare) o si opponga al loro trattamento. L'Interessato ha il diritto di ottenere la limitazione del trattamento qualora: contesti l'esattezza dei dati personali, per il periodo necessario al Titolare per verificarne l'esattezza; il trattamento sia illecito e l'Interessato che ne sia limitato l'utilizzo, opponendosi alla relativa cancellazione; i dati personali siano necessari all'Interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria benché il Titolare non ne abbia più bisogno ai fini del trattamento; l'Interessato si sia opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare rispetto a quelli dell'Interessato. Se il trattamento è limitato, i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'Interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro. L'Interessato che ha ottenuto la limitazione del trattamento è informato dal Titolare prima della revoca di tale limitazione.

g) **Diritto alla portabilità dei dati** (art. 20): Si tratta di uno dei nuovi diritti previsti dal **Regolamento**, anche se non è del tutto sconosciuto agli Interessati consumatori (si pensi alla portabilità del numero telefonico). Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio. In particolare, sono portabili solo i dati trattati con il consenso dell'Interessato o sulla base di un contratto stipulato con l'Interessato. Quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del Titolare, per esempio. Il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro Titolare indicato dall'Interessato, se tecnicamente possibile, utilizzando *formati interoperabili*, che dunque i Titolari dovrebbero poter produrre (v. Considerando n. 68 GDPR e Linee-guida del Gruppo europeo WP29).

²³ Nella circostanza, i dati personali, dei quali veniva chiesta la cancellazione, si riferivano a persona condannata nel 2017 in sede di giudizio di responsabilità amministrativa per danno all'immagine. Sicché, ai fini di un corretto giudizio di bilanciamento tra le finalità informative sottese nell'obbligo di pubblicità di cui all'art. 56 del CAD e il diritto all'oblio di cui all'art. 17 del GDPR, non può non tenersi conto nella specie della natura dell'illecito (danno all'immagine), che, sostanziandosi in un pregiudizio inferto alla credibilità dell'Amministrazione, può rendere recessivo il diritto del singolo all'oblio a fronte dell'interesse pubblico a conoscere in tutti i suoi elementi (di fatto e di diritto) la riparazione che l'ordinamento ha apprestato, con le sentenze di condanna, al danno inferto alla Pubblica Amministrazione.

h) **Diritto di opposizione al trattamento** (art. 21). L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, compresa la profilazione sulla base di tali disposizioni. Il Titolare si astiene dal trattare ulteriormente i dati personali salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento prevalenti sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità. L'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici l'Interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo se il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

i) **Diritto a non subire decisioni basate unicamente su trattamenti automatizzati** (art. 22): è il diritto di non essere sottoposto a una decisione basata unicamente sul **trattamento automatizzato, compresa la profilazione, che produca effetti giuridici** che riguardano l'Interessato o che incidano in modo analogo significativamente sulla sua persona. Tale diritto *non* trova applicazione se la decisione: sia necessaria per la conclusione o l'esecuzione di un contratto tra l'Interessato e un Titolare del trattamento, ovvero se sussiste un consenso esplicito dell'Interessato e, in entrambi tali fattispecie il Titolare è tenuto ad attuare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, e almeno il diritto di ottenere l'intervento umano da parte del titolare, di esprimere la propria opinione e di contestare la decisione; sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare. Le decisioni, nelle ipotesi in cui sia escluso il diritto dell'Interessato, non si basano sulle categorie particolari di dati personali ex art. 9.1, a meno che non sia applicabile l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

2.4.1.1 Il Consenso dell'Interessato al trattamento

«**Consenso dell'Interessato**» è "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento" (art. 4, n. 11) GDPR). Il Titolare deve essere in grado di dimostrare che

L'Interessato ha prestato il consenso al trattamento dei propri dati personali. Se il consenso dell'Interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre materie, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. L'Interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'Interessato è informato della possibilità di revocarlo (art. 7 GDPR). Il Consenso deve essere, in tutti i casi, libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto. Deve essere manifestato attraverso *“dichiarazione o azione positiva inequivocabile”* ma non deve essere necessariamente documentato per iscritto, né è richiesta la forma scritta, anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere *“esplicito”* (per le particolari categorie di dati ex art. 9 GDPR)²⁴. Il Titolare deve essere in grado di dimostrare che l'Interessato ha prestato il consenso ad uno specifico trattamento (art. 7.1 GDPR). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali, in quanto è prevista una specifica base giuridica per l'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri (art. 6 GDPR).

2.4.1.2 Il Trasferimento dei dati dell'Interessato verso Paesi Extra UE

Il GDPR, rispetto ai trasferimenti dei dati personali verso Paesi terzi, ha confermato che mentre vige la più assoluta libertà di circolazione all'interno dell'UE e dello spazio economico europeo, posto sotto l'egida del GDPR, il trasferimento al di fuori di tali confini è vietato, a meno che il Titolare non possa far valere specifiche garanzie, chiarite dal Regolamento che introduce al contempo nuovi strumenti per consentire ai Titolari di procedere ai trasferimenti (mediante la certificazione o l'adesione ad un codice di condotta). Più in generale il GDPR ha reso più stringenti i requisiti che devono essere soddisfatti qualunque sia lo strumento di garanzia utilizzato per i trasferimenti di dati verso Paesi terzi, anche alla luce delle sentenze della Corte di Giustizia UE che, nel tempo, ha precisato i contorni della tutela che deve essere assicurata ad ogni dato personale quando lascia il territorio di uno Stato membro²⁵.

²⁴ Garante per la protezione dei dati personali, Guida all'applicazione del GDPR 2018.

²⁵ Garante per la protezione dei dati personali: Applicare il GDPR, le linee guida europee, pag. 350. V. anche la Sentenza della Corte di Giustizia UE *“Sentenza Schrems II”* del 16 luglio 2020 in merito al trasferimento dall'UE agli USA, relativamente alla quale la EDPB ha predisposto delle FAQ operative.

2.4.2 Il soggetto Terzo e i Destinatari del trattamento

«**Terzo**» è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'Interessato, il Titolare, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del responsabile (art. 4, punto 10) del GDPR);

«**Destinatario del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento. Il Regolamento precisa che il destinatario cui sono comunicati dati personali non deve necessariamente essere un Terzo. Pertanto, il destinatario può essere un Titolare, un Contitolare o un Responsabile del trattamento (art. 4, punto 9) del GDPR).

2.4.3 L'Autorità di Controllo italiana: il Garante per la protezione dei dati personali

L'Autorità di controllo, in Italia il **Garante per la protezione dei dati personali**, svolge le funzioni indicate nell'art. 57 GDPR, e principalmente: *sorveglia e assicura l'applicazione del Regolamento; promuove la consapevolezza dei Titolari del trattamento e dei Responsabili del trattamento riguardo agli obblighi imposti loro dal Regolamento; fornisce consulenza al Parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento; fornisce, su richiesta, informazioni all'Interessato in merito all'esercizio dei propri diritti; svolge le indagini opportune sull'oggetto del reclamo e informa il reclamante dello stato e dell'esito delle indagini; collabora, anche tramite scambi di informazioni, con le altre autorità di controllo e presta assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del regolamento; sorveglia gli sviluppi che presentano un interesse, se e in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione e le prassi commerciali; adotta le clausole contrattuali tipo; redige e tiene un elenco in relazione al requisito di una valutazione d'impatto sulla protezione dei dati; svolge indagini sull'applicazione del Regolamento, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica; incoraggia l'elaborazione di codici di condotta e l'istituzione di meccanismi di certificazione; agevola la proposizione di reclami tramite misure quali un modulo per la proposizione dei reclami compilabile anche elettronicamente, senza escludere altri mezzi di comunicazione.*

Nei casi in cui sia riscontrato un operato non conforme ai principi del GDPR, all'Autorità di controllo *sono conferiti poteri di indagine, correttivi, autorizzativi e consultivi, nonché il potere di infliggere sanzioni amministrative pecuniarie.*

Al Garante competono *attività di controllo ed ispettive*²⁶: nel corso dell'attività ispettiva, della quale può essere dato preavviso, il Garante può: *a) controllare, estrarre ed acquisire copia dei documenti, anche in formato elettronico; b) richiedere informazioni e spiegazioni; c) accedere alle banche dati ed agli archivi; d) acquisire copia delle banche dati e degli archivi su supporto informatico.*

2.4.3.1 Le Sanzioni del Garante

Le sanzioni amministrative pecuniarie devono essere effettive, proporzionate e dissuasive (art. 83 GDPR). Nel decidere se infliggere una sanzione amministrativa pecuniaria e fissare l'ammontare della stessa l'Autorità Garante tiene conto, ad esempio: della natura, gravità e durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento nonché il numero di interessati lesi dal danno e il livello del danno da essi subito; del carattere doloso o colposo della violazione; delle misure adottate dal Titolare o dal responsabile del trattamento per attenuare il danno subito dagli interessati; del grado di responsabilità del Titolare o del Responsabile del trattamento tenendo conto delle misure tecniche e organizzative messe in atto; delle eventuali precedenti violazioni pertinenti commesse dal Titolare o dal Responsabile del trattamento; il grado di cooperazione con l'Autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; le categorie di dati personali interessate dalla violazione.

Il Codice della protezione dei dati personali novellato dal D.lgs. n. 101/2018 prevede agli artt. 167-170 che siano sottoposti a *sanzioni penali* i seguenti casi:

- *trattamento illecito dei dati e comunicazione e diffusione illecita di dati personali* oggetto di trattamento su larga scala, acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala,
- *falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante, inosservanza dei provvedimenti del Garante, violazioni alle disposizioni in materia dei controlli a distanza e indagini sulle opinioni dei lavoratori.*

L'Ammontare delle sanzioni amministrative, ai sensi dell'art. 83 del GDPR è differenziato in base al tipo di violazione:

²⁶ Deliberazione del 4 aprile 2019 -Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali (G.U. n. 106 del 8 maggio 2019).

- fino a 10.000.000 euro o fino al 2 per cento del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, tra l'altro in caso di violazione di obblighi del Titolare e del Responsabile del trattamento;
- fino a 20.000.000 € o fino al 4 per cento del fatturato mondiale *totale annuo dell'esercizio precedente*, se superiore, in caso di violazione di: principi base del Regolamento, incluse le condizioni relative al consenso; diritti degli interessati; trasferimenti di dati personali a un destinatario in un Paese terzo o un'organizzazione internazionale; inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo.

3. Definizioni e Principi cardine nel GDPR

3.1 Dati personali e relative categorie; Trattamento e base giuridica del trattamento dati nel GDPR

a) **«Dato personale»:** *qualsiasi informazione riguardante una persona fisica identificata o identificabile («Interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.* Ad esempio, sono dati personali: il nome e cognome o denominazione; l'indirizzo, il codice fiscale; un'immagine, la registrazione della voce di una persona, la sua impronta digitale, i dati sanitari, attributi come file informatici, cookies e strumenti di profilazione e idonei a identificare le persone individuandone abitudini e comportamenti. Tali dati possono essere:

b) **«Dati appartenenti a categorie particolari»** corrispondono a quelli precedentemente identificati come dati sensibili nel Codice privacy previgente, quelli che *idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale.* Sono soggetti a un principio generale di divieto di trattamento, salvo alcune fattispecie tassativamente indicate (art. 9 GDPR). L'art. 2-sexies del Codice, ha specificato le ipotesi di *interesse pubblico rilevante*, ai sensi del paragrafo 2, lett. g), dell'art. 9 del GDPR, da considerarsi come base giuridica per il trattamento di tali dati, e l'art. 2-septies e ha previsto *misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute, stabilendo che tali dati, oltre a dovere essere trattati al ricorrere delle condizioni di cui al paragrafo 2 dell'art. 9 del GDPR, devono essere trattati in conformità alle specifiche misure di garanzia disposte dal Garante, da adottarsi con cadenza biennale.*

c) «**Dati relativi a condanne penali o reati**»: quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitiva, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato (art. 10 GDPR). Il trattamento di tali dati può avvenire soltanto «sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri, che preveda garanzie appropriate per i diritti e le libertà degli interessati». Inoltre, in ambito europeo il trattamento dei dati personali relativi a condanne penali e reati a titolo di prevenzione, indagine, accertamento e perseguimento di reati è disciplinato da uno strumento giuridico distinto, la direttiva 2016/680/UE, con norme specifiche di protezione dei dati vincolanti per le autorità competenti, che è attuata nell'ordinamento italiano con il D.lgs. 18 maggio 2018, n. 51.

