SEMINARIO DI FORMAZIONE PER PROFESSIONISTI ED IMPRESE

COMPLIANCE AZIENDALE

LA RESPONSABILITÀ DEGLI ENTI ED I MODELLI ORGANIZZATIVI DI PREVENZIONE E REPRESSIONE DEI REATI E LA NORMATIVA IN TEMA DI PRIVACY

LA NORMATIVA IN TEMA DI PRIVACY

QUARTO MODULO

LA NORMATIVA IN TEMA DI PRIVACY

Dott. Michele Giordano, Avv. Paola Casaccino, Avv. Alessandro Legnante

Compliance, Governance & Organisation

Studio Associato - Consulenza legale e tributaria

FONDAZIONE per la FORMAZIONE FORENSE dell'ORDINE degli AVVOCATI di FIRENZE - SCUOLA FORENSE

Fondazione dei Dottori Commercialisti e degli Esperti Contabili di Firenze

La difesa è diritto inviolabile

Articolo 24

Gruppo di Studio Penale e Civile

www.articolo24.net

KPMG

Regolamento 679/2016

Evoluzione della Normativa (1/2)

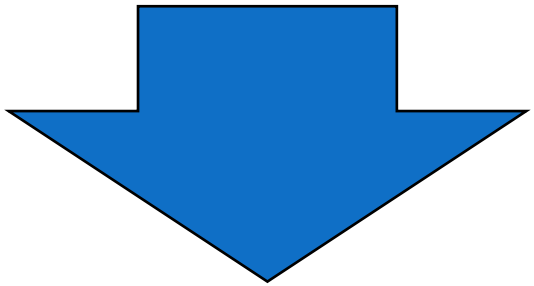
FONTI

- 1995 Direttiva Europea 95/46
- 1996 D. Lgs 675/1996
- 2001 Carta dei diritti fondamentali dell'Unione Europea – Carta Europea di Nizza
- 2002 Direttiva 2002/58/CE relativa al trattamento dei dati personali della vita privata nel settore delle comunicazioni elettroniche
- 2003 D. Lgs. 196/2003 – Codice della Privacy
- 2009 Trattato di Lisbona
- **2016 Regolamento Europeo sulla Privacy 2016/679**
- 2018 D. Lgs 51/2018 trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali
- **2018 D. Lgs 101/2018** c.d. «Decreto di armonizzazione»
- *Provvedimenti, Linee Guida, etc. dell' Autorità Garante e EDPB*

Evoluzione della Normativa (2/2)

REGOLAMENTO EUROPEO 679/2016

- Approvato il *27/04/2016*
- Pubblicato il *04/05/2016*
- In vigore dal *24/05/2016*
- Si applica dal *25/05/2018* (art. 99)
- Composto da ***173* considerando (???) e *99* Articoli**



FINALITA' *: assicurare un livello coerente di protezione delle persone in tutta l'Unione*

Obiettivo

REGOLAMENTO EUROPEO 2016/679

Ha in generale l'obiettivo di ***proteggere i diritti e le libertà delle persone fisiche*** *in ordine al trattamento dei dati personali*

Il Regolamento Europeo - *General Data Protection Regulation* – è, infatti, un quadro normativo comune in materia di tutela dei dati personali per tutti gli Stati Membri che ha l'obiettivo di uniformare ed armonizzare la disciplina all'interno dell'Unione Europea al fine di proteggere i dati personali delle persone fisiche.

Approccio

Considerando nr. 6

*La **rapidità dell'evoluzione tecnologica e la globalizzazione** comportano nuove sfide per la protezione dei dati personali.*

*La portata della **condivisione e della raccolta di dati personali** è aumentata in modo significativo. La **tecnologia** attuale consente tanto alle imprese quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza.*

*Sempre più spesso, le **persone fisiche rendono disponibili al pubblico** su scala mondiale informazioni personali che li riguardano.*

La tecnologia dovrebbe facilitare ancora di più la libera circolazione dei dati personali, garantendo al tempo stesso un elevato livello di protezione dei dati personali

Definizioni Chiave

1) **«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;

2) **«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;

Definizioni Chiave

3) **«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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

4) **«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;

5) **«consenso dell'interessato»:** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Definizioni Chiave

CATEGORIE PARTICOLARI DI DATI

Non esiste più una specifica definizione di dati personali "*sensibili*" o di dati personali "*giudiziari*", ancorchè la definizione sia ricavabile dagli articoli generali dedicati a queste categorie di informazioni.

