GRUPPO EUROPEO DEGLI ARCHIVI

GUIDA ALLA PROTEZIONE DEI DATI PERSONALI PER GLI ARCHIVI

Linee guida del Gruppo Europeo degli Archivi per l'applicazione nel settore archivistico del Regolamento europeo sulla protezione dei dati personali

Queste linee guida hanno lo scopo di aiutare gli Archivi che si trovano in Europa ad applicare il Regolamento europeo sulla protezione dei dati personali. Sono un testo non definitivo, che potrà essere migliorato e arricchito grazie alla vostra esperienza e ai vostri commenti; potrà inoltre essere emendato sulla base della futura giurisprudenza, nonché dei pareri e linee guida pubblicati dal Comitato europeo per la protezione dei dati.

Il Gruppo Europeo degli Archivi (European Archives Group – EAG) sarà grato per vostri commenti, che possono essere inviati all'indirizzo: *SG-EAG-GUIDELINES@ec.europa.eu.*

ESCLUSIONE DALLA RESPONSABILITÀ LEGALE

Questo documento non ha l'intento di fornire, e non costituisce o comprende, consulenza legale su una particolare questione ed è stato creato solo a scopo informativo generale. Non si dovrebbe agire o astenersi dall'agire sulla base del suo contenuto, senza essersi assicurata un'adeguata consulenza legale o professionale.

Titolo Guida alla protezione dei dati personali per gli archivi. Linee guida del Gruppo Europeo degli Archivi per l'applicazione nel settore archivistico del Regolamento europeo sulla protezione dei dati personali
Autore: © European Archives Group (EAG)
Data: Ottobre 2018

Edizione italiana a cura della Direzione generale archivi
Traduzione e note all'edizione italiana di Giulia Barrera e Caterina Fontanella

Copyright

SOMMARIO

Acronimi e abbreviazioni usati in queste linee guida

I. Introduzione

II. Principi generali

1. Principi generali applicabili al trattamento dei dati personali (art. 5)
2. Liceità del trattamento
3. Il GDPR protegge solo i dati personali delle persone in vita (ma le leggi nazionali possono proteggere anche i dati relativi ai defunti)

III. Cos'è la "archiviazione nel pubblico interesse"?

4. Regole diverse per archivi diversi (la "archiviazione nel pubblico interesse" secondo il considerando 158)
5. Garanzie e deroghe relative al trattamento ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici (art. 89)

IV. I diritti degli interessati

6. Il nocciolo della questione: garantire agli interessati il controllo sui propri dati
7. Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato (art. 14)
8. Diritto di accesso dell'interessato (art. 15)
9. Diritto di rettifica (art. 16)
10. Diritto alla cancellazione ('diritto all'oblio') (art. 17)
11. Diritto di limitazione del trattamento (art. 18) e diritto di opposizione (art. 21)
12. Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (art. 19)
13. Diritto alla portabilità dei dati (art. 20)

V. Il trattamento di categorie di dati che richiedono particolari garanzie

14. Trattamento di categorie particolari di dati personali
15. Trattamento dei dati personali relativi a condanne penali e reati (art. 10)

VI. Sicurezza dei dati

16. Protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25): cosa significa per gli archivi?
17. Sicurezza dei dati personali (artt. 32-34)
18. Valutazione d'impatto sulla protezione dei dati e consultazione preventiva (artt. 35-36)

VII. Misure per la trasparenza e per promuovere l'ottemperanza al GDPR

19. Registri delle attività di trattamento (art. 30)
20. Responsabile della protezione dei dati (art. 37): anche gli archivi devono designarlo?

Appendice:
Glossario
Dove cercare altre indicazioni
Appendice alla edizione italiana

ACRONIMI E ABBREVIAZIONI USATI IN QUESTE LINEE GUIDA

DIRETTIVA 95/46/CE: *Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*

DPO: Data Protection Officer – Responsabile della protezione dei dati

EAG: European Archives Group – Gruppo europeo degli archivi

EDPB: European Data Protection Board – Comitato europeo per la protezione dei dati

GDPR: General Data Protection Regulation – *Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*

NOTA ALLA EDIZIONE ITALIANA

In questo testo si è utilizzato il termine "Archivio" con la lettera maiuscola per indicare un istituto di conservazione (in inglese "archive service"), mentre "archivio" con la minuscola indica un complesso documentario selezionato per la conservazione permanente.

La traduzione italiana corrisponde integralmente all'edizione originale, se non per la correzione di alcuni refusi e l'aggiunta di alcune note dei traduttori. Per le citazioni testuali del GDPR si è utilizzata la traduzione pubblicata sulla Gazzetta ufficiale della UE del 4 maggio 2016.

1. INTRODUZIONE

1. **Destinatari**. Queste linee guida sono indirizzate alle istituzioni pubbliche e private che conservano archivi, ovvero documenti che sono stati selezionati per la conservazione permanente. Non sono rivolte solamente agli Archivi di Stato, ma anche agli Archivi comunali, ai musei, biblioteche, fondazioni e a tutti gli altri enti pubblici e privati che conservano archivi.

2. **Obiettivi**. Queste linee guida si propongono di fornire agli archivisti informazioni di base e direttive pratiche riguardo alle specifiche sfide che si devono affrontare quando si applica il Regolamento europeo sulla protezione dei dati personali (GDPR) nel settore archivistico.

3. **Ambito di applicazione.** Come ogni altro ente pubblico o privato, gli istituti di conservazione degli archivi (d'ora innanzi "Archivi" capitalizzato) trattano dati personali che riguardano il proprio personale. Queste linee guida non forniscono indicazioni sul trattamento dei dati personali da parte degli Archivi nella loro veste di datori di lavoro, né sul trattamento dei dati relativi agli utenti, ai donatori, ai collaboratori esterni e così via. Le autorità garanti per la protezione dati, i governi, la Commissione europea, il Comitato europeo per la protezione dei dati e altri soggetti stanno già producendo materiali informativi al riguardo (si veda l'Appendice *Dove cercare altre indicazioni*). Queste linee guida riguardano esclusivamente il trattamento dei dati personali contenuti nei fondi archivistici.

4. Il **GDPR: le stesse regole in tutta l'Unione europea (ma con eccezioni nel settore archivistico)**. Un regolamento europeo è un atto legislativo vincolante che deve essere applicato nella sua interezza in tutta l'Unione. In sostituzione della precedente normativa europea in materia di protezione dei dati personali (la Direttiva 95/46/CE[1]), l'Unione Europea ha deciso di adottare un regolamento – invece che un'altra direttiva – allo scopo di avere regole più uniformi nei paesi membri. Tuttavia, il GDPR lascia a questi ultimi la possibilità di introdurre deroghe in alcune aree specifiche; una di queste è "l'archiviazione per pubblico interesse"; un'altra è la ricerca storica. Gli archivisti dovranno quindi verificare se il loro legislatore nazionale abbia fatto uso della facoltà di introdurre deroghe, offerta dal GDPR.

5. **Minimizzazione dei dati vs. conservazione permanente**. Un principio chiave del GDPR è la minimizzazione dei dati. In realtà non si tratta di una novità: anche la Direttiva 95/46/CE si fondava su questo principio. I dati personali devono essere raccolti e trattati solamente se è davvero necessario farlo e dovrebbero essere "conservati in una forma che consenta l'identificazione degli interessati" (ovverosia le persone a cui si riferiscono i dati) solamente per il tempo necessario a raggiungere lo scopo per il quale sono stati raccolti (art. 5.1. b, e). Se questo principio non ammettesse eccezioni, nel futuro non ci sarebbero più archivi che includono dati personali. I legislatori europei hanno però introdotto delle deroghe a questa regola, riconoscendo che gli archivi sono necessari per proteggere diritti fondamentali. Infatti, il GDPR stabilisce che "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", purché si assumano specifiche misure "a tutela dei diritti e delle libertà dell'interessato" (art. 5.1 e).

[1] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

6. **Conservare i dati personali solo quando è necessario farlo: niente di nuovo per gli archivisti**. Una delle attività archivistiche fondamentali è la selezione dei documenti per la conservazione permanente. Solo una piccola percentuale dei documenti prodotti o ricevuti dallo Stato, dalle altre pubbliche amministrazioni o dai privati nel corso delle loro attività finisce negli Archivi. Gli archivisti selezionano per la conservazione illimitata solo i documenti necessari per tutelare i diritti dei cittadini e per la ricerca storica. Le istituzioni archivistiche dovrebbero rendere pubblici i criteri generali seguiti per la scelta dei documenti da destinare alla conservazione permanente e dovrebbero essere in grado di spiegare perché hanno deciso di conservare specifici fondi archivistici contenenti dati personali.

7. **Conservare i dati personali non vuol dire renderli consultabili**. In tutti i paesi dell'Unione Europea la legislazione nazionale stabilisce regole sull'accesso ai documenti conservati negli Archivi pubblici. Il periodo di esclusione dall'accesso per i documenti contenenti dati personali cambia da un paese all'altro e in base al tipo di dati personali. Per esempio, in Italia i dati personali utili a rivelare l'origine razziale o etnica, le opinioni religiose e politiche e l'appartenenza a partiti e sindacati sono esclusi dall'accesso per 40 anni, quelli relativi alla salute e alla vita sessuale lo sono per 70 anni, mentre i documenti utili a rivelare l'identità della madre che ha scelto il parto in anonimato sono esclusi dall'accesso per 100 anni. Il periodo di esclusione dalla consultabilità può essere anche più lungo; ad esempio, in Romania i documenti relativi alla salute e i registri di stato civile sono esclusi dalla consultazione per 100 anni, mentre i documenti sulla vita privata degli individui sono fuori consultazione fino a 40 anni dopo la morte dell'interessato. I cittadini possono fidarsi degli Archivi: non riveleranno indebitamente i loro dati personali.

8. **Il GDPR non cambia i termini di consultabilità dei documenti**. Il GDPR include disposizioni sul diritto degli interessati ad accedere ai propri dati personali, ma non detta regole sull'accesso agli archivi da parte del grande pubblico. Il periodo di esclusione dalla consultazione per i documenti che contengono dati personali rimane invariato.

9. **Il GDPR non modifica le leggi sulla libertà di informazione**. La *Carta dei diritti fondamentali dell'Unione Europea*[2] considera diritti fondamentali sia la protezione dei dati personali, sia la libertà di espressione e informazione (che include la libertà di ricevere e dare informazioni). Il GDPR non modifica le leggi sulla libertà di informazione e stabilisce che "i dati personali contenuti in documenti conservati da un'autorità pubblica o da un organismo pubblico dovrebbero poter essere diffusi da detta autorità o organismo se la diffusione è prevista dal diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti" (considerando[3] 154).

10. **Il GDPR non modifica le leggi sulla libertà di espressione**. Tra gli utenti degli archivi vi sono, tra gli altri, giornalisti, accademici e altri ricercatori di ogni ordine e grado, che – in molti casi – pubblicheranno il frutto delle loro ricerche. Il GDPR non modifica le leggi sulla stampa e le altre norme sulla libertà di espressione e afferma che "il diritto degli Stati membri concilia la protezione dei dati personali ai sensi del presente regolamento con il diritto alla libertà d'espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria" (art. 85). Gli Stati membri possono prevedere esenzioni o deroghe alla maggior parte delle norme del GDPR, quando i dati personali sono trattati per tali finalità (art. 85).