Con riguardo a tale categoria di dati giudiziari, il Garante, ha rilasciato il Parere n. 247 del 24 giugno 2021 sullo schema di regolamento, predisposto dal Ministero della giustizia, che disciplina il trattamento dei dati giudiziari e delle relative garanzie appropriate ai sensi dell'art. 2-octies, comma 2, del Codice, ai trattamenti di dati giudiziari previsti da altre disposizioni normative che tali garanzie non prevedano. Nel Parere citato, il Garante ha evidenziato, tra gli altri, la necessità di includere, nella categoria dei "dati giudiziari" oggetto del regolamento, anche quelli relativi all'applicazione, con provvedimento giudiziale, di misure di prevenzione; l'introduzione, con lo stesso regolamento, di *garanzie appropriate (tra le quali quelle concernenti l'affidabilità delle fonti e il rispetto dei principi di proporzionalità e minimizzazione) relative ai trattamenti svolti*, sulla base di altre disposizioni normative, che tuttavia non prevedano tali garanzie; la *proporzionalità del termine di conservazione dei dati*; le peculiarità del contesto lavoristico, ai fini dell'adozione di garanzie specificamente modulate su quella realtà; la legittimazione soggettiva rispetto al trattamento; l'inclusione delle *regole deontologiche* tra i parametri da osservare anche in termini di garanzie appropriate del trattamento; la *tutela da accordare ai dati dei defunti nell'ambito dei trattamenti svolti per fini di ricerca storica*; l'esigenza di un'adeguata differenziazione, sulla base dello specifico fine perseguito, della disciplina del trattamento dei dati giudiziari per fini di archiviazione nel pubblico interesse, di ricerca storica, scientifica, o a fini statistici; l'opportunità di disciplinare anche i trattamenti svolti, rispettivamente, da soggetti no-profit, per finalità di mediazione e conciliazione delle controversie civili e commerciali, nonché per finalità di accesso a sistemi o aree sensibili, particolarmente rilevanti nel contesto socio-economico attuale.

Per i trattamenti svolti nell'ambito del rapporto di lavoro, il Regolamento esaminato delinea le condizioni e i limiti per il trattamento dei dati giudiziari, prevedendo alcune

specifiche garanzie, quale, fra le altre, l'individuazione del termine di due anni dalla cessazione del rapporto di lavoro per la conservazione dei dati, fatta salva l'esigenza di ulteriore conservazione a fini di tutela giurisdizionale dei diritti.

Per una disamina di dettaglio degli argomenti disciplinati dal Regolamento oggetto del Parere del Garante privacy, si rimanda alla lettura di quest'ultimo.

d) **«Trattamento di dati»:** *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.* La protezione dei dati personali, si applica pienamente al trattamento automatizzato di dati personali, interamente o parzialmente. Qualsiasi trattamento di dati personali attraverso mezzi automatizzati, con l'ausilio di dispositivi tecnologici ricade nella disciplina regolamentare, al pari del trattamento manuale di dati. Ad esempio, la gestione dei documenti, dei fascicoli e degli archivi digitale, ai sensi del CAD ricade nell'alveo del Regolamento al pari di quella residuale cartacea. L'Archivio è un atto di fede pubblica ed è definito dal GDPR come *qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico* (art. 4, n. 6) e dalle regole tecniche sul protocollo informatico quale *“complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività* (All. 1 DPCM 3.12.2013 sul protocollo informatico). La trattazione dei dati contenuti nei documenti a loro volta parte di un contesto archivistico correttamente gestito e ordinato anche nel contesto digitale è conforme alla tutela del patrimonio informativo e, dunque, dei dati oggetto di tutela da parte del Regolamento. Il Codice privacy disciplina in modo specifico il trattamento dei dati:

- per fini statistici o di ricerca scientifica sono oggetto di specifica disciplina (artt. da 104 a 110) oltre a quella contenuta nell'art. 83 del Regolamento, nonché nelle pertinenti Regole deontologiche del Garante del 2018 (v. Appendice normativa);
- nell'ambito del rapporto di lavoro (art, 111-113) in relazione alla promozione di regole deontologiche; per la raccolta dati e pertinenza; per i C.V. (non è dovuto il consenso nei limiti delle finalità dell'art. 6 GDPR);

e) **«Base giuridica del trattamento-liceità»:** Il Regolamento conferma che *ogni trattamento, in via preventiva, deve trovare fondamento in un'idonea base giuridica.* I fondamenti di liceità del trattamento sono indicati all'art. 6 del Regolamento e

coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy (*consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il Titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del Titolare o di terzi cui i dati vengono comunicati*). Per il trattamento dei dati di cui all'art. 9 GDPR (già dati sensibili), oltre ad individuare una corretta base giuridica, occorre fare riferimento alle eccezioni indicate nello stesso articolo.

3.2 Dato Anonimo, Pseudonimizzazione, Profilazione

- a) «**Dato anonimo**»: il dato che in origine, o a seguito di trattamento, non può essere più associato ad un Interessato identificato o identificabile (anonimizzazione, processo irreversibile);
- b) «**Pseudonimizzazione**»: è una modalità di trattamento tale che i dati personali non possano più essere attribuiti a un Interessato specifico senza l'utilizzo di informazioni aggiuntive (processo reversibile), a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e a garanzia della non riconducibilità ad una persona fisica identificata o identificabile;
- c) «**Profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

3.3 Larga scala, Violazione, Rischio, Danno.

- a) «**Larga scala del trattamento**», mira al trattamento *“di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato”* (Considerando n. 91 GDPR). I Garanti europei²⁷, hanno evidenziato sul tema che è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati coinvolti per rispondere a tutte le possibilità; ciò che invece appare possibile ed utile è individuare *alcuni standard utili a specificare* in termini più precisi o quantitativi il concetto che si sta esaminando. Risulta necessario, caso per caso, porsi alcune domande del tipo es: qual è: il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; la durata, ovvero la persistenza, dell'attività di trattamento; la portata geografica dell'attività di trattamento. Sulla base di alcuni standard si possono

²⁷ “Linee guida sui responsabili della protezione dei dati (WP243).

individuare, a titolo indicativo, i seguenti “*trattamenti su larga scala*”: quelli che interessano i dati relativi ai pazienti svolti da un ospedale nell’ambito delle ordinarie attività; quelli che interessano i dati relativi agli spostamenti degli utenti di un servizio di trasporto pubblico cittadino; il trattamento dei dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food; il trattamento dei dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell’ambito delle ordinarie attività; il trattamento dei dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale o il trattamento di dati (metadati, contenuti, localizzazione) da parte dei gestori di servizi telefonici o telematici.

b) «**Violazione dei dati personali**» (*Data Breach*): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

c) «**Rischio dei trattamenti**»: Il Titolare o il Responsabile del trattamento devono valutare i rischi inerenti al trattamento e attuare misure per limitare i rischi alla integrità, riservatezza e disponibilità dei dati (per es. con la cifratura). La valutazione del rischio (DPIA) *tiene conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale* (Considerando n. 83 GDPR). Per rischio si intende uno scenario descrittivo di un evento, variabile in base alla natura e della portata del trattamento e delle relative conseguenze, che deve essere stimato, prima di effettuare il trattamento e in modo costante, in termini di probabilità (evento -causa) e gravità dell'*impatto* (conseguenza-effetto). Ciò consente ai Titolari del trattamento, tenuto conto che, anche con l’utilizzo sempre più diffuso delle nuove tecnologie e l’accresciuta complessità dei trattamenti di identificare, affrontare e mitigare adeguatamente i rischi con anticipo, limitando significativamente la probabilità di un impatto negativo sulle persone. Ad esempio, vanno valutate le operazioni su *larga scala*, che comportano il trattamento di *particolari categorie di dati*, presentando un livello di rischio molto più elevato per gli interessati; nonché nel caso in cui il trattamento richieda una *sorveglianza sistematica su larga scala di zone accessibili al pubblico*. **La gestione del rischio non è applicabile in modo generico, ma deve essere contestualizzata ed applicata nell’ambito dello specifico trattamento del dato.** È un processo teso ad assicurare il bilanciamento tra gli impatti dovuti a minacce alle

vulnerabilità dei sistemi e dei processi, da relegare entro limiti accettabili, e i costi da sostenere, che devono essere sostenibili, approntando adeguate e specifiche contromisure e controlli (mitigazione del rischio).

d) Negli ambiti della sicurezza informatica (*security*), per rischio si intende il rischio per la sicurezza delle informazioni, e viene associato alla possibilità di minacce che possono sfruttare le vulnerabilità di una risorsa informativa o di un gruppo di risorse informative causando dei danni. Il danno fisico, materiale o immateriale descritto dal Regolamento può comportare un danno economico e sociale significativo: ad es. il furto o la usurpazione di identità; il pregiudizio di reputazione; perdite finanziarie; la decifratura non autorizzata della pseudonimizzazione; la divulgazione di dati genetici o relativi alla salute o aspetti della sfera personale.

e) «**Danno**»: *“Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare o dal responsabile del trattamento”* (Art. 82 GDPR). Il Titolare risponde per il danno cagionato dal suo trattamento che violi il Regolamento. Un Responsabile del trattamento risponde per il danno causato solo se non ha adempiuto gli obblighi del Regolamento specificatamente diretti ai Responsabili del trattamento ovvero se ha agito in modo difforme o contrario rispetto alle istruzioni del Titolare. Qualora più Titolari del trattamento o Responsabili del trattamento, oppure entrambi, siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato, ogni Titolare o Responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, a garanzia del risarcimento effettivo dell'Interessato. Il Titolare o il Responsabile del trattamento è esonerato dalla responsabilità qualora dimostri che l'evento dannoso non gli è in alcun modo imputabile.

3.3 I Principi del GDPR

Il GDPR innova la modalità di governance del trattamento dei dati personali, imponendo l'adozione di misure tecniche ed organizzative ex ante da monitorare nel tempo (*privacy by design e by default*). In questo senso **non costituisce un adempimento formale e statico, ma una materia viva e dinamica a carattere interdisciplinare** che pervade vari *ambiti*: digitalizzazione dei processi; gestione delle banche dati e gestione e conservazione documentale e relative misure di sicurezza; trasparenza amministrativa; contrattualistica; performance; rapporti di lavoro. Necessita di essere presidiata anche con valutazioni intermedie delle misure adottate (monitoraggi, audit e revisioni) per poter intercettare l'eventuale aggravamento dei rischi che può sopraggiungere in seguito ad es. ad un cambiamento di processo, di tecnologia, etc., che può incidere in maniera significativa su trattamenti mappati. Inoltre, richiede una verifica della compatibilità al GDPR in relazione a casi concreti bilanciando i vari diritti

ed interessi dei soggetti attivi e passivi coinvolti nel trattamento. Principi generali del trattamento di dati personali.

In particolare, ogni trattamento di dati personali deve avvenire nei processi interni di lavoro nel rispetto dei principi del Regolamento di seguito evidenziati (art. 5 GDPR), che il Titolare deve essere in grado di comprovare documentandoli (*accountability*):

- a) **Trattati in modo lecito, corretto e trasparente nei confronti** dell'Interessato («*liceità, correttezza e trasparenza*»). In particolare, ogni trattamento deve trovare fondamento in un'idonea base giuridica (art. 6 GDPR) e ciò si verifica: quando l'Interessato ha espresso il proprio consenso (informato) al trattamento dei propri dati per una o più specifiche finalità; quando il trattamento è necessario all'esecuzione di un contratto di cui è parte; quando il trattamento è necessario per adempiere un obbligo legale a cui è soggetto il Titolare. Infine, il trattamento è lecito quando lo stesso è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica ovvero quando è necessario per l'esecuzione di un compito di interesse pubblico o per il perseguimento del legittimo interesse del Titolare. Il principio della trasparenza è un dovere del Titolare ed un diritto dell'Interessato: devono essere trasparenti le modalità con cui sono raccolti e utilizzati i dati personali e devono essere facilmente accessibili e comprensibili le informazioni e le comunicazioni relative al trattamento (es. identità del Titolare; finalità del trattamento; diritti degli interessati).
- b) **Raccolti per finalità determinate**, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («*limitazione della finalità*»);
- c) **Adeguati, pertinenti e limitati a quanto necessario** rispetto alle finalità per le quali sono trattati («*minimizzazione dei dati*»);
- d) **Esatti e, se necessario, aggiornati**; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («*esattezza*»);
- e) **Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità** per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici («*limitazione della conservazione*»);
- f) **Trattati in maniera da garantire un'adeguata sicurezza**, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («*integrità e riservatezza*»).

4. Strumenti di Accountability

Nel Regolamento il quadro normativo è prevalentemente incentrato sui doveri e sulla responsabilizzazione del Titolare. Il Titolare determina le finalità e i mezzi del trattamento, nonché le misure di sicurezza e pur avendo maggiore discrezionalità nel decidere come conformarsi alle disposizioni del nuovo Regolamento, egli ha l'onere di dimostrare le ragioni a supporto di tali decisioni e le motivazioni per cui ritiene che le medesime siano conformi con il Regolamento (*accountability*). Spetta al Titolare bilanciare il suo legittimo interesse con i diritti e libertà dell'Interessato, ma **la responsabilizzazione** (*accountability*) non riguarda solo il Titolare, in quanto coinvolge anche i Responsabili del trattamento, il DPO e il personale che tratta dati personali. Un elemento fondamentale dell'*accountability* è la revisione continua dei processi, a dimostrazione che la materia non è un adempimento formale, ma vivente, in continuo modificarsi al mutamento dei processi lavorativi e organizzativi interni. In tal senso anche la previsione regolamentare che affida al Titolare e Responsabile il presidio continuativo della riservatezza, integrità, disponibilità, resilienza sistemi ICT (art.32.1 lett. b) e la necessità per il Titolare di dover riesaminare la valutazione di impatto almeno quando insorgono variazioni del rischio (art.35.11).