L'articolo 9, difatti, individua in generale le **"*categorie particolari di dati personali*"** nelle informazioni "*che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona fisica*".

Il Regolamento introduce comunque **una nuova definizione limitata ai "*dati relativi alla salute*"** intesi quali i "*dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*".

L'articolo 10 del Regolamento disciplina poi il trattamento dei "***dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza*".**

Ambito di Applicazione

AMBITO APPLICAZIONE MATERIALE

Il Regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Eccezioni (!)

Il Regolamento **non si applica** ai trattamenti di dati personali:

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;

c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.

Ambito di Applicazione - Territoriale

AMBITO APPLICAZIONE TERRITORIALE

Il Regolamento si applica :

1) al trattamento di dati personali effettuato da un **titolare stabilito nella UE**;

ma anche

2) al trattamento di dati personali effettuato da **titolari non stabiliti nell'Unione Europea** se il **trattamento ha ad oggetto dati personali di interessati che si trovano nella UE** e riguarda
(1) **l'offerta di beni o servizi** (anche non a pagamento) ai suddetti interessati
(2) il **monitoraggio** del loro comportamento nel territorio dell'Unione Europea.

Modifiche alla Disciplina Esistente

Principali Modifiche

- Consenso (art. 7)
- Informativa (artt. 12 ss.)
- Diritto di accesso dell'interessato (artt. 15 ss)
- Diritto all'oblio (art.17)
- Compiti del responsabile (art. 28)
- Sicurezza del trattamento (art. 32)
- Sanzioni (artt. 82 e ss)

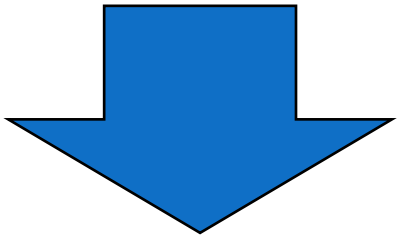
Principali Novità

- Diritto alla ***portabilità*** dei dati (art. 20)
- ***Accountability***
- ***Trasparenza*** (art. 24)
- ***Privacy by design and by default*** (art. 25)
- ***Registro dei trattamenti*** (art. 30)
- ***Notifica*** della violazione dei dati personali (art. 33)
- ***Valutazione*** di impatto (art. 35)
- ***Data protection officer*** - responsabile della protezione dei dati (art. 37)

Wrap Up

Cambiamento Radicale di Approccio

Compliance Formale / Compliance Sostanziale



Centralità Interessato e

Responsabilizzazione del Titolare

Il Decreto legislativo n. 101/2018

Premessa

• Anche se il Regolamento è **direttamente applicabile** e vincolante in tutti gli Stati membri dell'Unione europea, in quanto non richiede una legge di recepimento nazionale, diverse sue disposizioni lasciano liberi gli Stati Membri - o richiedono agli stessi - di introdurre **ulteriori regole e condizioni**

• Gli Stati hanno avuto due anni per porre in essere gli adeguamenti richiesti dalla normativa in questione alle proprie politiche per la protezione ed il trattamento dei dati personali.

• Infatti, oltre al Regolamento, del pacchetto di riforma, fa parte una Direttiva indirizzata alla regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali.

• Esistono dei campi d'azione in cui il regolamento cede il passo alla normativa nazionale, laddove manca un'armonia a livello sovranazionale.

D.Lgs. 10 agosto 2018, numero 101

GAZZETTA UFFICIALE
DELLA REPUBBLICA ITALIANA

Il Decreto legislativo 10 agosto 2018, numero 101, è stato pubblicato nella Gazzetta Ufficiale – Serie Generale del 4 settembre 2018, numero 205.