11. **Queste linee guida non sono un codice di condotta**. Il GDPR incoraggia "l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione" del Regolamento (art. 40.1).

[2] (2000/C 364/01)

[3] In premessa, il GDPR reca centosettantatre considerazioni preliminari (in inglese *recital*), che in italiano vengono denominate "considerando" (NdT).

Stabilisce inoltre che “le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta” (art. 40.2) e prevede una specifica procedura per l’approvazione di essi da parte delle Autorità di controllo nazionali (se il codice ha solo portata nazionale) o da parte del Comitato europeo per la protezione dei dati e della Commissione Europea (se il codice deve essere applicato in diversi Stati membri).

Queste linee guida sono state redatte dallo European Archives Group (Gruppo europeo degli archivi), un gruppo di esperti della Commissione Europea, composto da rappresentanti degli Archivi nazionali e delle Direzioni generali per gli archivi degli Stati membri dell’Unione. Non sono state sottoposte al processo di approvazione previsto dall’art. 40 del GDPR per i codici di condotta e possono piuttosto essere considerate un testo di orientamento.

II. PRINCIPI GENERALI

1. PRINCIPI GENERALI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI (ART. 5)

Gli archivisti debbono conoscere i principi generali relativi al trattamento dei dati personali, fissati dall'art. 5 del GDPR:

1. I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, paragrafo 1, considerato incompatibile con le finalità iniziali ("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, conformemente all'art. 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato ("limitazione della conservazione");

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, 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").

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo ("responsabilizzazione").

Questi principi hanno varie conseguenze pratiche per gli Archivi e devono quindi essere sempre tenuti a mente. Gli archivisti, ad esempio, sono abituati ad applicare il principio della "riservatezza": per gli istituti archivistici, proteggere le informazioni riservate dagli accessi non autorizzati è prassi abituale. Alcune delle implicazioni di questi principi sono però meno ovvie. Ad esempio:

- il principio della "trasparenza" implica – tra le altre cose – che gli Archivi devono pubblicare informazioni chiare e di facile comprensione sui loro compiti, in particolare su come e perché trattano i dati personali e su come gli interessati possono avere accesso ad essi;
- il principio dell'"integrità" implica – tra le altre cose – che la negligenza che provoca la perdita di documenti contenenti dati personali costituisce una violazione non solamente della normativa sugli archivi e dei principi della professione archivistica, ma anche del GDPR.

2. LICEITÀ DEL TRATTAMENTO

Il GDPR stabilisce che il trattamento dei dati personali è legittimo solamente se si verifica almeno una delle condizioni previste dall'art. 6: "l'interessato ha espresso il consenso al trattamento dei propri dati personali"; "il trattamento è necessario per l'esecuzione di un contratto di cui l'interessato è parte", "il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento", e così via. Di particolare interesse per gli archivisti è la condizione posta al comma 1, lett. e), che stabilisce che il trattamento dei dati personali è legittimo se "è necessario per l'esecuzione di un compito di interesse pubblico".

Il GDPR lascia che siano la normativa dell'Unione europea o le leggi nazionali a determinare quali tipi di attività siano da considerarsi di pubblico interesse. La legge degli Stati membri può ad esempio definire la conservazione degli archivi da parte di una specifica istituzione o la conservazione di determinate categorie di archivi come "compito di interesse pubblico".

3. IL GDPR PROTEGGE SOLO I DATI PERSONALI DELLE PERSONE IN VITA (MA LE LEGGI NAZIONALI POSSONO PROTEGGERE ANCHE I DATI RELATIVI AI DEFUNTI).

Il GDPR protegge i dati personali delle persone viventi e non detta regole inerenti i dati personali dei defunti. Gli archivisti devono però considerare che la legislazione nazionale può farlo[4]. Il GDPR infatti stabilisce che "Gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute" (considerando 27).

Come possono gli archivisti sapere se una persona è deceduta? In molti casi non possono, ma si può ragionevolmente presumere che persone nate più di cento anni fa siano morte. Se, per esempio, gli archivisti stanno trattando documenti personali di soldati che hanno combattuto la Prima guerra mondiale, si può dare per scontato che nessuno di essi sia ancora in vita e che dunque il GDPR non si applichi a questi documenti. In molti casi, tuttavia, la situazione non sarà così chiara e gli archivisti dovranno valutare caso per caso la possibilità che i fondi archivistici di cui si occupano possano contenere dati relativi a persone viventi.

[4] È il caso dell'Italia: si veda l'Appendice all'edizione italiana (NdT).

III. COS'È LA "ARCHIVIAZIONE NEL PUBBLICO INTERESSE"?

4. REGOLE DIVERSE PER ARCHIVI DIVERSI ("ARCHIVIAZIONE NEL PUBBLICO INTERESSE" SECONDO IL CONSIDERANDO 158)

Il GDPR ammette diverse deroghe a favore della "archiviazione nel pubblico interesse". Il considerando 158 spiega il significato di questa espressione:

> le autorità pubbliche o gli organismi pubblici o privati che *tengono registri*[5] *di interesse pubblico* dovrebbero essere servizi che, in virtù del diritto dell'Unione o degli Stati membri, hanno l'obbligo legale di acquisire, conservare, valutare, organizzare, descrivere, comunicare, promuovere, diffondere e fornire accesso a *registri* con un valore a lungo termine per l'interesse pubblico generale. (corsivo aggiunto)

Quali archivi rientrano in questa definizione? Come si può notare, non è la natura degli archivi, ma il mandato dell'istituzione che li conserva a fare la differenza. Di certo gli Archivi nazionali, gli Archivi di Stato e gli Archivi comunali − così come l'Archivio storico dell'Unione Europea − effettuano "archiviazione nel pubblico interesse" ai sensi del GDPR.

A seconda delle normative nazionali, anche altre istituzioni che conservano archivi possono essere comprese in questa definizione. Ad esempio, la legge di un paese membro potrebbe affidare ad un ente il compito di acquisire, conservare e rendere accessibile ai ricercatori le carte personali degli scrittori; potrebbe istituire un museo della storia della scienza che include tra le sue competenze l'acquisizione e conservazione delle carte personali degli scienziati; potrebbe altresì creare un istituto per lo studio della storia di un regime autoritario la cui missione include la conservazione del patrimonio documentario riguardante le vittime della repressione politica.

È importante a questo proposito tenere presente che quando il GDPR parla di "legislazione nazionale" non si riferisce solamente a un testo di legge approvato da un Parlamento nazionale. Il considerando 41 afferma, infatti, che "qualora il presente regolamento faccia riferimento a una base giuridica o a una misura legislativa, ciò non richiede necessariamente l'adozione di un atto legislativo da parte di un parlamento." Lo strumento giuridico che può conferire ad un ente l'obbligo legale di acquisire, conservare, ordinare e dare in consultazione archivi può essere diverso da un paese all'altro, a seconda dei rispettivi ordinamenti costituzionali: può essere ad esempio una legge nazionale, una legge regionale, un decreto ministeriale e così via. Gli archivisti debbono quindi tenere presente che un Archivio o un'altra istituzione culturale che ha la missione istituzionale di acquisire, conservare e fornire accesso agli archivi per finalità di interesse pubblico, ricade nella definizione del considerando 158.

Non tutti gli enti che conservano archivi hanno l'obbligo legale di acquisirli e dunque non tutti rientrano nella definizione sopra ricordata; in molti casi, però, tali enti hanno una chiara missione culturale e conservano archivi a fini di ricerca storica. Il GDPR prevede deroghe in caso di trattamento dei dati personali a fini di ricerca storica sia nell'art. 89, che in diversi altri articoli.

[5] Il termine "registri" è un errore di traduzione che compare nella versione in italiano della Gazzetta ufficiale della UE. Nell'originale inglese, le espressioni utilizzate sono *records of public interest*" e poi *records of enduring value*; in questo contesto, l'inglese "records" in italiano si traduce con "documenti d'archivio" o, per estensione, "archivi"; in francese è stato tradotto con *archives qui sont à conserver à titre définitif* (NdT).

Infine, gli archivisti devono tenere presente che le deroghe a favore della "archiviazione nel pubblico interesse" riguardano solo i trattamenti dei dati personali contenuti nei fondi archivistici conservati dagli Archivi. Tutti gli altri trattamenti di dati personali effettuati dagli Archivi ricadono sotto le stesse regole che si applicano a qualsiasi altro ente pubblico o privato. In altre parole, quando gli Archivi trattano i dati personali di utenti, di studenti che partecipano ad attività didattiche, di persone che partecipano a un convegno, e così via, non possono godere di alcuna deroga.

5. GARANZIE E DEROGHE RELATIVE AL TRATTAMENTO A FINI DI ARCHIVIAZIONE NEL PUBBLICO INTERESSE, DI RICERCA SCIENTIFICA O STORICA O A FINI STATISTICI (ART. 89)

Nel GDPR compaiono frequenti riferimenti agli archivi e alla ricerca storica. Diversi articoli che stabiliscono obblighi o divieti per il titolare del trattamento, infatti, ammettono deroghe quando il trattamento è necessario per fini di archiviazione nel pubblico interesse o a fini di ricerca scientifica o storica.

Inoltre, il GDPR contiene un articolo dedicato specificamente al "trattamento a fini di archiviazione nel pubblico interesse, ai fini di ricerca scientifica o storica o ai fini statistici" (art. 89). Il primo paragrafo stabilisce regole comuni al trattamento dei dati personali sia "a fini di archiviazione nel pubblico interesse" che "ai fini di ricerca scientifica o storica o a fini statistici".

> 1. Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.

L'art. 89 stabilisce inoltre che

> 2. Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18 e 21 (…)
>
> 3. Se i dati personali sono trattati per finalità di archiviazione nel pubblico interesse, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18, 19, 20 e 21 (…)

In entrambi i casi, le deroghe sono possibili

> (…) fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

Il principio della minimizzazione dei dati e l'obbligo di garantire adeguate garanzie per proteggere i diritti degli interessati sono comuni sia al "trattamento ai fini di archiviazione nel pubblico interesse" che al "trattamento ai fini di ricerca scientifica o storica o a fini statistici", ma la concreta attuazione di questi principi è diversa nei diversi settori.

Quando si fa una ricerca in ambito sanitario, è importante mantenere la correlazione tra i diversi dati clinici riguardanti un determinato paziente, ma il nome del paziente è irrilevante. In questo caso, la pseudonimizzazione delle cartelle cliniche sarebbe una misura appropriata. Invece una istituzione archivistica che conserva archivi nel pubblico interesse deve preservare nella loro integrità le cartelle cliniche selezionate per la conservazione permanente, nell'interesse delle persone a cui si riferiscono. Ad esempio, di recente alcuni paesi sono stati in grado di pagare un risarcimento a persone che decine di anni prima erano state sottoposte a sterilizzazione forzata, proprio grazie al fatto che la documentazione sanitaria che le riguardava era stata conservata nella sua integrità. La storia europea presenta molti altri casi in cui la conservazione integrale dei documenti contenenti dati personali è stata determinante per ristabilire i diritti delle persone interessate.