Il principio di responsabilizzazione determina un comportamento preventivo e proattivo, teso a dimostrare la conformità al GDPR senza attendere che gli interessati o le autorità di controllo intervengano evidenziando criticità nei trattamenti.

4.1 Il Registro delle attività di trattamento dei dati personali

I Titolari e i Responsabili di trattamento devono tenere un Registro delle operazioni di trattamento quale strumento fondamentale e necessario per poter effettuare ogni valutazione e analisi del rischio, che consente di disporre di un quadro aggiornato dei trattamenti in essere per l'organizzazione. I contenuti minimi del Registro sono fissati dal Regolamento. Il Registro deve avere forma scritta, anche elettronica, da utilizzare anche per provare, documentandola, l'*accountability* richiesta al Titolare e al Responsabile del trattamento e deve essere esibito su richiesta al Garante. La tenuta del Registro dei trattamenti non costituisce un adempimento formale ma è parte integrante di un sistema di corretta gestione dei dati personali. Pertanto, il Registro deve essere mantenuto aggiornato nel tempo, per consentire contestualmente di:

a) **mappare i procedimenti e i trattamenti** in essere. In tal senso il Registro consente al Titolare e al Responsabile del trattamento di essere consapevole delle tipologie di dati personali trattati al fine di monitorare e vigilare con consapevolezza rispetto alla conformità dei trattamenti al GDPR;

- b) **identificare in modo puntuale i flussi documentali e i dati** in termini di origine e forma in cui sono archiviati; di soggetti che sono autorizzati a trattarli; di dove sono archiviati e della relativa condivisione e circolazione. Si tratta di documentare-archiviare in maniera ordinata, organizzata e verificabile da terzi le informazioni relative all'adozione delle misure tecniche ed organizzative adeguate ed efficaci finalizzate ad attuare il principio di accountability;
- c) **censire le banche dati**;
- d) **pianificare e controllare le attività di trattamento dei dati personali** per garantirne l'integrità, la riservatezza e la disponibilità, riducendo i rischi di eventuali trattamenti illeciti.

Le informazioni da riportare e documentare nel Registro sono quelle minime indicate dal Regolamento per il Titolare (art. 30) e consentono allo stesso di acquisire la consapevolezza sui trattamenti svolti, identificando i flussi documentali e le responsabilità anche ai fini della determinazione dei rischi e della valutazione di impatto (DPIA).

Il Titolare della Corte dei conti, con atto n. 49/2019, ha adottato il *format standard* di rilevazione dei trattamenti in uso nella Corte, che compone il Registro delle attività di trattamento, documento obbligatorio ai sensi dell'art. 30 GRPR. Si tratta di un modello aggiornato nel tempo, la cui tenuta è stata affidata al DPO per conto del Titolare.

Il flusso di comunicazione delle attività di trattamento dei dati personali nella Corte dei conti che popolano il Registro dei trattamenti è contenuto nel diagramma esplicativo evidenziato nell'Appendice 5.

Gli Uffici della Corte sono tenuti a comunicare e a segnalare eventuali aggiornamenti rispetto alle attività di trattamento già censite nel Registro²⁸, indipendentemente dalle richieste periodiche di aggiornamento del DPO, anche richiedendo un supporto informativo, in allegato alla mail da inviare al DPO all'indirizzo: responsabile.protezione.dati@corteconti.it.

4.2 Le misure di sicurezza

Il Regolamento prevede che, nell'adozione di **misure tecniche ed organizzative** adeguate, il Titolare e il Responsabile del trattamento, tengano conto «*dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*» (art. 32.1).

Le misure tecniche adeguate ai sensi del Regolamento consistono:

²⁸ Primo censimento con mail del DPO del 16 dicembre 2019.

- nel *ridurre al minimo* il trattamento dei dati personali (minimizzazione del trattamento),
- nell'utilizzo della pseudonimizzazione e cifratura dei dati personali per realizzare la tutela fin dalla progettazione, ossia per integrare la protezione dei dati nei sistemi avanzati di trattamento (*privacy by design e by default*);
- nella capacità di assicurare su base permanente la *riservatezza, l'integrità, la disponibilità e la resilienza* dei sistemi e dei servizi di trattamento;
- nella capacità di *ripristinare tempestivamente* la disponibilità e l'accesso dei dati personali, in caso di incidente fisico o tecnico;
- disponibilità di una *procedura per testare, verificare e valutare* regolarmente l'efficacia delle misure tecniche e organizzative;
- *nell'adesione ad un codice di condotta o a un meccanismo di certificazione approvati* può contribuire a dimostrare la conformità al requisito della sicurezza del trattamento
- nell'offrire la *trasparenza sulle funzioni e il trattamento di dati personali*, consentendo all'Interessato di controllare il trattamento dei dati e al Titolare di creare e migliorare la sicurezza,
- nell'adottare misure di tipo organizzativo (es. *designazione dei Responsabili, dei Designati e Autorizzati; attività formative ed informative come l'adozione di Linee guida*); di tipo fisico (es. *ingressi controllati dei locali di custodia degli archivi*); di tipo tecniche (es. *sistema di autenticazione e di autorizzazione, antivirus, firewall, cifratura dei dati*). Al riguardo, il Garante ha precisato che dalla data di attuazione del Regolamento (25.5.2018) non potranno sussistere obblighi generalizzati di adozione di misure minime di sicurezza ex art. 33 Codice, poiché tale valutazione sarà rimessa al Titolare e al Responsabile, caso per caso, in rapporto ai rischi specificamente individuati come dall'art. 32 del Regolamento.

4.3 Le attività di monitoraggio

La conformità alla normativa sulla protezione dei dati personali è un processo dinamico e continuo, che non si esaurisce con una prima messa a punto delle attività di aggiornamento, ma presuppone *un processo di adeguamento nel tempo*. Il monitoraggio deve essere volto ad assicurare un aggiornamento del sistema di gestione privacy e della relativa documentazione (informative, atti di nomina, etc.) che tenga conto:

- *delle modifiche e delle novità normative o giurisprudenziali* in tema di diritto alla protezione dei dati e comprende anche linee guida delle Autorità europee e delle Linee Guida e pronunce del Garante per la protezione dei dati personali;
- *delle decisioni organizzative che impattano sul trattamento di dati personali* (es. modifiche nella gestione delle risorse umane; sostituzione di un fornitore; innovazioni

tecnologiche ed informative; misure di conformità a normative generali come nel caso Covid-19);

- *della necessità di formazione e aggiornamento del personale* in materia di protezione dei dati personali, organizzandosi periodicamente, previo coinvolgimento del DPO, dei corsi specialistici idonei;
- *dell'impatto multidisciplinare della materia su tutta l'organizzazione*, con la necessità che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali

4.4 La Valutazione di impatto (VIA o DPIA)

Particolare rilievo assume, nell'ambito degli obblighi gravanti sul Titolare, quello relativo all'analisi del rischio e alla valutazione dell'impatto nota anche come DPIA (*Data protection impact assessment* - art. 35 del GDPR). Si tratta di un'analisi per determinarne l'origine, la natura, la particolarità e la gravità del rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella scelta delle misure opportune da adottare per dimostrare che il trattamento dei dati personali è conforme al Regolamento. Ai fini dello svolgimento della valutazione di impatto non esiste una metodologia standard applicabile in astratto a tutti i casi, ma sussistono diverse procedure e diversi standard metodologici. Occorre sempre far riferimento alle seguenti indicazioni sul tema DPIA:

- sito web del Garante per la protezione dei dati personali sulla DPIA;
- Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati dei Garanti Europei sulla protezione dei dati personali (oggi *European Data Protection Board -EDPB*) (WP248) 2017. In particolare il Gruppo di lavoro dei Garanti ha elaborato *novi criteri* per determinare se in un caso specifico sia necessaria una valutazione d'impatto sulla protezione dei dati (valutazione o assegnazione di un punteggio; processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente; monitoraggio sistematico; dati sensibili; trattamento di dati su larga scala; creazione di corrispondenze o combinazioni di insiemi di dati; dati relativi a interessati vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo); utilizzo innovativo o applicazione di soluzioni tecnologiche o anche con particolari misure di carattere organizzativo (es. sistemi di intelligenza artificiale; utilizzo di assistenti vocali on line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità; se il trattamento in sé «impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto»). Il Gruppo ha definito una regola indicativa sul grado di rischio e DPIA in base al

quale: i trattamenti che soddisfano meno di due criteri presentano un livello di rischio meno elevato e non richiedono una DPIA; i trattamenti che soddisfano due o più criteri richiederanno la DPIA; nei casi in cui non viene raccomandato di effettuarla comunque. In ogni caso, qualora entri in uso una nuova tecnologia di trattamento dei dati, è importante che sia effettuata una DPIA e maggiore è il numero di criteri soddisfatti dal trattamento, maggiore è la probabilità che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, sia necessario effettuare una DPIA.

Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati.

La DPIA va eseguita **almeno nelle tre ipotesi seguenti** (art. 35. 4):

- *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;*
- *trattamento, su larga scala, di dati sensibili e giudiziari;*
- *sorveglianza sistematica su larga scala di una zona accessibile al pubblico.*

Una DPIA può riguardare un singolo trattamento, ma è possibile utilizzarne una unica per valutare più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi. Non è necessario, invece, condurre una DPIA per i trattamenti in corso già oggetto di una verifica del Garante, purché non siano intervenute variazioni dei rischi e modalità di gestione. Quando la DPIA è valutata come necessaria, i Titolari del trattamento devono stimare la necessità e la proporzionalità del trattamento e i possibili rischi per i diritti delle persone. In particolare, al Titolare spetta sempre:

- valutare i rischi insiti nei propri trattamenti così da individuare le situazioni in cui una determinata tipologia di trattamenti può presentare un rischio elevato;
- consultare il DPO;
- consultare del Garante, nel caso in cui la DPIA indichi che il trattamento presenti un *rischio residuo elevato*, fornendo alcune informazioni minime (responsabilità del Titolare, degli eventuali Contitolari e dei Responsabili del trattamento; finalità e i mezzi del trattamento previsto e le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati; dati di contatto del DPO, se designato; valutazione d'impatto sulla protezione dei dati; ogni altra informazione richiesta dall'Autorità di controllo);
- descrivere i contenuti minimi della DPIA (art. 35.7 GDPR);
- conservare la documentazione della DPIA riesaminandola periodicamente.

5. La Violazione dei dati personali (personal data breach)

Il GDPR definisce «violazione dei dati personali» (art. 4.12): *la violazione di sicurezza che comporta accidentalmente o in modo illecito: la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.*

Pertanto, sussistono *tre tipologie di effetti*:

- a) l'accesso e divulgazione non autorizzati che attiene alla confidenzialità delle informazioni (*confidentiality breach*)
- b) la loro distruzione, perdita, che attiene alla disponibilità (*availability breach*);
- c) dunque, la modifica non autorizzata, che attiene alla loro integrità (*integrity breach*).

Al riguardo, la posizione del Comitato dei Garanti europei (EDBP già WP) evidenziano rispetto alla violazione dei dati le seguenti caratteristiche²⁹:

- un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione,
- la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche
- la valutazione sulla "*capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*" e sulla "*capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico*". Nel valutare l'adeguato livello di sicurezza, si tiene conto, in particolare, dei rischi presentati dal trattamento che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati (art. 32 GDPR). *Una violazione dei dati personali, se non affrontata in modo adeguato e tempestivo, può, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifrazione non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica* (Considerando n. 85 GDPR). I due elementi essenziali per la valutazione della violazione sono dunque:
 - la gravità del rischio per i diritti e le libertà degli interessati,
 - la probabilità di rischio e di rischio elevato, per i diritti e le libertà degli interessati.

Le fonti normative principali di riferimento per il *data breach* sono costituite:

- *dal Regolamento: Considerando nn. 75, 76 e 85 e artt. 4.12) e 33-34;*

²⁹ Linee guida europee (WP 250 rev. 01).

- dalle Fonti europee: Linee guida sul data breach "Guidelines 01/2021 on Examples regarding Data Breach Notification" 19 gennaio 2021;
- dalle Opinioni del Comitato WP29, Opinion 3/2014; le Raccomandazioni dell'Agenzia europea per la Cybersicurezza – ENISA "For a methodology of the assessment of severity of personal data breaches (2013)".