Il provvedimento, finalizzato ad adeguare il quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679, si compone di 27 articoli che apportano modifiche al Codice in materia di trattamento dei dati personali di cui al Decreto legislativo n. 196/2003 ed entrerà in vigore il **19 settembre 2018**.

Iter di Emanazione

L’iter di emanazione del Decreto 101/2018 attuativo del Nuovo Regolamento europeo è stato molto sofferto; prima di giungere all’emanazione sono stati vari i cambi di rotta sul Tavolo dei lavori:

- nella **prima fase** la Commissione sembrava infatti più propensa ad **abrogare “in toto”** il vecchio codice privacy con l’obiettivo di alleggerire e semplificare la disciplina;

- ad una **seconda valutazione**, è cambiato totalmente l’orientamento optando per una decretazione “modificatrice ed integrativa”. A tale impostazione si è addivenuti nella **considerazione e nella consapevolezza di dover armonizzare ed inserire nuove indicazioni e disposizioni in un contesto caratterizzato ancora da “scarsa cultura della privacy”** ed in un ambito normativo già ben stratificato e con non poche complessità pregresse.

Duplice Scopo

La necessità di emanare il Decreto 101/2018 trova dunque il suo fondamento nell'esigenza di contemperare un **duplice scopo**:

- il primo "**abrogativo**", si procede all'abolizione di alcune disposizioni del vecchio codice: principi, diritti degli interessati, obblighi generali di titolari e responsabili, misure di sicurezza, adempimenti e notifiche nei confronti dell'Autorità;

- il secondo "**innovativo**", con l'inserimento e la modifica di nuove disposizioni perseguendo l'ambizione di completare il quadro della "nuova privacy" adeguando le vecchie disposizioni del Codice privacy rimanenti in vigore in una nuova rilettura tutta "europea" disciplinata dal GDPR.

Principi Consenso e Informativa (1/2)

Consenso dei minori in relazione ai servizi della società dell'informazione (Art.2-quinquies)

L'età minima richiesta al minore per esprimere il consenso è stata abbassata a 14 anni. Sotto tale soglia il consenso per essere ritenuto lecito dovrà essere prestato da chi esercita la potestà genitoriale.

Trattamento dei dati sanitari, genetici e biometrici (Art.2-septies, Art.100, Art. 104, Art. 110)

Non occorre più il consenso per il trattamento dei dati sanitari, genetici e biometrici se tali dati vengono trattati per finalità di diagnosi, cura, ricerca scientifica, biomedica o epidemiologica. Vista la "particolarità" dei dati sarà il Garante a dare indicazione sulle "misure di garanzia" da adottare nel trattamento di tali dati.

Trattamento di dati per fini di rilevante interesse pubblico (Art.2-sexies)

Viene individuato un elenco di trattamenti per categorie "particolari" di dati il cui trattamento trova legittimazione nel presupposto che vengano effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (accesso a documenti amministrativi e accesso civico, tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, delle liste elettorali, rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità, tenuta di registri pubblici relativi a beni immobili o mobili, tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli, cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato.)

Principi Consenso e Informativa (2/2)

Informativa ed invio di curriculum (Art.111-bis)

L'informativa privacy secondo le nuove indicazioni, potrà essere resa anche successivamente, ovvero al momento del primo contatto utile con il soggetto che ha proposto la sua candidatura con l'invio spontaneo del proprio curriculum, al fine della instaurazione di un rapporto di lavoro.

Figure intermedie operanti sotto l'autorità del titolare o responsabile (Art.2-quaterdecies)

Viene introdotta la figura del "soggetto designato" o "autorizzato". Il Titolare ed il Responsabile, infatti, potranno delegare compiti e funzioni specifiche che il soggetto nominato dovrà svolgere sotto la loro diretta autorità e responsabilità.

Diritti dell'Interessato

Esercizi dei diritti dell'interessato – Limitazioni (artt. 2-undecies e 2-duodecies)

I diritti riconosciuti all'interessato dal Regolamento (GDPR) non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto su interessi normativamente tutelati (antiriciclaggio, sostegno delle vittime di atti estorsivi, attività delle commissioni parlamentari d'inchiesta, controllo dei mercati finanziari e monetari, esercizio di diritti in sede giudiziaria e per ragioni di giustizia, indipendenza della magistratura). Diritto all'eredità del dato in caso di decesso (Art.2 –terdecies).I diritti riferiti a persone decedute possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato, in qualità di suo mandatario o per ragioni familiari meritevoli di protezione.