Tutelare il diritto alla verità e il diritto ad un rimedio e ad una riparazione per le vittime di gravi violazioni dei diritti umani richiede la conservazione integrale degli archivi

Le vittime delle persecuzioni fasciste e naziste o dell'utilizzo nazista di lavoro schiavistico hanno potuto essere identificate e indennizzate perché sono stati conservati archivi contenenti i loro dati personali. La conservazione degli archivi nella loro integrità è stata anche lo strumento che ha permesso la restituzione delle proprietà confiscate dopo la caduta del Comunismo.

Il GDPR incoraggia la conservazione degli archivi che documentano violazioni dei diritti umani. Infatti il considerando 158 afferma che:

> gli Stati membri dovrebbero inoltre essere autorizzati a prevedere il trattamento ulteriore dei dati personali per finalità di archiviazione, per esempio al fine di fornire specifiche informazioni connesse al comportamento politico sotto precedenti regimi statali totalitari, a genocidi, crimini contro l'umanità, in particolare l'Olocausto, o crimini di guerra.

Quando assumono decisioni in merito alla conservazione o distruzione dei documenti contenenti dati personali, gli archivisti debbono ricordare che la protezione dei dati personali deve essere bilanciata con il diritto alla giustizia, il diritto alla verità e il diritto a rimedi e riparazioni per gravi violazioni dei diritti umani.

Riconoscendo che i trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici necessitano di strumenti di diverso tipo per mettere in pratica il principio della minimizzazione dei dati, il GDPR non impone sempre la pseudonimizzazione, ma solo quando "tali finalità possono essere conseguite in tal modo".

Gli archivisti applicano il principio della minimizzazione dei dati in modi diversi rispetto agli scienziati e agli statistici. Innanzi tutto, selezionano per la conservazione permanente documenti che contengono dati personali solo quando è veramente necessario farlo, ai sensi della missione istituzionale che la legge assegna all'Archivio in cui operano; inoltre applicano la normativa sulla consultabilità ed escludono dall'accesso i documenti contenenti dati personali per tutto il tempo richiesto dalla legge (le restrizioni di legge per l'accesso agli archivi cambiano di paese in paese e per alcune tipologie di dati personali il periodo di esclusione può arrivare a 120 anni).

Quando i documenti contenenti dati personali diventano consultabili, ma vi è ancora la possibilità che la persona a cui si riferiscono sia viva, gli archivisti si astengono da ogni trattamento che potrebbe

ledere la dignità dell'interessato. Non scordano mai l'art. 1 della *Carta dei diritti fondamentali dell'Unione europea*, secondo cui "La dignità umana è inviolabile. Essa deve essere rispettata e tutelata"; un modo per mettere in pratica questo principio è astenersi dal pubblicare online documenti archivistici o strumenti di ricerca la cui diffusione potrebbe rappresentare un danno per la dignità della persona interessata.

Gli Archivi possono anche utilizzare la pseudonimizzazione, ma se effettuata da un Archivio, la pseudonimizzazione deve essere pienamente reversibile e deve essere effettuata in modo da non mettere a rischio il valore di prova dei documenti d'archivio. Nel caso di dati personali conservati a fini di archiviazione nel pubblico interesse, gli Archivi debbono conservare una copia integrale dei documenti originali in un deposito protetto e possono creare una copia in cui i dati personali sono pseudonimizzati da mettere a disposizione dei ricercatori, se tale finalità può essere perseguite in questo modo.

Il GDPR permette la conservazione degli archivi d'impresa contenenti dati personali?

Alcune imprese private conservano archivi vecchi di secoli, che costituiscono una fonte preziosissima per gli storici. Gli storici del futuro avranno a disposizione simili fonti archivistiche? In altre parole, il GDPR permette la conservazione degli archivi d'impresa contenenti dati personali? È una domanda a cui non è facile rispondere.

I documenti d'archivio creati da enti privati possono essere trattati a fini di archiviazione nel pubblico interesse tanto quanto quelli creati da enti pubblici. Tale trattamento, però, può essere considerato "archiviazione nel pubblico interesse" solo se effettuato da un ente pubblico o privato che abbia "l'obbligo legale di acquisire, conservare, valutare, organizzare, descrivere, comunicare, promuovere, diffondere e fornire accesso a registri con un valore a lungo termine per l'interesse pubblico generale" (considerando 158). Che cosa si intenda per "obbligo legale" è diverso nei paesi di *common law* e nei paesi a diritto codificato.

Gli enti che hanno come fine la ricerca storica, ma che non hanno l'obbligo legale di acquisire e trattare archivi, possono trattare archivi d'impresa a fini di ricerca storica. Sia il principio della "limitazione delle finalità" che quello della "limitazione della conservazione" ammettono infatti deroghe non solo per fini di archiviazione del pubblico interesse, ma anche per fini di ricerca storica. Tali deroghe sono possibili a condizione che vengano adottate adeguate misure per salvaguardare le libertà e i diritti degli interessati. L'interpretazione di queste norme risulterà più chiara mano a mano che le autorità garanti nazionali e il Comitato europeo per la protezione dei dati emaneranno le loro decisioni e linee guida.

IV. I DIRITTI DEGLI INTERESSATI

6. IL NOCCIOLO DELLA QUESTIONE: GARANTIRE AGLI INTERESSATI IL CONTROLLO SUI PROPRI DATI

Uno dei principali obiettivi del GDPR è permettere agli individui di avere il controllo dei propri dati personali. Per questo motivo, riconosce loro un complesso organico di diritti relativi ai propri dati personali (il diritto di sapere quali dati siano trattati e perché, il diritto d'accesso, i diritto alla cancellazione, al trasferimento dei dati, ecc.) che prevedono solo limitate eccezioni. L'archiviazione nel pubblico interesse è motivo di deroga alla maggior parte dei diritti degli interessati. In due casi – il diritto all'informazione (art. 14) e il "diritto all'oblio" (art. 17) – il GDPR introduce direttamente deroghe in caso di archiviazione nel pubblico interesse; in altri casi, permette invece agli Stati membri di farlo. Come già menzionato, infatti, l'art. 89 permette agli Stati membri di introdurre deroghe ai diritti di cui agli articoli 15, 16, 18, 19, 20 e 21 del GDPR. Questo significa che archivisti nel diversi paesi della UE potranno dover obbedire a norme diverse, in materia dei diritti degli interessati.

In tutti i casi, le deroghe non sono mai assolute, ma soggette all'adozione delle garanzie indicate dall'art. 89, comma 1, ovverosia misure tecniche e organizzative finalizzate a garantire il rispetto del principio della minimizzazione dei dati e la protezione delle libertà e dei diritti degli interessati. Inoltre, gli Archivi debbono cercare di garantire agli interessati il massimo controllo possibile sui propri dati. Questo principio ha particolare rilevanza quando gli Archivi conservano le carte personali di persone viventi, acquisite per dono, deposito o acquisto; oppure quando gli Archivi conservano registrazioni di interviste raccolte nell'ambito di progetti di storia orale. Tuttavia, gli Archivi non possono accondiscendere a richieste degli interessati, se questo implicherebbe violare la loro missione istituzionale di preservare l'integrità degli archivi e di ordinarli, descriverli, e metterli in consultazione.

7. INFORMAZIONI DA FORNIRE QUALORA I DATI PERSONALI NON SIANO STATI OTTENUTI PRESSO L'INTERESSATO (ART. 14).

Il GDPR stabilisce che il titolare del trattamento deve fornire all'interessato determinate informazioni sul trattamento praticato, anche nel caso in cui il titolare non abbia ottenuto i dati personali direttamente dall'interessato (art. 14). Questa è la tipica situazione degli Archivi, che normalmente trattano documenti contenenti dati personali che non hanno acquisito direttamente, ma sono stati acquisiti dal soggetto produttore dell'archivio.

Il GDPR ammette però alcune deroghe a questo obbligo e una riguarda gli archivi. L'art. 14 prevede, infatti, che il dovere di fornire all'interessato le informazioni sul trattamento dei dati personali quando questi non siano stati ottenuti presso l'interessato, non si applica quando sarebbe "impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica". In questi casi, l'art. 14 incoraggia esplicitamente i titolari a rendere pubbliche le informazioni.

Quando gli Archivi acquisiscono, riordinano, descrivono, conservano e mettono in consultazione fondi archivistici che contengono dati personali relativi ad un numero indefinito di persone, al punto che informare gli interessati riguardo a tali trattamenti sarebbe "impossibile o implicherebbe uno sforzo sproporzionato", la cosa migliore da fare sembra essere pubblicare sul sito web dell'istituto informazioni su tali trattamenti, in modo da informarne il pubblico.

In alcuni casi, si può intraprendere un tentativo di informare gli interessati più focalizzato. Ad esempio, se un Archivio acquisisce la documentazione prodotta da un'associazione, un partito o un sindacato che trattava dati personali solo dei propri associati, potrebbe concordare con l'ente produttore di utilizzare i suoi canali informativi (notiziari, siti web, mailing list, ecc.) al fine di informare gli associati in merito al trattamento che l'Archivio effettuerà.

L'art. 14 include una lista dettagliata di informazioni che i titolari debbono fornire agli interessati, quando i dati personali non sono stati ottenuti da loro. In estrema sintesi, gli Archivi devono spiegare in termini facilmente comprensibili da qualcuno che non sa nulla di archivi, che tipo di trattamenti effettuano e perché, e su quale base giuridica. Inoltre, devono spiegare agli interessati come possono accedere ai propri dati ed informarli del fatto che sono consultabili da altri, nei limiti stabiliti dalla normativa sulla consultabilità dei documenti d'archivio contenenti dati personali. Infine, se un interessato contatta un Archivio e chiede informazioni sul tipo di trattamenti che effettua, gli archivisti devono essere pronti a fornirgli ogni possibile spiegazione.

8. DIRITTO DI ACCESSO DELL'INTERESSATO (ART. 15)

Di regola, gli interessati hanno il diritto di ottenere dal titolare del trattamento la conferma se sia o meno in corso un trattamento di dati personali che li riguardano. Inoltre, gli interessati hanno il diritto di conoscere lo scopo del trattamento, le categorie di dati personali coinvolte e altre informazioni sul trattamento dei dati personali che li riguardano.

Gli Archivi conservano una grandissima quantità di dati personali che sono stati acquisiti da altri soggetti. Quando questi soggetti versano i loro archivi ad un istituto di conservazione, dovrebbero congiuntamente versare i relativi strumenti di ricerca, per permettere agli archivisti di sapere, tra le altre cose, quali dati personali essi contengono. Capita però frequentemente che gli Archivi ricevano versamenti priva di dettagliati strumenti di ricerca, accompagnati solo da un sommario elenco di versamento; di conseguenza, gli archivisti non possono sapere quali dati personali siano contenuti nei fondi in questione. Spesso, inoltre, gli Archivi ricevono documentazione che ha perso l'ordine originario e necessita di un attento lavoro di riordinamento per ripristinarlo.