Il Titolare deve:

- a) **documentare-registrare qualsiasi violazione** dei dati personali, comprese le circostanze, le cause, i fatti e i dati personali interessati, gli effetti e le conseguenze nonché i provvedimenti adottati per porvi rimedio. Le linee guida sul *data breach* raccomandano al Titolare di documentare anche il ragionamento alla base delle decisioni prese in risposta a una violazione. In particolare, se una violazione non viene notificata, è opportuno documentare una giustificazione di tale decisione. Tale documentazione sarà oggetto di verifica del Garante e va conservata, ma il Regolamento non definisce il relativo periodo di conservazione. Qualora tali registrazioni contengano dati personali, spetta al Titolare determinare il periodo appropriato di conservazione ed indicare la base legale per il trattamento. Il Gruppo di lavoro dei Garanti europei WP29 raccomanda al Titolare di documentare la motivazione delle decisioni prese a seguito di una violazione e qualora una violazione non sia stata notificata, raccomanda di documentare la motivazione circa tale decisione.
- b) **notificare al Garante** la violazione non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il Titolare (informato dal Responsabile del trattamento senza ingiustificato ritardo) dovrebbe notificare la violazione dei dati personali senza ingiustificato ritardo e, ove possibile, entro **72 ore dal momento in cui ne è venuto a conoscenza**, a meno che il Titolare non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica è corredata delle ragioni del ritardo e le informazioni che non sia possibile fornire contestualmente, possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo (art. 33).
- c) Il Garante ha reso disponibile nel portale dei servizi online dell'Autorità **la procedura telematica per la notificazione di un data breach**, oltre che messo disposizione un apposito strumento di autovalutazione (self assessment) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

Va anche considerato che, essendo la protezione dei dati personali una *materia dinamica*, può accadere che una situazione che inizialmente non aveva dato origine alla notifica per l'inesistenza di un rischio probabile, possa successivamente modificarsi richiedendo

una rivalutazione del rischio (es. se la chiave di cifratura risulta successivamente essere stata compromessa o essere stata esposta a una vulnerabilità nel *software* di cifratura).

d) **comunicare agli Interessati la violazione senza ingiustificato ritardo, con un linguaggio semplice e chiaro** la natura della violazione dei dati personali al fine di consentirgli di prendere le precauzioni necessarie e dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione. **La comunicazione non è dovuta se** il Titolare: ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (es. la cifratura); ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati; la comunicazione richiederebbe sforzi sproporzionati e, in tale ipotesi, si attua una comunicazione pubblica con la quale gli interessati sono informati con analoga efficacia.

e) **Qualora il Titolare non abbia ancora comunicato all'Interessato la violazione, l'Autorità dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, può richiedere che vi provveda** (art. 34.4). Il Garante ha precisato che *“Tale comunicazione, inviata anche con mezzi elettronici, dovrà essere differenziata in funzione dei rischi e delle specifiche caratteristiche che le violazioni dei dati personali in esame presentano per ciascun Interessato coinvolto e dovrà essere effettuata, senza ingiustificato ritardo, anche nei confronti di altri interessati che verranno individuati all’esito di eventuali ulteriori attività di analisi condotte”*³⁰ dal Titolare e *“Il contesto ... - che potrà essere tenuto in considerazione nel corso dell’istruttoria per valutare l’adeguatezza e la proporzionalità delle misure tecniche e organizzative – non può rilevare ai fini della valutazione del rischio per la comunicazione della violazione agli interessati ai sensi dell’art. 34 del Regolamento. Tale*

³⁰ Garante per la protezione dei dati personali - Provvedimento del 14 maggio 2020 [9344061].

valutazione, infatti, va effettuata a posteriori, sulla base degli scenari di rischio che in concreto possono verificarsi in danno dei diritti e delle libertà degli interessati.”

➤ **Nella Corte dei conti, al fine di adempiere agli obblighi previsti dal Regolamento sulla violazione dei dati personali, l’art. 3, commi 3 e 4, del D.P. n. 20/2021 prevede che:**

1. il soggetto *Designato*, qualora venga a conoscenza di una violazione di dati personali è tenuto a comunicarla al Presidente della Corte in qualità di Titolare;
2. in relazione alla violazione dei dati personali trattati in modo automatizzato sui sistemi informatici della Corte dei conti, la *notifica al Garante* (dal Titolare) avviene su motivata segnalazione del Dirigente Generale dei Sistemi Informativi Automatizzati, previa comunicazione al DPO.
3. *L’obbligo di tempestiva comunicazione* a norma del Regolamento europeo grava anche sui Responsabili del trattamento, secondo la procedura di notifica (flusso) allegata all’atto di nomina o al contratto di prestazione di servizi o fornitura.
4. Una volta ricevuta tale comunicazione, competerà al Titolare provvedere alla notifica della violazione al Garante per la protezione dei dati personali, entro il termine di 72 ore dall’avvenuta conoscenza della violazione (entro 24 ore nel caso di *cybersecurity*).

Nell’Appendice 7 sono illustrati i diagrammi di flusso per la notifica di un *data breach*.

6. La protezione dei dati personali: casi particolari

6.1 Il trattamento dati personali nell’ambito del rapporto di lavoro

Il trattamento dei dati personali nei rapporti di lavoro, come per ogni trattamento, deve essere lecito e si basa sull’esecuzione del contratto e sulla necessità di adempiere un obbligo legale del datore di lavoro.

Il GDPR ha lasciato agli Stati membri la possibilità di prevedere, con legge o nei contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell’ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto, di gestione, pianificazione e organizzazione del lavoro, parità, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro, nonché per finalità di cessazione del rapporto di lavoro (art. 89).

Gli artt. 113 del D.Lgs n. 196/2003 in materia di trattamento dei dati nel rapporto di lavoro, richiama la l. n. 300 del 20 maggio 1970 - Statuto dei lavoratori - e, in particolare l’art. 8 (Divieto di indagini sulle opinioni). Inoltre, richiama l’art. 10 del d.lgs. n. 276 del

10 settembre 2003 (Divieto di indagini sulle opinioni e trattamenti discriminatori). L'art. 114 del Codice Privacy disciplina il controllo a distanza dei lavoratori, rimandando alle garanzie previste dall'art. 4 dello Statuto dei lavoratori (a tenore del quale l'installazione di strumenti di controllo è possibile solo per esigenze organizzative e produttive, di sicurezza del lavoro e tutela del patrimonio aziendale e previo accordo sindacale (o, in mancanza, previa autorizzazione dell'Ufficio periferico del lavoro o dell'Ispettorato), peraltro non richiesto nel caso di strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e per gli strumenti di registrazione degli accessi e delle presenze; per la videosorveglianza lo Statuto prevede che le informazioni raccolte sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli); il successivo art. 115 disciplina il telelavoro, il lavoro agile, sancendo che il datore deve garantire il rispetto della personalità e della libertà del lavoratore.

Per quanto riguarda il trattamento di particolari categorie di dati, esso è autorizzato, tra gli altri, ai sensi dell'art. 9 Par.2. lett. b) del GDPR, per l'assolvimento di obblighi e l'esercizio di diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale; lett. g) per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione; lett. h) per finalità di medicina preventiva o di medicina del lavoro, la valutazione della capacità lavorativa del dipendente e, in tali casi se sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale; lett. i) per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale, il Garante ha previsto un'autorizzazione generale (n. 1/2016, n. 146/2019) per perseguire specifiche finalità.

6.2 Il trattamento dati personali nell'emergenza sanitaria COVID-19

Il Garante per la protezione dei dati personali, in merito ai diritti, deroghe e limiti in materia di protezione dei dati personali si è espresso evidenziando che: *“La gravissima emergenza che il Paese sta affrontando ha imposto l'adozione, con norme di vario rango, di misure limitative di molti diritti fondamentali, necessarie per contenere auspicabilmente, il numero dei contagi. La protezione dei dati personali – fondamentale diritto “di libertà”, sancito dalla Carta di Nizza – non poteva fare, naturalmente, eccezione, benché le limitazioni sinora adottate siano nel complesso contenute. Alcune deroghe al regime ordinario di gestione dei dati sono state previste sin dalle primissime ordinanze intervenute pochi giorni dopo la deliberazione dello stato di emergenza, con prevalente riferimento all'ambito di comunicazione dei dati sanitari. L'art. 14 d.l. 14/2020 ha sostanzialmente replicato tale disposizione, elevandone la fonte e rimarcandone il carattere temporaneo, senza tuttavia allo stato attuale riferirsi a raccolte di dati particolarmente “innovative”.*

Nuove e più invasive raccolte di dati potrebbero fondarsi su esigenze di sanità pubblica che, al pari del “soccorso di necessità” costituiscono autonomi presupposti di liceità, in presenza di una previsione normativa conforme ai principi di necessità, proporzionalità, adeguatezza, nonché del rispetto del contenuto essenziale del diritto”.

Durante la 23-esima sessione plenaria, il Comitato europeo per la protezione dei dati (European Data Protection Board- EDPB) ha adottato due Linee-guida 3/2020 sul trattamento di dati relativi alla salute per finalità di ricerca nel contesto dell'emergenza legata al COVID-19, e sull'utilizzo della geolocalizzazione e di altri strumenti di tracciamento nel contesto dell'emergenza sanitaria, chiarendo che il GDPR contiene numerose disposizioni in merito al trattamento dei dati relativi alla salute per finalità di ricerca scientifica, che trovano applicazione anche nel contesto della pandemia soprattutto per quanto concerne il requisito del consenso e le norme nazionali rispettivamente applicabili. Il Regolamento prevede la possibilità di trattare alcune categorie particolari di dati personali (come i dati relativi alla salute) se ciò risulta necessario per perseguire scopi di ricerca scientifica.

In ossequio al *principio di minimizzazione*, in virtù del quale il trattamento dei dati personali non deve comportare la rilevazione di dati eccedenti le finalità perseguite e, in particolare, di dati inerenti la condizione sanitaria dell'interessato³¹, si è espresso favorevolmente il Garante con il Parere del 9/6/2021, in merito ai profili di compatibilità con la normativa privacy dello schema di DPCM che ha introdotto la Piattaforma nazionale *Digital Green Certificate* (“Piattaforma nazionale - DGC” o anche “PN-DGC”) per l'emissione, rilascio e verifica delle certificazioni verdi Covid-19 (EU

³¹ Il Garante per la protezione dei dati personali risponde ad alcuni quesiti sul green pass – [link](#).

Digital COVID Certificate, già Digital Green Certificate), tenuto conto della specifica integrazione di valutazione di impatto relativa alle nuove funzionalità del sistema di allerta Covid-19 e dell'App Immuni connesse al recupero, da parte degli interessati, delle certificazioni verdi Covid-19, e dei dettagli esplicativi contenuti nei documenti tecnici esplicativi allegati (dati trattati; funzioni, servizi e regole di rilascio; struttura dell'identificazione univoco; modalità di autenticazione e fruizione della certificazione; misure di sicurezza).

Con il successivo Parere del 31/8/2021, il Garante si è espresso favorevolmente sullo schema di D.P.C.M. che ha introdotto modalità semplificate di verifica del possesso delle certificazioni verdi COVID 19 da parte del personale scolastico³², alternative a quelle ordinarie attraverso l'app VerificaC19, disponendo, nell'ambito di uno specifico allegato tecnico, le *“Modalità di interazione tra il Sistema informativo dell'istruzione-Sidi e la Piattaforma nazionale-DGC per il controllo semplificato del possesso della certificazione verde Covid-19 da parte del personale scolastico”*.

Il d.l. 21 settembre 2021, n. 127, recante *“Misure urgenti per assicurare lo svolgimento in sicurezza del lavoro pubblico e privato mediante l'estensione dell'ambito applicativo della certificazione verde COVID-19 e il rafforzamento del sistema di screening”* ha introdotto dal 15 ottobre fino al 31 dicembre 2021, tra le altre: disposizioni di disciplina delle certificazioni verdi in ambito lavorativo pubblico, la cui verifica è demandata ai datori di lavoro nei confronti del personale delle amministrazioni pubbliche e dei *“soggetti che svolgono, a qualsiasi titolo, la propria attività lavorativa o di formazione o di volontariato presso le amministrazioni di cui al comma 1, anche sulla base di contratti esterni, con verifica per tali soggetti, del rispetto delle prescrizioni previste nel decreto, “anche dai rispettivi datori di lavoro”*. (art. 1, commi 1 e 2); l'utilizzo delle certificazioni verdi da parte dei magistrati ordinari, amministrativi, contabili e militari, e per i componenti delle commissioni tributarie negli uffici giudiziari e, laddove le disposizioni siano compatibili anche nei confronti dei magistrati onorari, con verifica dei requisiti da parte dei *“responsabili della sicurezza delle strutture in cui si svolge l'attività giudiziaria”* (art. 2). Il decreto ha previsto l'adozione di linee guida per l'omogenea definizione delle modalità organizzative per le verifiche del rispetto delle prescrizioni, da emanarsi con dPCM, su proposta dei Ministri per la pubblica amministrazione e della salute.

³² Cfr. D.P.C.M. 10 settembre 2021 (G.U. n.217 del 10-9-2021, recante *“Modifiche al decreto del Presidente del Consiglio dei ministri del 17 giugno 2021, recante «Disposizioni attuative dell'articolo 9, comma 10, del decreto-legge 22 aprile 2021, n. 52, “Misure urgenti per la graduale ripresa delle attività economiche e sociali nel rispetto delle esigenze di contenimento della diffusione dell'epidemia da COVID-19”*” e il D.l. 10 settembre 2021, n. 122, recante *“Misure urgenti per fronteggiare l'emergenza da COVID-19 in ambito scolastico, della formazione superiore e socio sanitario-assistenziale”*.