Queste circostanze creano difficoltà oggettive nell'attuazione di alcuni dei diritti degli interessati previsti dal GDPR; il Regolamento riconosce questo fatto e, come si è già ricordato, l'art. 89 prevede che il diritto dell'Unione o degli Stati membri possa introdurre deroghe ai diritti degli interessati.

Gli archivisti devono dunque verificare se il legislatore del loro paese ha introdotto deroghe al diritto d'accesso previsto dall'art. 15 del GDPR. Queste deroghe proteggono gli archivisti da ogni responsabilità, nel caso in cui non siano in grado di soddisfare completamente la richiesta dell'interessato di ricevere informazioni sui trattamenti effettuati da un Archivio sui dati che lo riguardano. Ma queste deroghe non esentano l'archivista dal dover fare tutto il possibile per soddisfare le richieste degli interessati.

Se un interessato si rivolge ad un archivio e chiede di accedere ai dati personali che lo riguardano, gli archivisti devono fornire ogni possibile assistenza, spiegando come svolgere la ricerca in archivio, indicando in quale fondi è più probabile che siano contenuti dati personali e illustrando come consultare gli strumenti di ricerca e come richiedere la consultazione di un fascicolo. Se l'interessato ha particolari difficoltà a effettuare la ricerca a causa dell'età avanzata, del livello di alfabetizzazione o di un impedimento fisico, gli archivisti devono fornire particolare assistenza, nel limite del possibile, tenuto conto di vincoli come il numero degli addetti.

9. DIRITTO DI RETTIFICA (ART. 16)

L'art. 16 del GDPR prevede che l'interessato ha il diritto alla rettifica dei propri dati personali inesatti e all'integrazione di quelli incompleti. Il titolare ha il dovere di corrispondere a tali richieste "senza ingiustificato ritardo".

Gli Archivi devono tutelare l'integrità degli archivi, allo scopo di preservare il valore probatorio dei documenti; tutto ciò è necessario a proteggere i diritti degli interessati. Ad esempio, i fascicoli di polizia dei regimi repressivi in genere includono informazioni dispregiative sugli oppositori politici. Preservare l'integrità di questi documenti è necessario per consentire agli interessati di chiedere un risarcimento per le discriminazioni subite ad opera del regime.

Il GDPR permette di conciliare il dovere degli Archivi di conservare l'integrità dei documenti con il diritto degli interessati ad ottenere la rettifica dei dati personali inesatti che li riguardano; la rettifica può essere effettuata "fornendo una dichiarazione integrativa". Inoltre, come già ricordato, l'art. 89 prevede che il diritto dell'Unione o degli Stati membri possa introdurre deroghe ai diritti degli interessati previsti dall'art. 16.

Gli Archivi devono favorire l'esercizio del diritto degli interessati all'aggiornamento, a rettifica o all´integrazione dei dati "fornendo una dichiarazione integrativa" e devono assicurare che i dati siano conservati in modo tale che la fonte originaria rimanga separata e distinta da ogni informazione successivamente acquisita.

10. DIRITTO ALLA CANCELLAZIONE («DIRITTO ALL'OBLIO») (ART. 17)

L'esistenza di un "diritto all'oblio" nell'ambito della UE è stata affermata per la prima volta nel 2014 da un'epocale sentenza della Corte di giustizia della Unione Europea sul caso Google Spagna. La Corte europea ordinò a Google Spagna di rimuovere due notizie riguardanti una bancarotta dai risultati delle ricerche relative a un cittadino spagnolo, Mario Costeja Gonzàles. Le notizie erano state legittimamente pubblicate da un quotidiano nel 1998 e apparivano ancora tra i primi risultati quando si cercava il nome di Costeja. La sentenza della Corte di giustizia lasciò intatti gli archivi analogici e digitali del quotidiano; ha avuto conseguenze solo sui risultati che appaiono cercando il nome di Costeja su Google (le notizie sono tuttora rintracciabili utilizzando altre chiavi di ricerca). A seguito di questa sentenza, le persone possono chiedere che i dati personali che li riguardano (se sono inadeguati, irrilevanti o non più rilevanti) siano deindicizzati dai motori di ricerca, in modo da non apparire più se si cerca il loro nome.

La sentenza della Corte di Giustizia della UE sul caso Google Spagna si basava sulla Direttiva 95/46/CE, che non parlava esplicitamente di un "diritto all'oblio". Invece il GDPR usa questa espressione nel titolo dell'art. 17 "Diritto alla cancellazione ('Diritto all'oblio')".

Ai sensi del GDPR, il diritto all'oblio non si riferisce alla deindicizzazione, ma alla vera e propria cancellazione dei dati personali. L'art. 17 permette infatti all'interessato di ottenere dal titolare la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo.

Tale diritto può essere esercitato quando "i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti" o quando "l'interessato revoca il consenso" al loro trattamento, e in altre circostanze. Allo stesso tempo, il diritto all'oblio è soggetto a diverse limitazioni, e non si applica se il trattamento è necessario a fini di archiviazione nel pubblico interesse, se la cancellazione rischia "di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento (art. 17, c. 3)

Il considerando 158 spiega che le pubbliche autorità e gli altri enti che conservano archivi nel pubblico interesse sono servizi che hanno "l'obbligo legale" di trattare archivi selezionati per la conservazione permanente. La cancellazione di dati personali contenuti in documenti archivistici renderebbe impossibile, per questi organismi, assolvere alla missione istituzionale assegnatagli dalla legge. Il diritto alla cancellazione delineato dall'art. 17 non si applica dunque ai documenti selezionati per la conservazione permanente da Archivi che rientrano nella definizione del considerando 158.

Allo stesso tempo, gli archivisti dovrebbero ricordare che il diritto all'oblio, così come affermato dalla Corte di giustizia della Unione Europea (cioè non cancellazione, ma deindicizzazione dei dati personali) può essere messo in pratica dagli Archivi senza pregiudicare i loro compiti istituzionali. Deindicizzare o rimuovere un link, o prevenire in ogni altro modo la ricerca di nomi all'interno dei documenti da parte dei motori di ricerca, non compromette, infatti, l'integrità dei documenti d'archivio e non mette a rischio la loro conservazione permanente. Inoltre gli Archivi possono impedire la ricerca dei nomi contenuti in un documento pubblicato online, mantenendo la possibilità di rintracciarlo utilizzando chiavi di ricerca diverse dai nomi di persona.

In primo luogo, gli archivisti devono astenersi dal pubblicare online documenti archivistici o strumenti di ricerca contenenti dati personali la cui diffusione possa mettere a rischio la dignità degli interessati. In secondo luogo, ogni volta che rendono disponibili online documenti archivistici o strumenti di ricerca che contengono dati personali relativi a persone in vita, dovranno valutare – in relazione alla natura dei dati personali – l'opportunità di pubblicarli in un'area del loro sito web ad accesso riservato, non indicizzabile da parte dei motori di ricerca. Caso per caso, gli archivisti dovranno valutare come meglio bilanciare il loro obbligo legale di "descrivere, comunicare, promuovere, diffondere e fornire accesso" ad archivi selezionati per la conservazione permanente (considerando 158) con il principio della minimizzazione dei dati (art. 5), che richiede di limitare il trattamento dei dati allo strettamente necessario.

11. DIRITTO DI LIMITAZIONE DI TRATTAMENTO (ART. 18) E DIRITTO DI OPPOSIZIONE (ART. 21)

Il GDPR garantisce agli interessati sia il diritto di ottenere dal titolare la limitazione di trattamento sia il diritto di opporsi al trattamento dei dati che li riguardano. Quali sono le differenze tra questi diritti e quali le loro implicazioni pratiche rilevanti per gli Archivi?
Entrambi i diritti sono accomunati dall'obiettivo di garantire agli individui il controllo sui trattamenti dei dati personali che li riguardano, ma si applicano in circostanze diverse e hanno differenti conseguenze. Ciò che più interessa gli archivisti è che la normativa nazionale può introdurre deroghe a entrambe le fattispecie, in caso di trattamento dei dati personali per fini di archiviazione nel pubblico interesse (art. 89, c. 3).

Nelle specifiche circostanze elencate dall'art. 18, c. 1, gli interessati hanno il diritto di ottenere la *limitazione* del trattamento dei loro dati personali. Fondamentale per gli archivisti è che la limitazione di trattamento non impedisce la conservazione dei dati personali (art. 18, c. 2): la conservazione dei documenti d'archivio, non può dunque essere ostacolata dalla limitazione di trattamento.

Gli interessati hanno inoltre il diritto di *opposizione* al trattamento dei dati che li riguardano, anche se il trattamento è "necessario per l'esecuzione di un compito di interesse pubblico". In questo caso, "il titolare del trattamento si astiene dal trattare ulteriormente i dati personali" (art. 21, c. 1). Il titolare può però continuare il trattamento, se è in grado di dimostrare che vi sono "motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato"

(art. 21, c. 1). Questa disposizione potrebbe applicarsi al trattamento di archivi nel pubblico interesse, ma gli archivisti non devono darlo per scontato: è consigliabile tenersi informati su come la giurisprudenza interpreta questa norma.

In primo luogo, gli archivisti devono verificare se i loro legislatori nazionali hanno fatto uso della facoltà di introdurre deroghe ai diritti di limitazione (art. 18) e opposizione (art. 21) al trattamento e, in caso, se la normativa nazionale indichi quali siano le garanzie adeguate per i diritti e le libertà degli interessati che gli Archivi devono assicurare. Se la normativa nazionale non indica quali siano le garanzie adeguate, gli Archivi valuteranno caso per caso come meglio applicare i principi generali relativi al trattamento dei dati personali, indicati dall'art. 5 del GDPR.

Infine, gli archivisti devono considerare che

> qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'art. 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento dei dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico (art. 21, c. 6).

Questa norma può essere utile per gli archivisti che lavorano in musei o altri istituti culturali o organizzazioni che conservano archivi per motivi di interesse pubblico, che non rientrano nella definizione di "archiviazione nel pubblico interesse" del considerando 158.

12. OBBLIGO DI NOTIFICA IN CASO DI RETTIFICA O CANCELLAZIONE DEI DATI PERSONALI O LIMITAZIONE DEL TRATTAMENTO (ART. 19)

Il GDPR stabilisce che "il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate (…) salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato" (art. 19). Come già ricordato, la legislazione nazionale può introdurre deroghe ai diritti di rettifica, cancellazione e limitazione del trattamento, in caso di trattamento di dati personali per finalità di archiviazione nel pubblico interesse. È quindi improbabile che dati personali contenuti in fondi archivistici conservati da Archivi possano essere oggetto di rettifica, cancellazione o limitazione di trattamento.