A tal proposito, il Garante per la protezione dei dati personali ha reso il Parere del 12 ottobre 2021 sul dPCM (12 ottobre 2021) che ha introdotto nuove modalità di verifica del *green pass* in ambito lavorativo pubblico e privato, indicando che tale attività non deve comportare la raccolta di dati dell'interessato in qualunque forma, ad eccezione di quelli strettamente necessari, in ambito lavorativo, all'applicazione delle misure derivanti dal mancato possesso della certificazione. In tal senso, il sistema utilizzato per la verifica del *green pass* non deve conservare il QR code delle certificazioni verdi sottoposte a verifica, né estrarre, consultare registrare o comunque trattare per altre finalità le informazioni rilevate. Il Garante ha anche richiamato la necessità che il personale interessato dal processo di verifica delle certificazioni verdi venga opportunamente informato dal proprio datore di lavoro sul trattamento dei dati *“attraverso una specifica informativa, anche mediante comunicazione resa alla generalità del personale, in conformità agli artt. 5, par. 1, lett. a), 13 e 14 del Regolamento e all'art. 17-bis, comma 5, del d.l. 17 marzo 2020, n. 18 (art. 1, comma 1, lett. r), dello schema)”*.

6.3 Il trattamento dati personali relativo alle condanne penali e in ambito giudiziario

Il Regolamento prevede che il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, par. 1, debba avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Il trattamento di dati personali relativi a condanne penali e a reati o a collegate misure di sicurezza è consentito solo se autorizzato da una norma di legge o di regolamento nei casi previsti dalla legge, che prevedano garanzie appropriate per i diritti e le libertà degli interessati e, in mancanza di queste, il trattamento deve essere autorizzato da uno specifico decreto del Ministro della giustizia sentito il Garante privacy (art. 2- *octies* del Codice Privacy).

Il trattamento dei dati personali per ragioni di giustizia e di controllo effettuato dai Magistrati, nell'esercizio dell'attività giurisdizionale (giudicante e requirente) e di controllo, è autorizzato senza necessità di specifico provvedimento al trattamento dei dati personali (artt. 4 e 5 del D.P. n. 20/2021).

Con riguardo alla pubblicazione delle sentenze, l'art 52 Codice Privacy prevede che per motivi legittimi l'interessato possa chiedere che - prima che sia definito il relativo grado di giudizio, con richiesta depositata nella cancelleria o segreteria dell'ufficio che procede - sia apposta a cura della medesima cancelleria o segreteria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di

riproduzione della sentenza o provvedimento in qualsiasi forma, l'indicazione delle generalità e di altri dati identificativi dell'interessato riportati sulla sentenza o sul provvedimento. Su tale richiesta l'autorità che pronuncia la sentenza o adotta il provvedimento provvede in calce con decreto, senza ulteriori formalità. La medesima autorità può disporre d'ufficio che sia apposta l'annotazione di che trattasi, a tutela dei diritti o della dignità degli interessati. In tali fattispecie, all'atto del deposito della sentenza o provvedimento, *“la cancelleria o segreteria vi appone e sottoscrive anche con timbro la seguente annotazione, recante l'indicazione degli estremi del presente articolo: 'In caso di diffusione omettere le generalità e gli altri dati identificativi di...’*”. Sull'anonimizzazione il Garante per la protezione dei dati personali si è pronunciato nel 2010 con le *“Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica”*. Inoltre, in occasione della Relazione annuale 2020, il Garante ha ribadito³³ - richiamando le *Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati* (Provvedimento 15 maggio 2014, n. 243) che, *“laddove l'amministrazione riscontri l'esistenza di un obbligo normativo che impone la pubblicazione dell'atto o del documento sul proprio sito web istituzionale, essa deve selezionare i dati personali da rendere pubblici, verificando caso per caso se ricorrono i presupposti per l'oscuramento di determinate informazioni in conformità al principio di minimizzazione dei dati quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o altre modalità che permettano di identificare l'interessato solo in caso di necessità (art. 5, par. 1, lett. c), del RGPD)*. Pertanto, anche in presenza degli obblighi di pubblicazione ai sensi del d.lgs. n. 33/2013, i soggetti chiamati a darvi attuazione non possono comunque rendere *“intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione”* (art. 7-bis, comma 4, d.lgs. n. 33/2013). Le medesime considerazioni valgono altresì in merito agli obblighi derivanti dall'art. 124, d.lgs. n. 267/2000, invocato per giustificare la pubblicazione di taluni degli atti amministrativi nella sezione Albo pretorio del sito web istituzionale, atteso che anche a tali pubblicazioni si applicano i limiti sopra menzionati con riguardo al rispetto del principio di minimizzazione dei dati e alle cautele da adottare nel caso in cui gli atti da pubblicare contengano dati appartenenti a categorie particolari o giudiziari. La pubblicazione della determinazione, con il previo oscuramento dei dati relativi all'interessato, non avrebbe peraltro compromesso il principio di adeguata motivazione di cui all'art. 3, l. n. 241/1990, poiché la versione integrale della determinazione sarebbe in ogni caso restata agli atti dell'amministrazione, accessibile, da parte di soggetti qualificati, nei modi e nei limiti previsti dalla legge” e ha ribadito che *“le informazioni relative a vicende connesse alla commissione di reati o a procedimenti penali che interessano una persona fisica sono soggetti al regime*

³³ Cfr. Relazione annuale 2020, pagg. 174-175.

di cui all'art. 10 del RGPD, senza che rilevi la circostanza che tali informazioni non contengano riferimenti agli specifici reati commessi e allo stato in cui si trovino i procedimenti penali in questione”.

7. Entrata in vigore, pubblicità e revisione

Le presenti Linee Guida entrano in vigore dal giorno della pubblicazione sul sito internet e sul sito internet della Corte dei conti e ne viene data ampia diffusione interna.

Le Linee Guida saranno aggiornate periodicamente, anche in relazione all'entrata in vigore di nuove disposizioni con impatto significativo sulla materia della protezione dei dati personali.

APPENDICE 1. Formula normativa standard privacy per atti

Nel raccomandare l'adeguamento ai riferimenti corretti della normativa applicabile alle singole fattispecie da trattare all'interno dei documenti in uso (atti normativi; circolari interne; linee guida; contratti, convenzioni e altri atti a rilevanza interna ed esterna), viene di seguito illustrato l'esempio della corretta indicazione della formula normativa standard sulla protezione dei dati personali, chiedendo alle strutture l'aggiornamento del caso.

Tale formula necessiterà di essere dettagliata caso per caso, con il riferimento puntuale richiamo specifico ed articolato normativo applicabile alla fattispecie concreta da trattare (es. articolo, paragrafo/comma, punto, lettera, del GDPR o del Codice; Linee guida del Garante sulla materia; etc.) nel caso in cui questa riguardi la conformità di specifiche procedure o processi o attività alla normativa sulla protezione dei dati personali.

A tal fine, nell'Appendice 2 sono riportati i link ipertestuali per ricerca rapida delle norme più rilevanti sulla materia.

Nelle more di aggiornamenti e formulazioni standard nel tempo forniti dal DPO della Corte dei conti, tutti gli Uffici sono tenuti comunque a verificarne l'attualità ed ad aggiornarla, anche chiedendo un supporto del DPO mediante mail a: responsabile.protezione.dati@corteconti.it.

In un preambolo normativo:

Tenuto conto che, Visto, In conformità al, Ai sensi del...

1) Formula essenziale:

il Regolamento (UE) 2016/679 (Regolamento o GDPR) e il D.lgs. del 30 giugno 2003, n. 196 recante il Codice in materia di protezione dei dati personali (Codice Privacy), come modificato e integrato dal D.lgs. n. 101/2018.

2) Formula estesa:

Corpus normativo sulla protezione dei dati personali e, in particolare: il Regolamento (UE) 2016/679 (Regolamento o GDPR) e il D.lgs. del 30 giugno 2003, n. 196 recante il Codice in materia di protezione dei dati personali (Codice Privacy), come modificato e integrato dal D.lgs. n. 101/2018; le Linee Guida e le Opinioni, Indicazioni, Pareri delle Autorità Garanti Europee sulla protezione dei dati personali (European Data Protection Board - EDPB); le Linee guida, i Provvedimenti; i Pareri, i Chiarimenti anche in forma di FAQ, nel tempo emanati dall'Autorità Garante per la protezione dei dati personali.

APPENDICE 2. Esempi di Informativa

Il modello proposto che segue è meramente indicativo e va adattato/completato dai singoli Uffici della Corte dei conti in relazione alle tipologie di trattamento effettuate, come censite nel Registro delle attività di trattamento.

Viene proposta sia una versione sintetica che una versione estesa.

In caso di necessità di supporto è possibile contattare il DPO all'indirizzo mail: responsabile.protezione.dati@corteconti.it .

a) Informativa: versione sintetica

<p><i>Informativa sul trattamento dei dati personali ex art. 13</i> del Regolamento (UE) 679/2016 (General Data Protection Regulation - GDPR)</p>
<p>In relazione al trattamento relativo a _____, le categorie di dati personali trattati (v. nota n. 34 _____), relativi alle seguenti categorie di Interessati (v. nota n. 35 _____) non saranno oggetto di diffusione a terzi, ma potranno essere comunicati alle Autorità sanitarie competenti, sulla base della normativa di settore. La Corte dei conti, in qualità di Titolare del trattamento, conserverà i dati personali comunicati dagli Interessati, che saranno trattati in modalità mista, analogica e digitale, in un arco temporale non superiore rispetto a quello strettamente necessario per il conseguimento delle finalità per i quali sono raccolti. I diritti degli Interessati previsti dal GDPR, nel Capo III dagli artt. 15-23, potranno essere esercitati contattando il Titolare e/o il DPO mediante una mail a: responsabile.protezione.dati@corteconti.it .</p>

b) Informativa: versione estesa

<p><i>Informativa sul trattamento dei dati personali ex art. 13</i> del Regolamento (UE) 679/2016 (General Data Protection Regulation - GDPR)</p>
<p>In relazione al trattamento dei dati (descrizione sintetica dell'oggetto oggetto del trattamento), la Corte dei conti è il Titolare del trattamento dei dati personali ("Titolare"), ai sensi dell'art. 4 par. 1, lett.f) del Regolamento (UE) 679/2016 (GDPR o Regolamento).</p> <p><u>Base giuridica, liceità del trattamento</u></p> <p>La base giuridica del trattamento dei dati personali è³⁴ _____ al quale è soggetto la Corte dei conti in particolare _____ ai sensi del _____</p> <p><u>Tipi di dati trattati , finalità del trattamento, categorie di dati trattati e categorie di Interessati soggetti al trattamento</u></p>

³⁴ es. l'adempimento di un obbligo legale ai sensi dell'art. 6, par. 1, lett. e) "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri cui è investito il Titolare

Il trattamento dei dati personali nella procedura svolta ai sensi del _____, comprenderà i soli dati personali necessari per il trattamento delle attività connesse a _____³⁵ e riguarderà le seguenti categorie di interessati³⁶: _____

Modalità del trattamento

Il trattamento sarà svolto, mediante strumenti informatici, da dipendenti e collaboratori a ciò autorizzati, che operano secondo le istruzioni impartite dal Titolare, con sistemi strettamente correlati alle finalità indicate e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati personali trattati.

Sono adottate specifiche misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o di perdita, anche accidentale, dei dati oggetto di trattamento, di accesso non autorizzato, di trattamento non consentito o non conforme rispetto alle finalità indicate nella presente informativa.

Periodo di conservazione dei dati

I dati oggetto di trattamento saranno conservati per un periodo di tempo strettamente necessario e connesso all'esecuzione del procedimento³⁷. Il Titolare provvederà, una volta concluso il procedimento, a adottare misure preordinate alla cancellazione o all'anonimizzazione dei dati che non debbano essere conservati per specifici obblighi di normativi.

Categorie di destinatari di comunicazioni

I dati personali dell'interessato potranno essere comunicati e trattati da dipendenti e collaboratori della Corte dei conti a ciò autorizzati, nell'ambito delle rispettive competenze. Al di fuori di tali casi, i dati personali non saranno comunicati, diffusi, ceduti o comunque trasferiti a terzi per scopi illeciti o non connessi alle finalità della raccolta e, in ogni caso, senza rendere idonea informativa agli interessati e acquisirne il consenso, ove richiesto dalla Legge. Resta salva l'eventuale comunicazione dei dati su richiesta dell'Autorità Giudiziaria, nei modi e nei casi previsti dalla legge. I dati personali non saranno trasferiti all'estero, verso Paesi o Organizzazioni internazionali non appartenenti all'Unione Europea che non garantiscono un livello di protezione adeguato, riconosciuto, ai sensi dell'art. 45 GDPR, sulla base di una decisione di adeguatezza della Commissione UE. I dati personali non saranno sottoposti a processi automatizzati relativi alle persone fisiche, né a profilazione (art. 22 GDPR).

Diritti dell'interessato

A norma del Regolamento, l'interessato ha il diritto di accedere ai propri dati personali e di ottenere: 1) l'aggiornamento, la rettifica o l'integrazione dei propri dati; 2) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione alle finalità del trattamento; c) la limitazione del trattamento, quando ricorre una delle ipotesi di cui all'articolo 18 GDPR; 3) che il Titolare comunichi a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche, cancellazioni o limitazioni, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato; 4) la trasmissione dei dati che lo riguardano, forniti al Titolare e trattati sulla base del consenso espresso dall'interessato per una o più specifiche finalità, in un formato strutturato, di uso comune e leggibile da dispositivo automatico. Ai sensi dell'art. 20 del GDPR, l'interessato ha, inoltre, il diritto di trasmettere tali dati a un altro Titolare del trattamento senza

³⁵ Descrivere il trattamento e i tipi di dati trattati (es. se particolari categorie di dati) e se ad es. si utilizzano videoriprese.

³⁶ Descrivere i soggetti interessati (es. dipendenti, collaboratori, stagisti, volontari, dipendenti di imprese esterne, e tutte le persone che accedono ai locali aziendali per lo svolgimento di un'attività lavorativa, etc.).

³⁷ Indicare, qualora esattamente conosciuto, il tempo di data retention-conservazione.

impedimenti e, se tecnicamente fattibile, di ottenere la trasmissione diretta dei dati personali da un Titolare del trattamento all'altro; 5) qualora il trattamento sia basato sul consenso, revocare il proprio consenso in qualsiasi momento (ex art. 7, par. 3 GDPR).

L'interessato ha diritto di opporsi, in tutto o in parte al trattamento dei propri dati personali: a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; b) a processi decisionali automatizzati che incidano significativamente sulla sua persona.

Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato ha il diritto di proporre reclamo e/o segnalazione a un'Autorità di controllo.

Esercizio dei diritti

I diritti di cui sopra, ovvero la richiesta di maggiori informazioni sulle finalità e sulle modalità di trattamento dei dati personali, possono essere richiesti con richiesta rivolta al Titolare e/o al DPO contattabili ai seguenti indirizzi: PEC: responsabile.protezione.dati@cor-teconticert.it, Posta elettronica: responsabile.protezione.dati@cor-teconti.it . Per proporre un reclamo l'interessato può rivolgersi all'Autorità Garante per la protezione dei dati personali, consultando il sito web all'indirizzo <http://www.garanteprivacy.it/> .

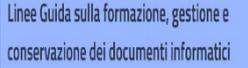
APPENDICE 3. Normativa con Link

<p>EUR-Lex L'accesso al diritto dell'Unione europea</p>	
<p>Regolamento UE sulla Protezione dei dati Personali (General Data Protection Regulation-Regolamento o GDPR)</p>	 <p>Reg UE 679/2016</p>
<p>Codice della Protezione dei dati personali (Codice privacy)</p>	 <p>Dlgs. n. 196/2013, come modificato dal D.Lgs. 101/2018 a seguito dell'entrata in vigore del Regolamento Europeo 679/2016 (testo coordinato)</p>
<p>Trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.</p>	 <p>D.lgs. n. 51/2018 Attuazione della Direttiva relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati</p>
<p>Contratti di fornitura di contenuto digitale e di servizi digitali</p>	 <p>DIRETTIVA (UE) 2019/770 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali</p>
 <p>Il Comitato europeo per la protezione dei dati-European Data Protection Board - EDPB (già WP29)</p>	 <p>Linee guida dei Garanti Europei su varie materie della protezione dei dati personali.</p>
<p>Trasparenza e privacy</p>	 <p>Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017 As last Revised and Adopted on 11 April 2018</p>
<p>Governance dei dati</p>	 <p>Data Governance ACT (proposta 2020) (5)...”L'idea che i dati generati a carico dei bilanci pubblici dovrebbero apportare benefici alla società in generale è da molto tempo parte delle politiche dell'Unione. La direttiva (UE)</p>

		2019/1024 e la legislazione settoriale garantiscono che il settore pubblico renda facilmente disponibile per l'utilizzo e il riutilizzo una quota maggiore dei dati che produce. Spesso talune categorie di dati (dati commerciali riservati, dati statistici protetti dal segreto, dati protetti da diritti di proprietà intellettuale di terzi, compresi segreti commerciali e dati personali non accessibili sulla base di una specifica legislazione nazionale o dell'Unione, quali il regolamento (UE) 2016/679 e la direttiva (UE) 2016/680) non sono tuttavia messe a disposizione..."
Valutazione di impatto - DPIA		Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati a rischio elevato (WP248)
Dispositivi video		Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video
Geolocalizzazione e strumenti di tracciamento		Linee-guida 3/2020 sul trattamento di dati relativi alla salute per finalità di ricerca e Linee-guida sulla geolocalizzazione e altri strumenti di tracciamento, nel contesto dell'emergenza legata al COVID-19
		Linee-guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19
Notifica data breach		Linee guida in materia di notifica delle violazioni di dati personali (<i>data breach notification</i>) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679
Responsabile e Incaricato del trattamento		WP29, Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento" (WP169).
Clausole contrattuali tipo		Il comitato europeo per la protezione dei dati e il Garante europeo per la protezione dei dati adottano pareri congiunti su nuove clausole contrattuali tipo 15 gennaio 2021

		OPINIONE n. 14/2019 in merito alla proposta di clausole contrattuali dell'autorità di controllo danese.
Trasferimento dati verso paesi extra UE		FAQ Domande frequenti sulla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 - Data Protection Commissioner/Facebook Ireland Ltd e Maximilian Schrems (24 luglio 2020)
Intelligenza Artificiale		Linee guida UE sull'intelligenza artificiale. White Paper on Artificial Intelligence: a European approach to excellence and trust (19 febbraio 2020).
		Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO sui principi etici per lo sviluppo, la diffusione e l'utilizzo dell'intelligenza artificiale, della robotica e delle tecnologie correlate 20 ottobre 2020
		Guida del Garante per la protezione dei dati personali all'applicazione del GDPR 2018
Regole deontologiche		Regole deontologiche in materia di dati personali
Coronavirus e protezione dei dati personali		Coronavirus e protezione dei dati: documenti e approfondimenti
		Covid-19, test sierologici sul posto di lavoro: i chiarimenti del Garante privacy
Rapporto di lavoro pubblico		Linee guida 14/06/2007 in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico
Trasparenza		Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati - 13 maggio 2014

<p>Particolari categorie di dati</p>	 <p>Provvedimento 5 giugno 2019 recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101</p>
<p>Anonimizzazione Trattamento dati relativi a condanne penali e reati</p>	 <p>Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica - 2 dicembre 2010</p>  <p>Parere del Garante n. 247 del 24 giugno 2021 su uno schema di regolamento recante l'individuazione dei trattamenti di dati personali relativi a condanne penali e reati e delle relative garanzie appropriate ai sensi dell'articolo 2-octies, comma 2, del Codice - 24 giugno 2021</p>
<p>Green Pass</p>	 <p>GreenPass: Provvedimenti del Garante, comunicati stampa e documenti</p>  <p>GreenPass: il Garante risponde ad alcuni quesiti</p>  <p>Parere sul DPCM di attuazione della piattaforma nazionale DGC per l'emissione, il rilascio e la verifica del Green Pass - 9 giugno 2021 [9668064]</p>  <p>Parere sullo schema di decreto concernente Misure recanti modifiche ed integrazioni alle disposizioni attuative dell'articolo 9, comma 10, del decreto-legge 22 aprile 2021, n. 52, recante "Misure urgenti per la graduale ripresa delle attività economiche e sociali nel rispetto delle esigenze di contenimento della diffusione dell'epidemia da COVID-19" - 31 agosto 2021. Registro dei provvedimenti n. 306 del 31 agosto 2021</p>  <p>Parere sullo schema di Dpcm che introduce nuove modalità di verifica del green pass in ambito lavorativo pubblico e privato 11 ottobre 2021</p>

<p>Tutti i Provvedimenti</p>	 <p>Tutti i Provvedimenti del GARANTE per area tematica</p>
<p>Deep Fake</p>	 <p>Il vademecum del Garante -<i>Deepfake</i>. Il falso che ti "rub" la faccia (e la privacy)</p>
	 <p>Piano Triennale per l'informatica nella PA</p>  <p>Linee Guida sulla formazione, gestione e conservazione dei documenti informatici</p> <p>Linee Guida Sulla Conservazione Dei Documenti Informatici</p>
	 <p>D.P n. 20/2021 approvazione dell'Organigramma privacy nella Corte dei conti</p>  <p>Organigramma Privacy della Corte dei conti</p>  <p>Manuale di gestione documentale della Corte dei conti - Protocollo informatico e conservazione</p>  <p>Linee guida sull'utilizzo delle risorse informatiche 2018 - DGSIA/CUS.</p>

APPENDICE 4. Il Responsabile esterno del trattamento dati ex art. 28 GDPR nella fase precontrattuale e contrattuale Raccomandazioni operative e diagramma sintetico delle attività

Come descritto nel paragrafo 2.3.2 , per la Corte dei conti i Responsabili esterni per il trattamento dei dati personali ai sensi dell'art. 28 GDPR aderiscono, sottoscrivendolo, ad un contratto o altro atto scritto giuridicamente rilevante. Spetta al Presidente della Corte dei conti, quale Rappresentante legale della Corte dei conti, designare e firmare l'atto di nomina del Responsabile del trattamento, che sottoscriverà per accettazione.

Nella fase precontrattuale e comunque preventiva alla sottoscrizione di un contratto di fornitura, si raccomanda di *verificare*:

- ❖ la sussistenza almeno degli obblighi per il Responsabile esterno al trattamento indicati nell'art. 28 GDPR, nonché di quelli riportati nel par.2.3.2 suddetto;
- ❖ la presenza, nella documentazione precontrattuale, di clausole di esonero anche parziale di responsabilità del fornitore sfavorevoli per l'amministrazione, tenuto conto della sussistenza di responsabilità del fornitore in solido con il Titolare per il trattamento dati nell'ambito della fornitura, nel caso di risarcimento dei danni all'Interessato e in caso di violazione degli obblighi del Regolamento o delle istruzioni impartite dal Titolare, ai sensi dell'art. 82 GDPR. Tale attenzione dovrebbe essere posta in particolare, con riferimento alla presenza della clausola per la quale qualunque sia la finalità e la durata del trattamento effettuato da parte del Responsabile, i dati rimarranno sempre e comunque di proprietà esclusiva del Titolare e, pertanto, che i dati non potranno essere ceduti, in tutto o in parte, ad altri soggetti e dovranno essere restituiti dal Titolare alla conclusione o revoca dell'incarico, o in qualsiasi momento il Titolare ne faccia richiesta, nonché che qualunque sia la finalità e la durata del trattamento effettuato dal Responsabile, lo stesso si impegna a non vantare alcun diritto sui dati e sui materiali presi in visione. Inoltre, che una volta cessati i trattamenti oggetto del Contratto, salvo rinnovo, il Responsabile si impegna a restituire al Titolare i dati personali acquisiti o pervenuti a sua conoscenza in relazione all'esecuzione del servizio prestato, cancellandoli allo stesso tempo dai propri archivi oppure distruggendoli, ad eccezione dei casi in cui i dati debbano essere conservati in virtù di obblighi di legge; che non sia presente per il Responsabile del trattamento la possibilità, vietata dal Regolamento, che vengano inviati messaggi pubblicitari, commerciali e promozionali, e comunque di contattare gli "interessati" per finalità diverse da quelle indicate nel contratto o altro atto; che sia verificata la possibilità di nominare *Sub-Responsabili* da parte del Responsabile del trattamento che il Titolare volta per volta dovrà autorizzare singolarmente, prevedere un'autorizzazione generale da parte del Titolare nei

confronti del Responsabile primario. In tal caso, l'elenco dei *Sub-Responsabili* dovrebbe essere incluso anche solo in appendice al contratto e dovrebbe essere costantemente aggiornato³⁸. Infine, che nessun dato personale possa essere trasferito verso Paesi extra europei o Organizzazioni internazionali (art. 44 GDPR), anche per il tramite di eventuali *Sub-Responsabili*, senza la preventiva e documentata autorizzazione scritta del Titolare. Qualora tale autorizzazione fosse concessa, l'attività di trasferimento dei dati personali oggetto del trattamento dovrà essere comunque disciplinata da uno specifico accordo giuridico concluso tra le Parti contenente le "Clausole Contrattuali Standard europee". Nel caso in cui il Responsabile si avvalga di un *Sub-Responsabile* anche le intese contrattuali intercorrenti tra dette parti dovranno essere conseguentemente integrate con la previsione delle "Clausole Contrattuali Standard europee", in modo che i medesimi obblighi incombenti sul Responsabile siano previsti anche in capo al *Sub-Responsabile* che effettua il trasferimento di dati;