Inoltre le normative nazionali possono prevedere deroghe anche all'obbligo di notifica, se i dati personali sono trattati per finalità di archiviazione nel pubblico interesse (art. 89, c. 3). Gli archivisti, inoltre, devono considerare che il titolare del trattamento deve assolvere all'obbligo previsto dall'art. 19, a meno che "ciò si riveli impossibile o implichi uno sforzo sproporzionato", come probabilmente è il caso per gli Archivi.

13. DIRITTO ALLA PORTABILITÀ DEI DATI

Il GDPR garantisce agli interessati "il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento" (art. 20, c. 1). Inoltre, "l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile (art. 20, c. 2). Gli Archivi non ricevono direttamente dagli interessati i dati personali contenuti nei fondi che conservano, a meno che non si tratti di carte personali. La maggior parte dei fondi archivistici oggi conservati dagli archivi sono in formato analogico, quindi la trasmissione agli interessati dei dati personali contenuti nei fondi in un formato "leggibile da dispositivo automatico" risulta, per lo più, non "tecnicamente fattibile".

Infine, gli archivisti debbono ricordare che la normativa nazionale può introdurre deroghe al diritto alla portabilità dei dati, se sono trattati a fini di archiviazione nel pubblico interesse (art. 89, c. 3).

V. IL TRATTAMENTO DI CATEGORIE DI DATI CHE RICHIEDONO PARTICOLARI GARANZIE

14. IL TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI

Il GDPR accorda una particolare protezione a determinate categorie di dati personali, il cui trattamento potrebbe generare un alto rischio per i diritti e le libertà fondamentali degli interessati. Dispone infatti:

> È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9, c. 1).

Il GDPR però ammette delle deroghe a questa norma. Il divieto di trattare queste tipologie di dati sensibili non si applica se "il trattamento è necessario a fini di archiviazione nel pubblico interesse" o a fini di ricerca storica. Tale trattamento deve trovare fondamento in una norma giuridica ed essere "proporzionato alla finalità perseguita"; inoltre deve rispettare "l'essenza del diritto alla protezione dei dati" e prevedere "misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato" (art. 9, c. 2, lett. j).

Le prescrizioni contenute nell'art. 9 per la maggior parte non sono nuove; la Direttiva 95/46/CE già proibiva, infatti, il trattamento di categorie particolari di dati personali, salvo eccezioni. Il GDPR ha esteso le categorie di dati personali che meritano particolare protezione, includendo nel novero indicato dall'art. 9 anche i "dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica".

Nei paesi membri della UE, le leggi nazionali escludono dalla consultazione i documenti contenenti categorie particolari di dati personali, per periodi che variano da pochi decenni a oltre un secolo. Gli archivisti hanno dunque già una lunga e consolidata esperienza nell'applicazione di leggi che limitano l'accesso alle categorie particolari di dati personali.

15. TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (ART. 10)

Il GDPR impone regole molto stringenti in merito al trattamento dei dati personali relativi a condanne penali e reati, che non ammettono deroghe. Il trattamento di tali tipologie di dati personali "deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri". La legge deve prevedere "garanzie appropriate per i diritti e le libertà degli interessati" (art. 10).

Nei paesi membri della UE, le leggi nazionali stabiliscono che dopo un certo numero di anni – generalmente 20 o 30 – sentenze, fascicoli processuali e archivi delle carceri che sono stati selezionati per la conservazione permanente, siano versati agli Archivi di Stato o ad altre istituzioni archivistiche. Questi Archivi trattano dunque grandi quantità di dati relativi a condanne penali: li selezionano, li trasferiscono nei depositi, li riordinano e descrivono e li rendono accessibili ai ricercatori. Questi trattamenti sono pienamente conformi al GDPR, in quanto sono previsti dalla legge ed effettuati da

autorità pubbliche con appropriate garanzie per i diritti e le libertà degli interessati. Se ad esempio la legislazione nazionale limita l'accesso alla documentazione giudiziaria per un certo numero di anni, gli archivisti applicano scrupolosamente questo tipo di restrizione. Se pubblicano online, liberamente accessibili, documenti relativi a condanne penali ed esiste la possibilità che le persone interessate siano ancora in vita, gli Archivi possono assumere precauzioni come pubblicare i documenti in un'area del sito accessibile solo previa registrazione, o come oscurare i nomi, in ossequio al principio fondamentale di rispettare e proteggere la dignità degli individui.

Se un'istituzione pubblica o privata (ad esempio una università, una fondazione o una organizzazione della società civile) conserva archivi di avvocati, oppure copie di fascicoli processuali o sentenze, o in altro modo raccoglie, conserva e rende disponibili ai ricercatori documentazione contenente dati personali relativi a condanne penali o reati (ad esempio un centro accademico specializzato in studi sul terrorismo o un centro studi creato da attivisti antimafia) è opportuno che contatti la propria autorità garante e chieda istruzioni su quali siano le misure più consone da adottare per la salvaguardia dei diritti e delle libertà degli interessati.

VI. SICUREZZA DEI DATI

16. PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA (ART. 25): COSA SIGNIFICA PER GLI ARCHIVI?

L'art. 25 prevede che i titolari, quando stanno pianificando i mezzi per trattamento di dati personali, debbono mettere in atto "misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati". Questo è ciò che il GDPR definisce come "protezione dei dati fin dalla progettazione".

Uno dei principi fondamentali della protezione dei dati personali è la minimizzazione dei dati. L'art. 25 prevede infatti che i titolari del trattamento mettano in atto "misure tecniche e organizzative adeguate per garantire che siano trattati, *per impostazione predefinita*, solo i dati personali necessari per ogni specifica finalità di trattamento" (corsivo aggiunto).

L'articolo 25 trova attuazione soprattutto quando si creano nuovi sistemi informativi. Negli Archivi, potrebbe essere il caso quando:

- si crea un deposito per documenti nativi digitali;
- si crea una banca dati degli atti di stato civile o di altri fondi archivistici contenenti dati personali;
- si crea un sistema informativo per la gestione della sala di studio;
- si creano strumenti per l'accesso ai documenti online.

Gli Archivi debbono sempre tenere presente l'art. 25 quando pianificano le differenti tipologie di attività caratteristiche della loro missione, come la selezione dei documenti da acquisire, gli ordinamenti, la descrizione, fornire accesso agli archivi e divulgarli.

Selezione: gli Archivi adottano una politica di acquisizioni che limita la conservazione permanente dei fondi archivistici contenti dati personali a ciò che è realmente necessario, in base alla loro missione istituzionale. Mettono in pratica l'art. 25 preparando con cura i piani di conservazione che definiscono quali tipologie di fascicoli contenenti dati personali debbono essere selezionati per la conservazione permanente. Per gli Archivi, i piani di conservazione sono strumenti per dimostrare l'applicazione dell'art. 25.

Ordinamento e conservazione: gli Archivi applicano il principio della minimizzazione dei dati quando creano strumenti di ricerca. Quando riordinano e descrivono fondi archivistici che contengono dati su persone viventi relativi alla salute, alla vita sessuale, alle opinioni politiche o ad altre categorie particolari di dati, oppure riguardanti le condanne penali, gli Archivi debbono creare inventari con i nomi reali, al fine di poter essere in grado di rispondere a una eventuale richiesta d'accesso degli interessati, e permettere loro di esercitare gli altri diritti riconosciutigli dal GDPR. Allo stesso tempo, per ricerche online (nel caso la legislazione nazionale permetta l'accesso ai fondi in questione), gli Archivi possono creare inventari in cui i nomi sono sostituiti da pseudonimi, se la loro missione di permettere accesso agli archivi può essere assolta in questo modo. Software per la descrizione archivistica che permettono la creazione di due differenti versioni di un inventario (una con i nomi reali, l'altra con pseudonimi) sono strumenti per l'applicazione dell'art. 25.

Fornire accesso agli archivi: gli Archivi hanno l'obbligo di assicurare che l'accesso ai documenti sia gestito in modo corretto e che siano messe in pratica garanzie tecniche e organizzative appropriate. Gli Archivi hanno una grande esperienza nel gestire e garantire gli accessi ai documenti d'archivio tramite misure organizzative come ad esempio la richiesta di una tessera agli studiosi, la verifica che i documenti richiesti siano liberamente consultabili o la limitazione del numero dei fascicoli presenti in sala studio.

In ambiente digitale, i problemi dell'accesso saranno aggravati dalla quantità, varietà e complessità dei documenti elettronici. In molti casi, grandi masse di dati non potranno essere controllate e verificate manualmente prima dell'accesso, per cui le garanzie e i controlli dovranno essere sempre più automatizzati.

Vigilanza, sorveglianza e collaborazione con gli enti creatori di archivi: nell'ambito della UE, la natura delle relazioni tra gli enti che creano gli archivi e le istituzioni archivistiche variano a seconda dei paesi e tra settore pubblico e settore privato. In alcuni casi, le istituzioni archivistiche statali hanno il potere di esercitare la tutela sugli archivi in formazione, in altri non hanno tale autorità.

La progettazione di nuovi sistemi informativi da parte di pubbliche amministrazioni – i cui archivi potranno essere in futuro versati agli Archivi – è questione che interessa le istituzioni archivistiche. Una situazione particolarmente problematica può essere costituita dalla progettazione di nuovi sistemi informativi che intendono applicare il GDPR, se non si tiene conto dell'archiviazione nel pubblico interesse sin dalla prima fase di progettazione. È importante dunque che le istituzioni archivistiche siano coinvolte nella pianificazione e progettazione dei sistemi informativi, per garantire che, al momento opportuno, i documenti possano essere estratti dal sistema o duplicati, per essere poi versati in Archivio. L'ideale è che i sistemi informativi tengano automaticamente conto della destinazione finale dei documenti.

17. SICUREZZA DEI DATI PERSONALI (artt. 32-34)

SICUREZZA DEL TRATTAMENTO

Un principio chiave del GDPR è che "il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio" (art. 32). Questo è il "principio della sicurezza".

Applicarlo comporta che il titolare e il responsabile del trattamento devono valutare l'analisi del rischio, le politiche organizzative e le misure fisiche e tecniche più adeguate, nonché altri requisiti per la sicurezza del trattamento.

Il titolare e il responsabile, al momento di decidere quali misure adottare, possono valutare lo stato dell'arte e i costi di attuazione, ma le misure devono essere commisurate sia alle circostanze che al rischio che il trattamento comporta.

Le misure di sicurezza devono garantire "la riservatezza, l'integrità e la disponibilità" dei sistemi e dei dati personali da questi trattati, e devono assicurare che il titolare e il responsabile del trattamento siano in grado di ripristinare la fruibilità e l'accesso ai dati personali in modo tempestivo in caso di incidente fisico o tecnico.

Il titolare e il responsabile devono inoltre garantire di disporre di una procedura per testare l'efficacia delle misure adottate e intraprendere ogni miglioria necessaria.

TECNICHE PER LA GESTIONE DEL RISCHIO

Il GDPR non descrive le misure di sicurezza che il titolare e il responsabile del trattamento devono mettere in pratica, ma prescrive loro di dotarsi di un livello di sicurezza che sia "appropriato" ai rischi presentati dai loro trattamenti. Prima di decidere quali misure di sicurezza siano appropriate, essi devono dunque effettuare una valutazione del rischio, seguendo una formale metodologia di gestione del rischio.

VIOLAZIONI DEI DATI PERSONALI

Il GDPR delinea un sistema di notifica delle violazioni dei dati personali (art. 33). Per violazione si intende "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" (art. 4, punto 12). La violazione può essere conseguenza di cause accidentali o intenzionali; ciò vuol dire che una violazione è più che una mera perdita di dati personali.

Quando da una violazione di dati personali è probabile che derivi un rischio per i diritti e le libertà delle persone fisiche, il titolare deve notificare al più presto la violazione all'autorità di controllo competente, se possibile entro 72 ore.

Il responsabile del trattamento deve informare il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione (art. 33, c. 2).

Quali informazioni debba contenere la notifica è indicato dall'art. 33, c. 3, del GDPR.

GARANTIRE LA SICUREZZA DEI TRATTAMENTI DEI DATI PERSONALI NEGLI ARCHIVI E PROTEGGERE I DATI PERSONALI CONSERVATI NEGLI ARCHIVI DA ACCESSI NON AUTORIZZATI

Gli archivisti sono responsabili per la sicurezza dei dati personali sotto la loro custodia, salvaguardano la loro integrità e autenticità, e li proteggono da accessi non autorizzati, alterazioni, perdite, danneggiamenti o distruzioni, operando in linea con gli standard professionali esistenti.

I dati personali devono essere conservati in modo sicuro, garantendone in ogni momento la riservatezza. L'accesso deve essere permesso solamente a coloro che hanno una necessità conoscitiva che può essere soddisfatta senza violare la legge. L'ordinamento dei fondi archivistici e il principio di provenienza non debbono essere compromessi scorporando i documenti che contengono dati personali.

Il livello di sicurezza deve essere appropriato e proporzionato alla natura dei dati e al danno che può derivare da una violazione della sicurezza. Deve riflettere gli standard professionali e l'utilizzo di tecniche per la gestione del rischio, al fine di valutare la natura, il livello e l'impatto dei rischi e le misure appropriate che devono essere prese per proteggere i dati.

Misure pratiche di sicurezza da prendere in considerazione sono, fra le altre: installare dispositivi fisici di sicurezza come allarmi anti intrusione; porre restrizioni all'accesso in determinate aree; tenere un registro dei visitatori; sorvegliare, per quanto possibile, le loro attività. I dati elettronici devono essere messi in sicurezza, ad esempio mediante software di protezione contro virus e trojan, nonché accesso tramite password, riservato agli utenti autorizzati. I dati personali devono essere trasmessi in modo sicuro: è consigliabile usare strumenti di cifratura per una trasmissione sicura dei dati personali in formato elettronico.

La ragion d'essere degli Archivi è conservare e fornire accesso ai documenti, tuttavia non si devono mettere in consultazione documenti contenenti dati personali, se non si è in grado di conciliare le esigenze della ricerca – a fini storici o amministrativi – con i diritti e le libertà fondamentali degli interessati.

COSA POSSONO/DEVONO FARE GLI ARCHIVISTI IN CASO DI VIOLAZIONE DEI DATI?

In caso di grave violazione nel corso del trattamento di documenti – sia esso conservazione, accesso, comunicazione, ecc. – gli Archivi devono stimare se sia probabile che essa provochi un danno significativo ai diritti di persone viventi. In caso affermativo, deve essere valutato se effettuare una notifica della violazione all'autorità garante, nei termini previsti dall'art. 33.

L'art. 34, c.1, recita: "Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo". Tuttavia, se la "comunicazione richiederebbe sforzi sproporzionati" – che naturalmente potrebbe essere il caso quando avviene una violazione relativa a un grande fondo archivistico, contente migliaia di dati personali – l'art. 34, c. 3, lett. c) offre l'alternativa di "una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia". Si potrebbe trattare, ad esempio, di un avviso sul sito web o di una comunicazione tramite una mailing list.

Ogni violazione deve essere registrata e analizzata, e il personale deve essere incoraggiato a denunciare e reagire agli incidenti relativi alla sicurezza.

18. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI E CONSULTAZIONE PREVENTIVA (ARTT. 35-36)

Il GDPR prevede che i titolari effettuino, prima di procedere al trattamento, una valutazione dell'impatto sulla protezione dei dati (DPIA), se il trattamento può presentare "un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35, c. 1). "Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare" il rispetto del Regolamento[6].

CHE COS'È LA VALUTAZIONE D'IMPATTO?

Lo scopo della valutazione d'impatto è identificare e valutare il rischio che un nuovo tipo di trattamento può creare per le persone (cittadini, clienti, pazienti, ecc.). Il Gruppo di lavoro articolo 29 ha definito la valutazione d'impatto come "un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli"[7].

QUANDO È (O NON È) NECESSARIA LA VALUTAZIONE D'IMPATTO?

Quando vengono adottate nuove tecnologie per il trattamento dei dati personali o quando viene introdotta una nuova tipologia di trattamento, come prima cosa bisogna effettuare una valutazione del rischio. Se è probabile che la natura dei dati o la modalità di trattamento creino un alto rischio per gli interessati, bisogna fare una valutazione dell'impatto dei trattamenti.

La valutazione dell'impatto *non* è invece necessaria se è improbabile che il trattamento crei un alto rischio per gli interessati, o quando è simile ad altri trattamenti per i quali il titolare ha già effettuato

[6] Gruppo di lavoro articolo 29 per la protezione dei dati, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*, WP 248 rev.01 (ottobre 2017).

[7] *Ibidem*.

una valutazione d'impatto. Il GDPR infatti chiarisce che "Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi" (art. 35, c. 1).

È previsto che le autorità garanti pubblichino un elenco delle tipologie di trattamento che richiedono una valutazione d'impatto sulla protezione dei dati.

COSA SIGNIFICA "ALTO RISCHIO"?

Il GDPR non definisce con precisione quali tipologie di trattamento possano comportare un alto rischio, ma fornisce alcuni esempi, uno dei quali ha buone probabilità di riguardare gli Archivi, ovverosia il trattamento su larga scala di dati relativi a condanne penali o di dati sensibili (quelli che possono rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale) (art. 35, c. 3, lett. b). Inoltre gli Archivi, quando valutano se un trattamento possa comportare rischi elevati per i diritti e le libertà degli interessati, devono considerare se i dati si riferiscono a soggetti particolarmente vulnerabili, come ad esempio malati di mente (considerando 75).

QUAND'È CHE UN ARCHIVIO DEVE EFFETTUARE UNA VALUTAZIONE D'IMPATTO?

Quando un archivio decide di digitalizzare un fondo, o creare uno strumento di ricerca informatico relativo a documenti contenenti dati personali, potrebbe essere necessaria una valutazione dell'impatto del trattamento. È sicuramente opportuno farla se si trattano fondi archivistici contenenti dati sensibili, come cartelle cliniche, fascicoli processuali o fascicoli personali di detenuti.

COSA BISOGNA FARE?

Nello svolgimento della valutazione d'impatto, occorre descrivere sistematicamente i trattamenti previsti e l'interesse legittimo perseguito; devono essere quindi valutati la proporzionalità e la necessità delle attività previste; si devono poi valutare i rischi per i diritti e le libertà degli interessati, per poi redigere un piano dettagliato delle misure da adottare per la gestione dei rischi. Nel corso delle attività di trattamento, queste devono essere regolarmente monitorate e, in caso di necessità, si deve modificare la valutazione d'impatto.

Alcune autorità garanti hanno pubblicato strumenti per aiutare i titolari ad effettuare una valutazione d'impatto. Si veda ad esempio il software gratuito prodotto dal Garante francese https://www.cnil.fr/en/cnil-releases-free-software-pia-tool-help-data-controllers-carry-out-data-protection-impact

QUANDO DEVE ESSERE INFORMATA L'AUTORITÀ GARANTE?

L'autorità di controllo (cioè il Garante) deve essere consultato, nel caso la valutazione d'impatto sulla protezione dei dati "indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio" (art. 36). Se l'autorità di controllo ritiene che il trattamento programmato non sia conforme al regolamento o le misure previste per mitigare il rischio non siano sufficienti, essa deve fornire al titolare del trattamento un parere scritto.

VII. MISURE PER LA TRASPARENZA E PER PROMUOVERE L'OTTEMPERANZA AL GDPR

19. REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO (ART. 30)

L'art. 30, c. 1, stabilisce che "ogni titolare del trattamento e, ove applicabile, il suo rappresentante, tengono un registro delle attività di trattamento svolte sotto la propria responsabilità".

Il registro delle attività di trattamento – o registro dei trattamenti – è

> uno strumento molto utile a coadiuvare l'analisi delle implicazioni di ogni trattamento, già in corso o programmato. Il registro facilita la valutazione fattuale del rischio che le attività di trattamento effettuate da un titolare o da un responsabile possono costituire per i diritti degli individui e agevola l'identificazione e l'implementazione delle misure di sicurezza più appropriate alla salvaguardia dei dati personali – entrambi elementi chiave del principio di responsabilizzazione contenuto nel GDPR[8].

Il registro deve essere tenuto in forma scritta (anche in formato elettronico) e deve essere chiaro e facilmente comprensibile. Dato che le "attività di trattamento" nel contesto del GDPR riguarda le operazioni effettuate su dati personali riferibili ad una persona fisica identificata o identificabile, deve riguardare solo le attività relative ai dati personali.

L'obbligo di tenere un registro delle attività di trattamento non si applica alle organizzazioni con meno di 250 dipendenti a meno che

> non effettuino trattamenti che possono presentare un rischio (anche non elevato) per i diritti e le libertà degli interessati o trattino dati personali in modo non occasionale o tendano a trattare categorie particolari di dati di cui all'art. 9, paragrafo 1, o dati personali relativi a condanne penali e reati di cui all'art. 10. [9]

Se anche solamente una di queste circostanze si verifica – come nel caso di molte, per non dire tutte le istituzioni archivistiche – l'organizzazione è tenuta a dotarsi di un registro delle attività di trattamento.

Su richiesta, gli enti e i loro rappresentanti hanno il dovere di mettere il registro a disposizione dell'autorità di controllo.

Quali informazioni devono essere contenute nel registro delle attività di trattamento.

Il registro deve contenere specifiche informazioni su ogni attività di trattamento svolta:

- Il **nome** e i dati di contatto di:
    - l'Archivio o il suo rappresentante legale;

[8] Article 29 Data Protection Working Party, *Position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*, 19–04-2018.

[9] *Ibidem*.

- se necessario, altre organizzazioni con le quali l'Archivio abbia concordato finalità e mezzi del trattamento;
- il Responsabile della protezione dei dati (DPO), se l'Archivio ne è dotato.

- Le **finalità** per cui l'archivio tratta informazioni personali.

  Analogamente a "ricerca storica", che in passato è già stata riconosciuta come "finalità", indicare "(fini di) archiviazione nel pubblico interesse" dovrebbe essere sufficiente. Non è chiaro se la locuzione "per pubblico interesse" debba essere aggiunta per motivare l'informazione.