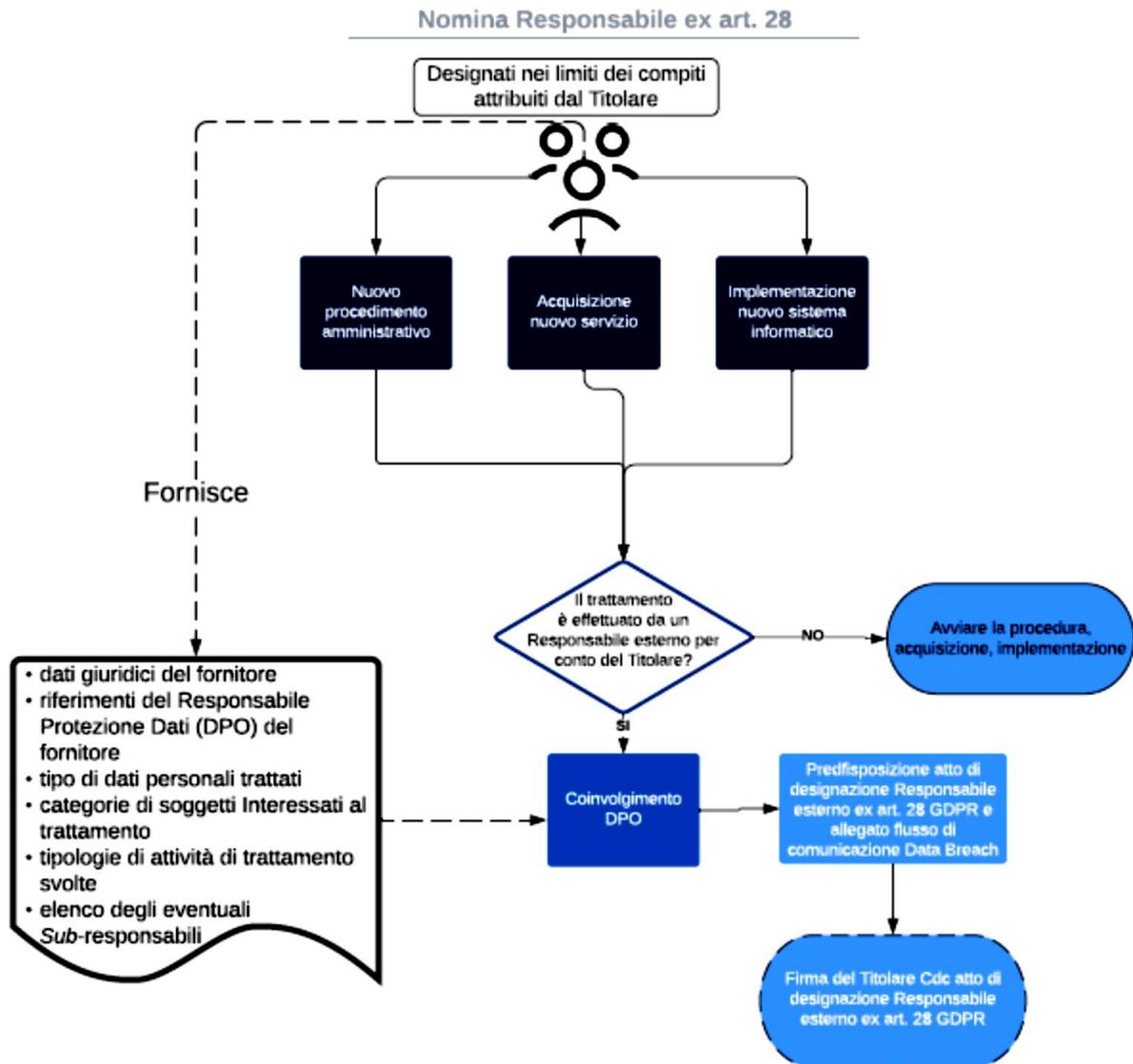
- ❖ l'eventuale adesione del fornitore a codici di condotta approvati o certificazioni per dimostrare la conformità al GDPR (artt. 41 e 42);
- ❖ per le forniture IT es. piattaforme: la presenza di SLA (livelli di servizio), da allegare ai contratti di fornitura, su: accessibilità alle piattaforme; modalità di ripristino; tempistiche di assistenza (e risoluzione) in caso di problemi di utilizzo; livelli di utilizzabilità della piattaforma e verifica di eventuali rallentamenti nella fornitura del servizio; livelli di servizio sul mantenimento dei dati (e documenti) e verificare le eventuali delimitazioni dell'indennizzo - ammissibilità anche in caso di colpa grave o violazione di misure adeguate di sicurezza ex art. 32 GDPR);
- ❖ l'attualità di format/modelli standard contrattuali già in uso all'interno o all'esterno dell'amministrazione, e la presenza di riferimenti e clausole conformi ed aggiornate al GDPR e al Codice della protezione dei dati personali mantenendoli aggiornati;
- ❖ che il fornitore abbia diretta e approfondita conoscenza degli obblighi che si assume in relazione a quanto disposto dal Regolamento e, più in generale, dalle Norme in materia di protezione dei dati personali;
- ❖ che il fornitore tratti i dati personali ponga in atto le misure tecniche ed organizzative necessarie al trattamento dei dati personali, attenendosi alle istruzioni di carattere generale nonché a ogni altra istruzione documentata impartita dal Titolare in materia di sicurezza dei dati personali (by design e by default ex art. 32 GDPR) al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato e di trattamento non

³⁸ Cfr. Comitato Europeo e Garanti europei - Pareri congiunti su nuove clausole contrattuali tipo del 15 gennaio 2021 e Opinione n. 14/2019 dell'European Data Protection Board-EDPB in merito alla proposta di clausole contrattuali dell'autorità di controllo danese.

consentito o non conforme alla raccolta e nel flusso di comunicazione delle eventuali violazioni dei dati personali, oltre che al rispetto della normativa vigente e ai provvedimenti dell'Autorità Garante dei dati personali (<https://www.garanteprivacy.it/>).

- ❖ Comunicare al DPO della Corte dei conti via mail (responsabile.protezione.dati@corteconti.it), anche allegando il contratto o altro atto giuridico di riferimento, per consentire la predisposizione dell'atto di designazione a Responsabile esterno ex art. 28 GDPR:
 - ✓ i dati giuridici del fornitore: Nome o Ragione sociale; Sede legale; Codice Fiscale/Partita Iva; il Legale rappresentante: (Nome, Cognome, CF);
 - ✓ i dati (nome e cognome; dati di contatto) del Responsabile Protezione Dati -DPO del fornitore;
 - ✓ il tipo di dati personali trattati:
 - ✓ Dati personali comuni: PRECISARE (es. anagrafici, fiscali);
 - ✓ Dati personali specifici: PRECISARE (es dati di profilazione; dati che consentono geolocalizzazione; audio/video/foto);
 - ✓ Particolari categorie di dati: PRECISARE (es. stato di salute, caratteristiche fisiche, assistenza sanitaria, genetici, biometrici);
 - ✓ Le categorie di interessati dei dati personali trattati: precisare (es. utenti, personale della Corte, altri soggetti);
 - ✓ Le tipologie di attività di trattamento svolte, anche al fine della successiva conciliazione tra i rispettivi Registri delle attività di trattamento dei dati personali;
 - ✓ L'Elenco degli eventuali Sub-responsabili e i dati di contatto, nominati dal Responsabile principale e le tipologie delle sub-attività affidate nell'ambito del trattamento dati principale di riferimento, ricevendo l'autorizzazione del Titolare per i Sub-Responsabili nominati successivamente alla sua nomina a Responsabile del trattamento ai sensi dell'art. 28 GDPR. In tale caso, il Titolare provvederà a rilasciare specifica autorizzazione ai Responsabile a nominare il fornitore quale Sub-Responsabile tenendo conto che l'adempimento alle prescrizioni del Regolamento, ivi incluse quelle relative alle misure di sicurezza ed alla privacy by default e by design da parte del Sub-Responsabile, saranno attuate sulla base delle condizioni e dei termini per la protezione dei dati personali stabilite da quest'ultimo.

Di seguito, il diagramma esplicativo delle attività di nomina del Responsabile ex art. 28 del GPPR:



APPENDICE 5. Il Registro delle attività di trattamento



Il Titolare della Corte dei conti, con atto n. 49/2019, ha adottato *il format standard* di rilevazione dei trattamenti in uso nella Corte, che compone il Registro delle attività di trattamento, quale documento obbligatorio ai sensi dell'art. 30 GRPR.

Il Format è un modello aggiornato nel tempo, la cui tenuta è stata affidata al DPO per conto del Titolare.

Gli Uffici della Corte dovranno segnalare eventuali aggiornamenti rispetto alle attività di trattamento già censite nel Registro, indipendentemente dalle richieste periodiche di aggiornamento del DPO, anche richiedendo un supporto informativo, richiedendo il format con mail da inviare al DPO all'indirizzo: responsabile.protezione.dati@cor-teconti.it

 **Registro dei trattamenti della Corte dei Conti**

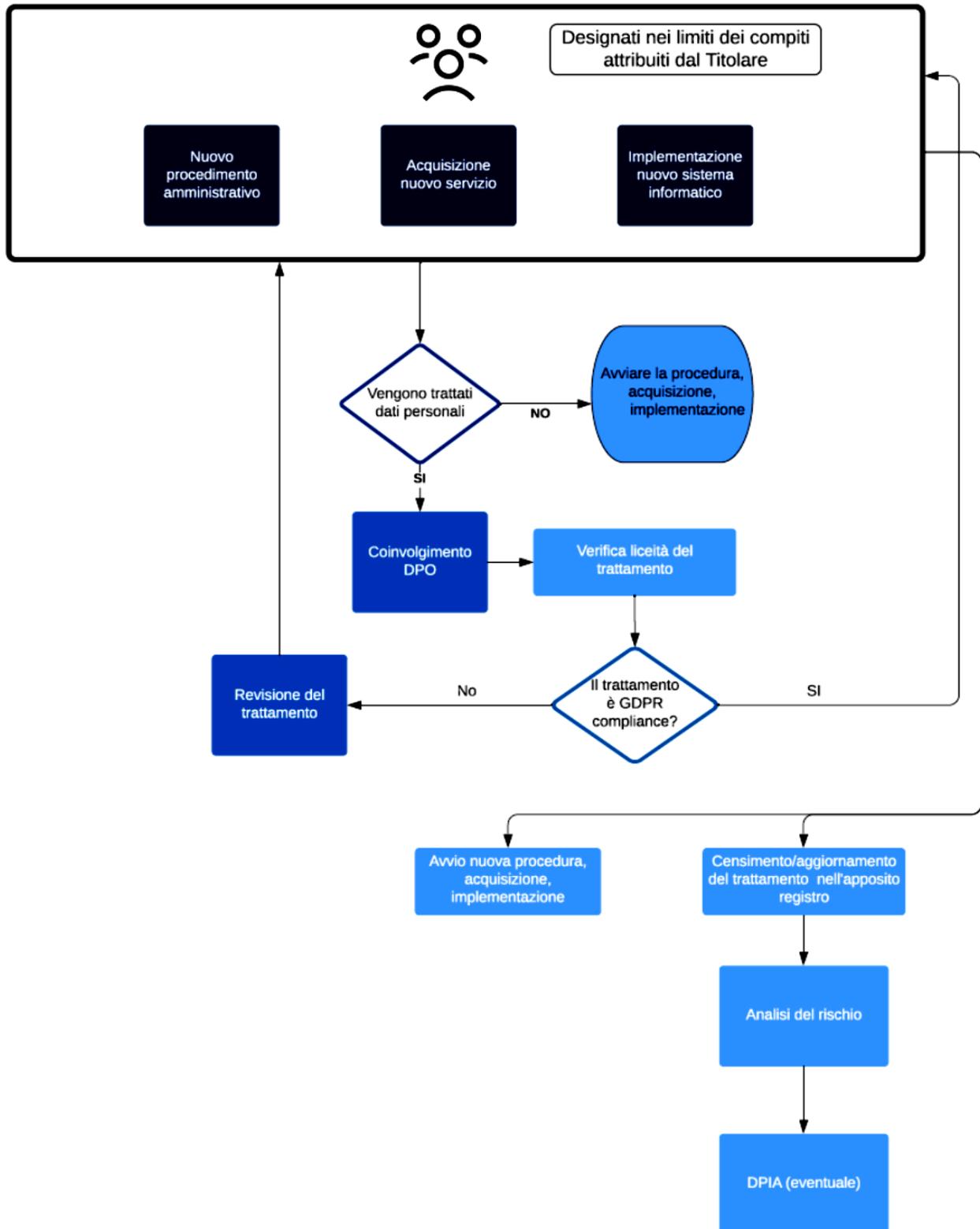
TITOLARE DEL TRATTAMENTO: La Corte dei conti rappresentata dal Presidente Guido Carlino - sede via Antonio Baiamonti, 25 00195 Roma- tel. 06/38762005 email: responsabile.protezione.dati@cor-teconti.it

RESPONSABILE DELLA PROTEZIONE DEI DATI: Cons. Luisa D'Evoli - Largo Don Giuseppe Morosini, 1- 00195 Roma Tel: 0638764782 pec: responsabile.protezione.dati@cor-teconticert.it - nominata con D.P. 39

Nome del trattamento	Descrizione del trattamento	Informazioni sulla Struttura Referente del trattamento					Tipologia di trattamento	Modalità di trattamento (selezionare da menu a tendina)	Finalità	Descrizione finalità	Fondamenti di liceità (selezionare da menu a tendina)	Descrizione fondamenti di liceità	Categoria di interessati dal trattamento	Categoria di personali trattati (selezionare da menu a tendina)
		REFERENT E del trattamento	DESIGNAT O DAL TITOLARE	Nome struttura per esteso	Segno della Struttura	Descrizione della Struttura (selezionare da menu a tendina in basso alla cella o descrivere nel campo bianco)								
							Recalco;		Il registro di protocollo è un atto pubblico di fede privilegiata, strumento finalizzato		D.lgs. n. 422/05 - Codice Amministrazione Digitale o Ragole	La categoria di interessati sono: il personale di manutenzione		

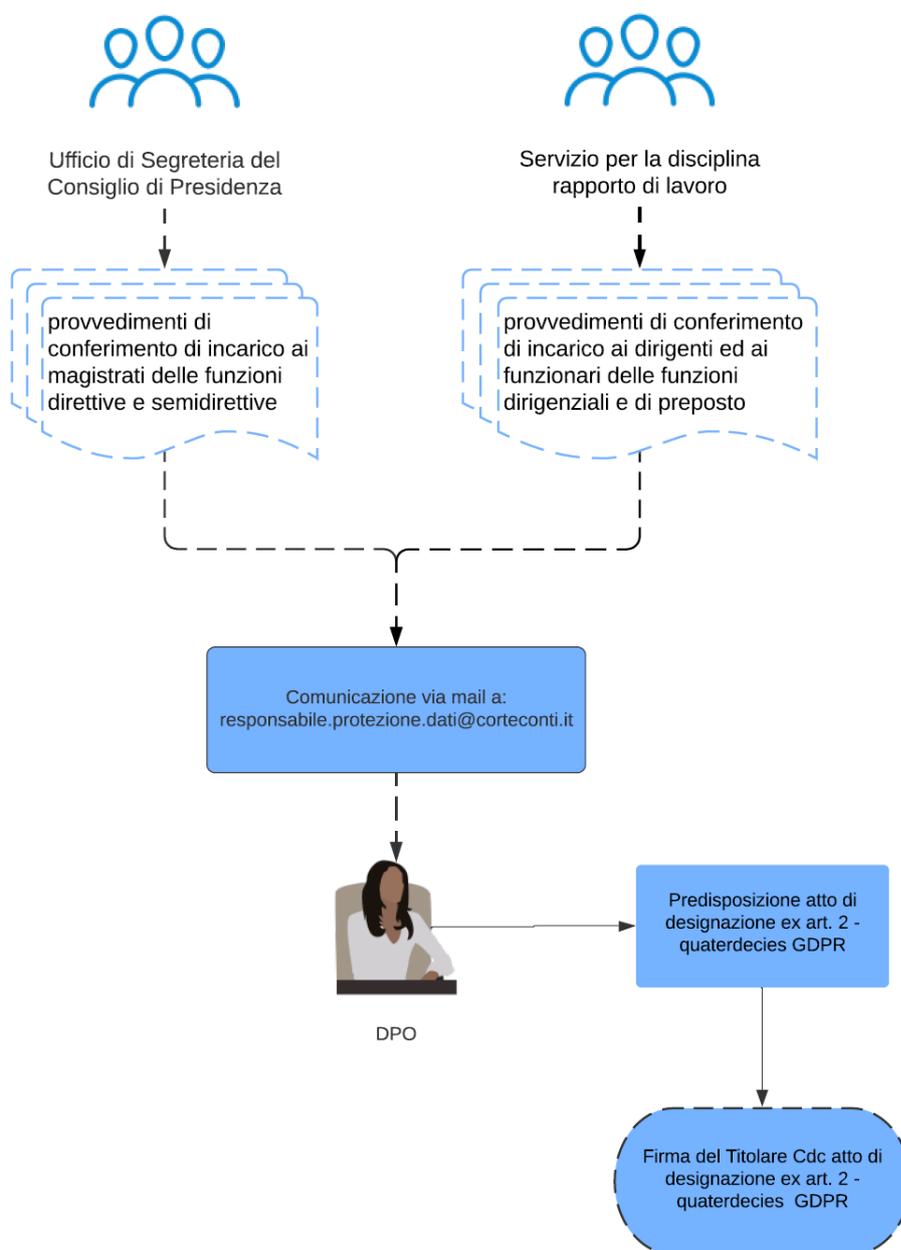
Di seguito, il diagramma esplicativo del flusso di popolamento/aggiornamento del Registro dei trattamenti:

Popolamento-aggiornamento Registro dei trattamenti



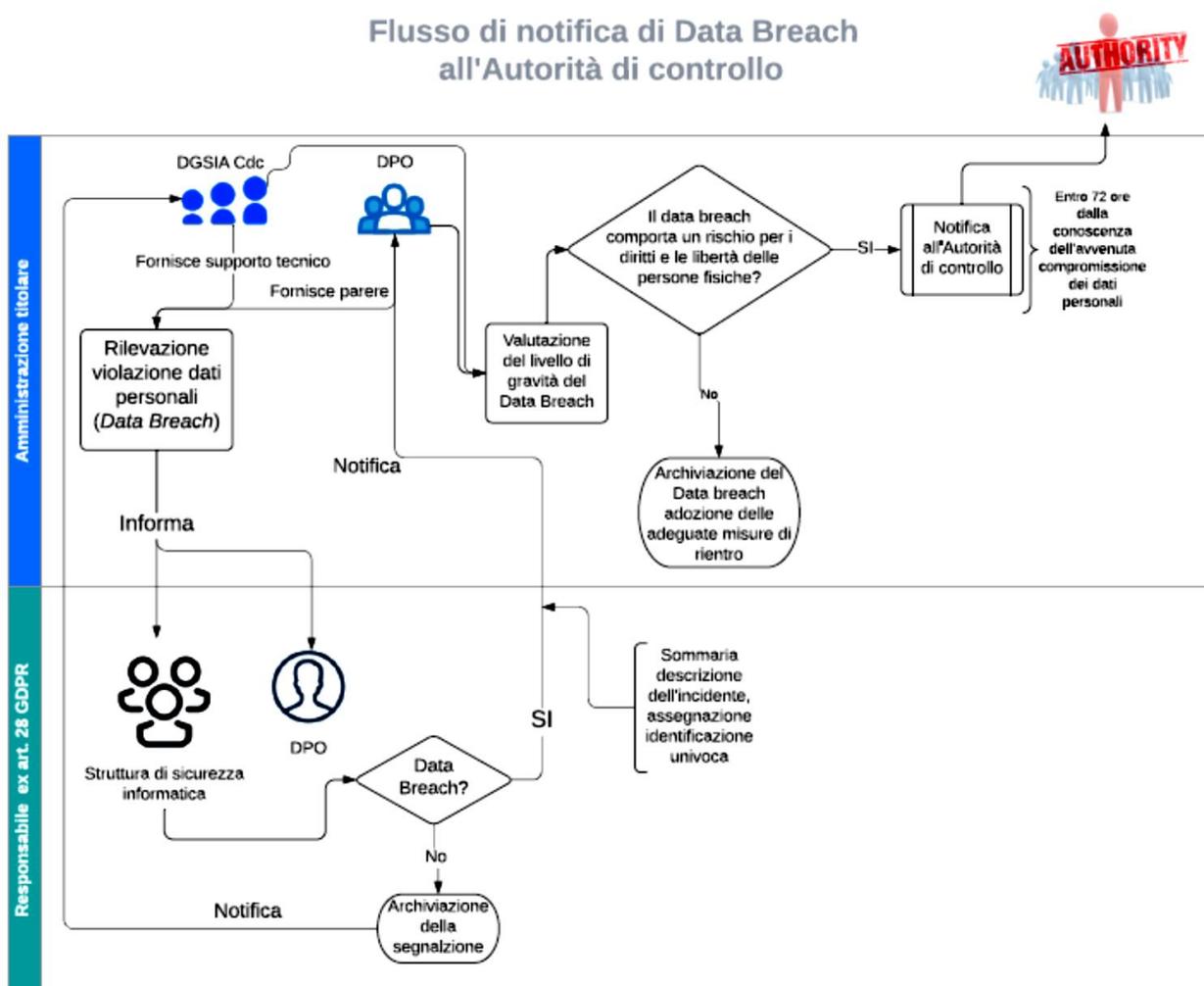
APPENDICE 6. Nomina Designati ex art. 2 quaterdecies GDPR - Diagramma di flusso

Nomina Designati ex art. 2- quaterdecies GDPR

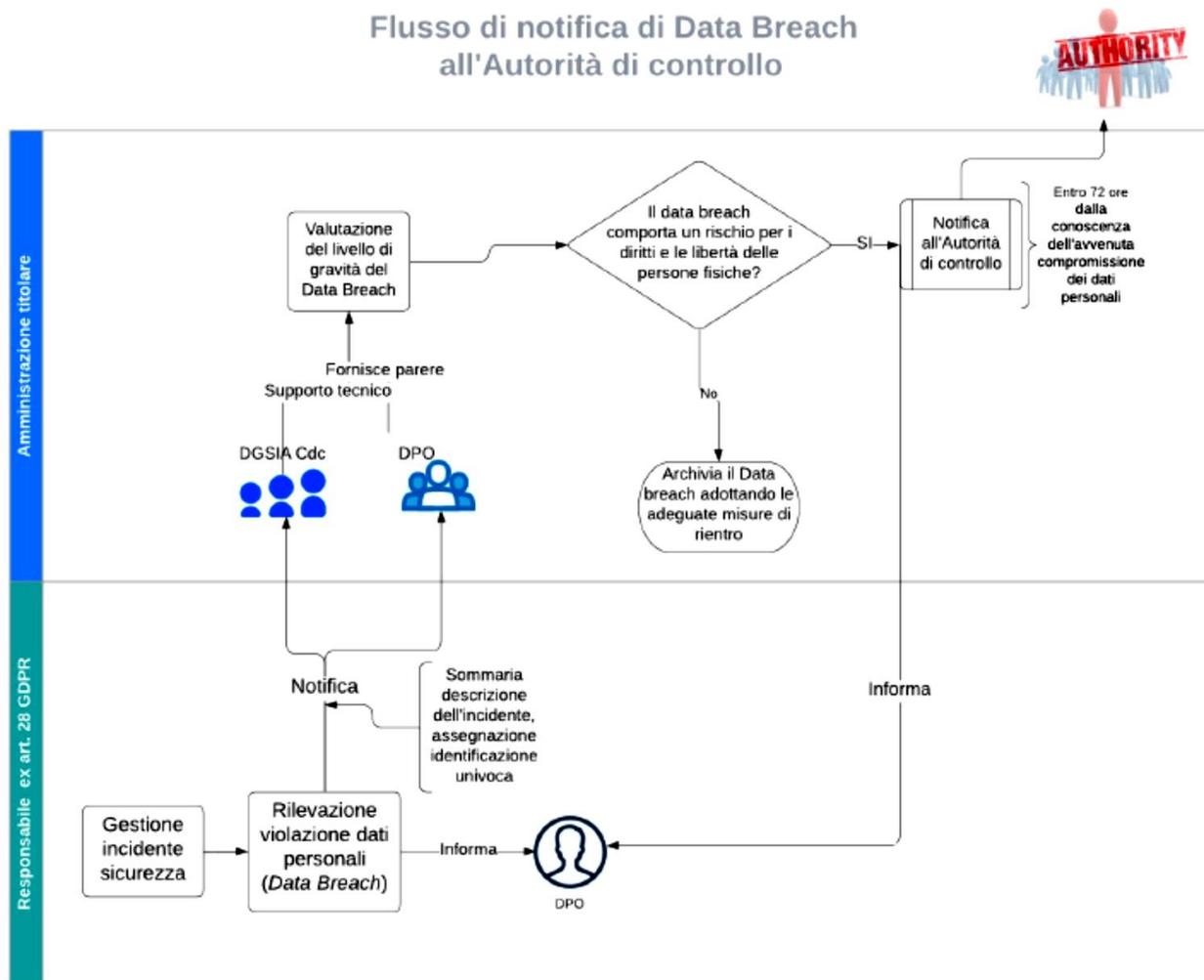


APPENDICE 7. Data Breach: il flusso di notifica - Diagramma di flusso

IPOTESI 1 - DATA BREACH RILEVATO DALLA CORTE DEI CONTI



IPOSTESI 2 - DATA BREACH PRESSO IL RESPONSABILE PROTEZIONE DATI PERSONALI



“Linee Guida sulla Protezione dei Dati Personali nella Corte dei conti - Vers. 1/2022”.

Le presenti Linee guida non esauriscono i temi e gli approfondimenti sulla protezione dei dati personali, oggetto di evoluzioni e aggiornamenti in continuo divenire.

Il documento è stato elaborato a cura del Responsabile Protezione dati (DPO) della Corte dei conti, Cons. Luisa D’Evoli, e del Nucleo di supporto al Responsabile protezione dati, Cristiana Carratu’, Rosamaria Berte’

mail: responsabile.protezione.dat@corteconti.it

pec: responsabile.protezione.dat@cortecconticert.it