- Una descrizione delle **categorie di persone** i cui dati vengono trattati dall'Archivio

  Ad esempio: studenti, militari di leva, imputati, pazienti…

- Una descrizione delle **categorie di dati personali** trattati. Occorre anche indicare l'eventuale trattamento di cosiddetti "dati sensibili", come le informazioni sulla salute o i dati giudiziari.

  Ad esempio: attività professionali, transazioni finanziarie, informazioni relative a condanne penali o reati, dati da cui è possibile desumere l'opinione politica…

- La **data in cui i dati dovranno essere distrutti** (se conosciuta).

  Attenzione: dal punto di vista delle istituzioni archivistiche, è importante precisare ai soggetti produttori d'archivio che "periodo di conservazione" non deve essere confuso con "scarto" dell'informazione, e che essi devono agire in conformità con le leggi archivistiche e con quanto stabilito dai piani di conservazione e massimari di scarto. I dati oggetto di archiviazione nel pubblico interesse non devono mai essere distrutti.

- Le **categorie di destinatari** a cui i gli Archivi comunicano i dati personali.

  Si noti che si sta parlando di "categorie di destinatari", il che vuol dire ad esempio: "università e istituti di ricerca", "singoli ricercatori"…

- L'Archivio condivide dati con un paese straniero o con una organizzazione internazionale al di fuori della UE? In caso, deve indicarlo nel registro.
- Una descrizione generale delle **misure tecniche e organizzative** finalizzate alla sicurezza dei dati personali sottoposti a trattamento, ovvero una descrizione delle tecnologie, applicativi e software usati per il trattamento (che corrisponde a quale tipo di "protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" sia in uso).

Le organizzazioni devono considerare il registro come strumento interno di aiuto per l'attuazione del GDPR. Il registro può contenere ogni altra informazione aggiuntiva considerata importante dal Responsabile protezione dati (DPO) in funzione delle attività svolte, come ad esempio l'indicazione della base legale per il trattamento o una sintesi delle violazioni dei dati personali.

TRATTAMENTI ESTERNALIZZATI

Nota bene: se un Archivio incarica altri soggetti di trattare i dati personali per suo conto, deve firmare con questi un "accordo sul trattamento dei dati", col quale si assicura che questi non usino o trattino i dati personali per proprie finalità.
Si devono affidare incarichi solo a soggetti che possono pienamente garantire l'ottemperanza ai requisiti di legge. Gli Archivi che decidono di esternalizzare attività di trattamento di dati personali restano pienamente responsabili del rispetto del dettato del GDPR.

ALCUNI MODELLI DI REGISTRO SONO DISPONIBILI ONLINE, AD ESEMPIO[10]:

Il modello proposto dall'Autorità di controllo belga, disponibile in francese e fiammingo: https://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement

L'autorità garante francese ha pubblicato due modelli di registro uno più complesso e uno più semplice: https://www.cnil.fr/fr/rgpd-et-tpepme-un-nouveau-modele-de-registre-plus-simple-et-plus-didactique

L'Autorità di controllo dei dati europea (cioè il Garante della protezione dei dati della UE) ha pubblicato un modello di registro: https://edps.europa.eu/data-protection/our-work/publications/other-documents/register-template-0_en

Gli Stati membri possono creare applicativi per la redazione dei registri di trattamento il cui uso è obbligatorio per le pubbliche amministrazioni, come è avvenuto in Belgio.

20. RESPONSABILE DELLA PROTEZIONE DEI DATI (ART. 37): ANCHE GLI ARCHIVI DEVONO DESIGNARLO?

Il responsabile della protezione dei dati (DPO) assiste il titolare o il responsabile del trattamento per tutte le questioni relative alla protezione dei dati personali. I suoi principali compiti sono:

- informare e fornire consulenza al titolare o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle norme nazionali sulla protezione dei dati;
- vigilare sull'osservanza del GDPR;
- fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati;
- cooperare con l'autorità di controllo.

Il GDPR introduce l'obbligo di designare un responsabile della protezione dei dati per le autorità pubbliche e per i soggetti privati che svolgono determinate tipologie di trattamento. Tutte le pubbliche autorità devono avere un responsabile della protezione dei dati, ma questo non significa che ciascun Archivio del settore pubblico debba designarne uno: in molti casi, l'istituzione da cui dipendono dovrà nominare un responsabile della protezione dei dati, sotto la cui responsabilità ricadrà anche l'Archivio. Per esempio, un Comune potrebbe avere un responsabile della protezione dei dati, incaricato di vigilare sull'osservanza del GDPR e di offrire consulenza a tutti gli uffici del Comune, compreso l'Archivio comunale.

[10] In Italia il Garante ha messo a disposizione sul suo sito un modello di "registro semplificato" per le PMI https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento (NdT).

I soggetti privati devono designare un responsabile della protezione dei dati se:

- la loro attività principale richiede un regolare e sistematico monitoraggio degli interessati su larga scala;
- la loro attività principale consiste nel trattamento di dati personali utili a rivelare origini etniche o razziali, opinioni politiche, credenze religiose o filosofiche o iscrizione a sindacati, o nel trattamento di dati genetici, dati biometrici intesi a identificare una persona fisica, dati relativi alla salute, dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica, o dati personali relativi a condanne penali e reati.

È molto improbabile che fondazioni, musei, biblioteche, associazioni culturali o altre organizzazioni private che conservano archivi pratichino "un regolare e sistematico monitoraggio degli interessati su larga scala". Invece, è del tutto possibile che la loro attività principale consista nel trattamento di dati sensibili.

Ci sono infatti fondazioni, Archivi creati da soggetti della società civile e altri enti del settore privato specializzati nella conservazione di archivi prodotti da ONG e organizzazioni per i diritti umani, che possono includere, ad esempio, dati personali che rivelano l'origine razziale o etnica di persone vittime di atti di intolleranza. Come già ricordato, ci sono centri accademici specializzati nello studio del terrorismo o Archivi creati da attivisti antimafia che trattano dati personali relativi a condanne penali e reati. Possono esistere Archivi che conservano fondi archivistici prodotti da organizzazioni femministe dedicate all'assistenza delle donne vittime di violenza, che contengono ogni sorta di dati sensibilissimi.

In tutti questi casi, gli enti privati devono nominare un responsabile per la protezione dei dati, che "può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi" (art. 37, c. 6). I piccoli enti possono condividere lo stesso responsabile della protezione dei dati con altri enti simili. È altamente consigliabile, per i piccoli enti che conservano archivi "per fini di archiviazione nel pubblico interesse" o a scopo di ricerca, di condividere lo stesso responsabile della protezione dei dati con altre organizzazioni simili, in modo che il DPO possa sviluppare una competenza specifica nelle loro particolari tipologie di trattamento di dati personali.

APPENDICI

GLOSSARIO

Archivio. Il GDPR non definisce il termine "archivio"[11]. In queste linee guida, "archivio" è utilizzato per indicare l'insieme dei documenti prodotti e ricevuti da una persona, una famiglia o un ente, pubblico o privato, nel corso della sua attività, e selezionato per la conservazione permanente. In alcune lingue europee, lo stesso termine è utilizzato sia per indicare gli archivi correnti, che gli archivi storici. In questo testo, il termine "archivio" è utilizzato solo nella seconda accezione[12].

Autorità di controllo. L'art. 51 del GDPR stabilisce che ogni Stato membro disponga di una o più autorità pubbliche indipendenti, responsabili di sorvegliare l'applicazione del Regolamento. Queste autorità hanno nomi differenti nei diversi paesi (per esempio, in Finlandia "Office of the Data Protection Ombudsman", in Francia "Commission Nationale de l'Informatique et des Libertés", in Irlanda "Data Protection Commissioner", in Italia "Garante per la protezione dei dati personali") e sono comunemente conosciute come Autorità per la protezione dei dati[13] (*Data Protection Authorities* – DPAs).

Comitato europeo per la protezione dei dati (EDPB). Il GDPR ha sostituito il Gruppo di lavoro articolo 29 con lo EDPB. A differenza del suo predecessore, è stato istituito quale organismo dell'Unione Europea dotato di personalità giuridica ed ha a disposizione una segreteria indipendente. Ha ampi poteri nel dirimere le controversie tra le diverse Autorità di controllo nazionali, nel fornire consulenze e orientamenti sui concetti chiave del GDPR. È composto dalle Autorità di controllo di ciascuno Sato membro e dal Garante europeo della protezione dei dati. La Commissione ha diritto di partecipare alle sue riunioni.

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" (GDPR, art. 4).

[11] Questa affermazione è vera solo in riferimento al testo originale inglese e ad altre traduzioni, ma non alla traduzione italiana, in cui nell'art. 4 *Definizioni* si trova la seguente definizione: "6) «archivio»: 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;". L'espressione inglese che qui è stata erroneamente tradotta con "archivio" è *filing system*, in francese tradotto con *fichier*. In italiano, *filing system* non ha un diretto corrispettivo; la traduzione letterale sarebbe "sistema di archiviazione", tuttavia in questo contesto una traduzione più efficace sarebbe stata "banca dati", anche in considerazione del fatto che il d.lgs. 196/2003 (prima delle modifiche introdotte dal d.lgs. 101/2018) recava all'art. 4, c. 1, una definizione di "banca dati" dal contenuto molto vicino a quello della definizione sopra citata: "p) «banca di dati», qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti" (NdT).

[12] In italiano, "Archivio" capitalizzato è stato utilizzato per indicare un istituto che conserva archivi (NdT).

[13] In italiano è anche in uso l'espressione "autorità garanti" (NdT).

Gli archivisti devono ricordare che il GDPR protegge solamente i dati personali delle persone in vita. Tuttavia gli Stati membri possono dettare norme sulla protezione dei dati personali anche delle persone decedute[14].

Garante europeo della protezione dei dati (EDPS): È l'organismo indipendente dell'Unione Europea responsabile di monitorare l'applicazione delle regole sul trattamento dei dati personali da parte delle istituzioni europee e di esaminare i reclami.

Garante per la protezione dei dati personali: vedi Autorità di controllo

Gruppo di lavoro articolo 29: Gruppo di lavoro creato in esecuzione dell'art. 29 della Direttiva 95/46/CE. Era composto dai rappresentanti delle autorità garanti degli Stati membri, dal Garante europeo della protezione dei dati e da un rappresentante della Commissione. Ha cessato di esistere il 25 maggio 2018, sostituito dal Comitato europeo per la protezione dei dati.

Interessato: la persona a cui si riferiscono i dati trattati.

Pseudonimizzazione: "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile" (GDPR, art. 4).
È importante notare che il GDPR suggerisce l'opzione della pseudonimizzazione dei dati personali conservati per fini di archiviazione nel pubblico interesse o a scopo di ricerca storica, mentre non parla mai di "anonimizzazione". A differenza della anonimizzazione, la pseudonimizzazione mantiene la correlazione tra i diversi dati che si riferiscono ad una stessa persona, così come la relazione tra i diversi record di dati. I dati personali pseudonimizzati mantengono la natura di dati personali e sono dunque soggetti alle disposizioni del GDPR.

Responsabile del trattamento: "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento" (GDPR, art. 4).

Responsabile della protezione dei dati (DPO): il responsabile della protezione dei dati assiste il titolare del trattamento e il responsabile del trattamento per tutte le questioni relative alla protezione dei dati personali. Il GDPR introduce l'obbligo di designazione del responsabile della protezione dei dati per le pubbliche amministrazioni e per i privati che svolgono determinate attività di trattamento dei dati.

Titolare del trattamento: "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" (GDPR, art. 4).

Trattamento: "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" (GDPR, art. 4).

[14] In Italia il legislatore si è avvalso della facoltà concessa dal GDPR agli Stati membri di introdurre norme anche relative ai dati delle persone decedute, con l'art. 2-terdecies del d.lgs. 196/2003, come modificato dal d.lgs 101/2018 (NdT).

Gli archivisti devono tenere presente che attività come la selezione di documenti contenenti dati personali ai fini della conservazione permanente, il loro trasferimento in un Archivio, il loro ordinamento, la loro descrizione e il renderli disponibili agli utenti sono tutte attività considerate "trattamento di dati personali" ai sensi del GDPR.

Violazione dei dati personali: "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" (GDPR, art. 4).
Questa definizione è della massima rilevanza per gli archivisti, perché implica che, se i dati personali sono stati selezionati per la conservazione permanente ed affidati alla custodia di un Archivio, gli archivisti devono preservarne l'integrità. Fra i principi applicabili al trattamento dei dati personali, il Regolamento include, infatti, "integrità e riservatezza" (art. 5). Perdite accidentali o alterazioni dei dati costituirebbero una violazione non solo dell'etica archivistica, ma anche del GDPR. Lo stesso dicasi se gli archivisti permettono, in assenza di autorizzazione, l'accesso ai dati personali o la loro divulgazione.

DOVE TROVARE ALTRE INDICAZIONI

- La Commissione europea ha creato, all'interno del suo sito web, una sezione intitolata "Protezione dei dati. Norme per la protezione dei dati personali all'interno e all'esterno dell'UE" (https://ec.europa.eu/info/law/law-topic/data-protection_it) dove sono pubblicate alcune FAQ sul GDPR (Che cosa sono i dati personali? Cosa costituisce trattamento dei dati? Chi sono le autorità per la protezione dei dati? Ecc.) rivolte ai lettori alle prime armi.

- *Manuale sul diritto europeo in materia di protezione dei dati*, edizione 2018 – http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law. Il manuale è stato redatto congiuntamente dall'Agenzia dell'Unione europea per i diritti fondamentali (FRA), dal Consiglio d'Europa (con la cancelleria della Corte europea dei diritti dell'uomo) e dal Garante europeo della protezione dei dati. Fornisce una panoramica della normativa in materia di protezione dei dati personali della Unione Europea e del Consiglio d'Europa, e illustra la giurisprudenza fondamentale della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo.

- Il Comitato europeo per la protezione dei dati (EDPB) pubblica linee guida, raccomandazioni e buone pratiche. È quindi utile tenere d'occhio il suo sito https://edpb.europa.eu/edpb_it, che è in tutte le lingue dell'Unione (anche se, per il momento, parecchi documenti sono disponibili solo in inglese). Durante il suo primo giorno di attività, il Comitato europeo per la protezione dei dati ha approvato le linee guida pubblicate dal suo predecessore, il "Gruppo di lavoro Articolo 29".

- Il "Gruppo di lavoro Articolo 29 in materia di protezione dei dati personali" (che ha cessato di esistere il 25 maggio 2018) ha pubblicato nove linee guida e altri documenti relativi all'applicazione del GDPR, per contribuire ad una interpretazione e applicazione uniforme da parte delle diverse Autorità di controllo e dei Governi dell'Unione. Il Comitato europeo per la protezione dei dati (EDPB) li ha tutti approvati e resi disponibili sul proprio sito https://edpb.europa.eu/edpb_it.

  - *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679* (wp259 rev.01) 16-04-2018
  - *Linee guida sulla trasparenza ai sensi del regolamento 2016/679* (wp260rev.01) 13-04-2018
  - *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679* (wp251 rev.01) 06-02-2018
  - *Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679* (wp250 rev.01) 06-02-2018
  - *Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679*, (WP 253) 3-10-2017.
  - *Linee guida per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento* (wp244 rev.01) 5-04-2017
  - *Linee guida sui responsabili della protezione dei dati (RPD)* (wp243rev.01) 5-04-2017
  - *Linee guida sul diritto alla portabilità dei dati* (wp242rev.01) 05-04-2017

- *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*, WP 248 rev.01 (ottobre 2017).
- *Position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*, 19–04-2018.[15]

- Le Autorità garanti degli Stati membri stanno pubblicando materiali informativi come opuscoli, fogli informativi, infografiche e altro, allo scopo di spiegare ai cittadini i loro nuovi diritti e aiutare le pubbliche amministrazioni e le piccole e medie imprese ad ottemperare al GDPR. Controllate il sito della vostra autorità garante! Le loro coordinate possono essere trovate qui: https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm.

- Il Garante europeo della protezione dei dati ha pubblicato sul suo sito web un *Glossario* (in inglese, francese e tedesco: https://edps.europa.eu/data-protection/data-protection/glossary_en) che include più di 70 termini, una biblioteca virtuale (Reference Library https://edps.europa.eu/data-protection/data-protection/reference-library_en) e altri materiali informativi, finalizzati soprattutto a guidare le istituzioni europee nell'applicazione del GDPR, ma che possono essere utili anche per enti pubblici e privati nazionali.

- I National Archives del Regno Unito, in collaborazione con altre autorità responsabili in materia di archivi e la Archives and Records Association, ha preparato una *Guide to archiving personal data*[16] (Guida all'archiviazione dei dati personali), che ha reso disponibile gratuitamente sul suo sito. Può essere una lettura utile anche per archivisti di altri paesi membri, a patto che non dimentichino che si tratta di una guida per lo specifico contesto giuridico britannico.
  http://www.nationalarchives.gov.uk/information-management/legislation/data-protection/

[15] Disponibile solo in inglese (NdT).

[16] Disponibile solo in inglese (NdT).

APPENDICE ALLA EDIZIONE ITALIANA

Nell'ordinamento della UE, i regolamenti sono l'equivalente di ciò che per gli Stati sono le leggi: sono direttamente applicabili in tutti i paesi membri, in tutte le loro parti, e i paesi non devono adottare provvedimenti per la loro attuazione (a differenza di ciò che avviene per le direttive). Però il GDPR ha lasciato ai paesi membri l'autonomia di regolare alcune materie, fra cui le deroghe in caso di "archiviazione nel pubblico interesse". È dunque necessario che gli archivisti, oltre al GDPR, conoscano la normativa nazionale.

Il Decreto legislativo 101/2018[17] ha adattato la normativa italiana al GDPR, abrogando tutti gli articoli del d. lgs. 196/2003 *Codice in materia di protezione dei dati personali* incompatibili con il GDPR, emendando vari degli articoli sopravvissuti ed introducendone di nuovi.

Per gli archivisti è essenziale sapere che:

- il vecchio *Codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici* (all. 2 al d.lgs.196/2003) è stato aggiornato nei riferimenti normativi, emendato (in modo marginale), e ribattezzato: *Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica* (Pubblicate sulla Gazzetta Ufficiale n. 12 del 15 gennaio 2019)[18].
  "Il rispetto delle disposizioni contenute nelle regole deontologiche (…) costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali" (d.lgs.196/2003 art. 2-quater c. 4).
  Per gli archivisti, le *Regole deontologiche* sono la bussola che deve sempre orientarne il comportamento, quando trattano dati personali.
- La facoltà che il GDPR conferisce agli Stati membri di introdurre deroghe ai diritti di cui agli articoli 15, 16, 18, 19, 20 e 21, in caso di trattamenti a fine di "archiviazione nel pubblico interesse", in Italia è stata esercitata mediante le *Regole deontologiche*, che all'art. 7 prevedono le modalità specifiche con cui si esercitano i diritti di rettifica e di accesso relativamente ai dati personali contenuti nei fondi archivistici.
- In Italia, la legge protegge i dati personali anche delle persone decedute. La materia è regolata dall'art. 2-terdecies (*Diritti riguardanti le persone decedute*) del d.lgs.196/2003, nonché dalle *Regole deontologiche* (art. 7 c. 3 e *passim*).
  Com'è noto, l'art. 122 del d.lgs 42/2004, relativo alla consultabilità dei documenti d'archivio, prevede l'esclusione dalla consultazione per 40 o 70 anni dei documenti contenenti determinate categorie di dati personali, indipendentemente dall'esistenza in vita o meno dell'interessato; implicitamente, dunque, anche il *Codice dei beni culturali* prevede la tutela dei dati personali dei defunti, se di data più recente rispetto ai termini di consultabilità.
- Permane, nell'ordinamento italiano, la distinzione tra "comunicazione" e "diffusione" dei dati personali (d.lgs.196/2003, art. 2-ter, c. 4).

[17] D. lgs. 10 agosto 2018, n. 101 *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE(regolamento generale sulla protezione dei dati)*

[18] Il cambio di denominazione si deve alla necessità di evitare confusione con i codici di condotta previsti dall'art. 40 del GDPR.

- Il d.lgs.196/2003, art. 2-sexies, riconosce il rilevante interesse pubblico, fra gli altri, dei "trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante (…)" (c. 2, lett. cc)
  Questo vuol dire che tali trattamenti sono leciti, anche in assenza di consenso da parte degli interessati (GDPR art. 6, c. 1 lett. e).

- Prima delle modifiche introdotte dal d.lgs 101/2018, il *Codice in materia di protezione dei dati personali* definiva come "dati sensibili", i dati relativi alla salute, alla vita sessuale, alle opinioni politiche, all'origine etnica ecc. Ora la definizione "dati sensibili" è stata abrogata (perché il GDPR non la utilizza) e dove prima il *Codice* usava questa espressione, ora si trova un riferimento alle categorie particolari di dati personali di cui all'art. 9 del GDPR.
- Prima delle modifiche introdotte dal d.lgs 101/2018, il *Codice in materia di protezione dei dati personali* definiva come "dati giudiziari" i dati del casellario giudiziale e dell'anagrafe delle sanzioni amministrative, dei carichi pendenti e della qualità di imputato o indagato. Ora la definizione di "dati giudiziari" è stata abrogata (perché il GDPR non la utilizza) e dove prima si usava questa espressione, ora si trova un riferimento ai dati di cui all'art. 10 del GDPR (ovverosia "dati personali relativi a condanne penali e a reati e a connesse misure di sicurezza").
- Il Garante per la protezione dei dati personali ha creato sul suo sito un'ampia sezione dedicata al GDPR, contenente molti materiali scaricabili gratuitamente, che vanno da opuscoli introduttivi per chi è del tutto digiuno della materia, a testi di approfondimento, strumenti di lavoro e linee guida. https://www.garanteprivacy.it/regolamentoue