Autorità di Controllo (1/2)

Forma di tutela alternativa per l'interessato (Art.140-bis)

Qualora l'interessato ritenga che i diritti di cui gode in base alla normativa sulla protezione dei dati siano stati violati deve scegliere quale forma di "tutela" attivare. Potrà scegliere di proporre il reclamo dinanzi al Garante o in alternativa il ricorso dinanzi all'Autorità giudiziaria competente. Una forma di tutela esclude l'altra.

Rafforzamento dell'indipendenza dei poteri e dei compiti del Garante (Art.2 quater)

Estensione e rafforzamento dei poteri del Garante (emanazione di provvedimenti specifici in merito al trattamento di dati particolari ; emanazione di provvedimenti che diano indicazione sulle "misure di sicurezza" anche tecniche necessarie a garantire i diritti degli interessati; adozione di provvedimenti riguardanti codici di condotta e regole deontologiche).

Modalità semplificate per le PMI (Micro, piccole e medie imprese) (Art.154-bis)

Il Garante dovrà adottare linee guida di indirizzo riguardanti le misure organizzative e tecniche di attuazione dei principi del Regolamento predisponendo nello specifico, modalità semplificate di adempimento degli obblighi del titolare del trattamento delle micro, piccole e medie imprese.

Legittimazione ad agire in giudizio del Garante (Art. 154-ter)

L'Autorità del Garante può agire in giudizio nei confronti del titolare o del responsabile in caso di violazione delle disposizioni in materia di protezione dei dati personali.

Autorità di Controllo (2/2)

Legittimazione ad agire in giudizio del Garante (Art. 154-ter)

L'Autorità del Garante può agire in giudizio nei confronti del titolare o del responsabile in caso di violazione delle disposizioni in materia di protezione dei dati personali.

Segnalazione all'Autorità del Garante (Art. 144)

Chiunque può rivolgere una segnalazione che il Garante può valutare anche ai fini dell'emanazione dei provvedimenti di cui all'articolo 58 del Regolamento.

Sanzioni

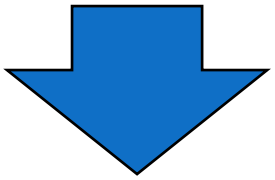
Sanzioni Amministrative Pecuniarie (Art. 166)

Sono definiti i criteri di applicabilità delle sanzioni amministrative pecuniarie di cui all'art. 83 GDPR.

Con il Decreto attuativo n. 101/2018 si definiscono i criteri secondo i quali applicare le sanzioni. Dall'applicazione delle sanzioni di minore entità, che possono raggiungere i 10 milioni di euro per i singoli e per le aziende fino al 2% del fatturato globale annuo riguardanti la violazione degli obblighi previsti per i titolari ed i responsabili, a quelle di maggiore entità, che possono arrivare a 20 milioni di euro per i singoli o fino al 4% del fatturato mondiale annuo per le aziende, a prescindere da dove sia la sede principale che può essere anche fuori dall'Europa.

Sanzioni penali (artt.167 e ss.)

Vengono introdotti reati più specifici in relazione al "Trattamento dei dati". Le sanzioni prevedono misure che vanno da 6 mesi fino ad arrivare ai casi più gravi a 6 anni di reclusione…



To be continued…

Alessandro Legnante

Senior Legal Specialist

Governance, Compliance & Organisation
Studio Associato KPMG
E: alegnante@kpmg.it

Mob. +39 3455989855

La Governance Privacy

Agenda

I. Introduzione
II. Il Governo del dato
III. Accountability e SGP
IV. Il processo per definire il Sistema di Gestione Privacy
V. Il SGP: focus procedure minime
VI. Il SGP: focus governance
VII. Il monitoraggio e controllo
VIII. Sistema di gestione integrato

La Governance ed il Sistema di Gestione Privacy: introduzione

Tra le novità principali, introdotte dal nuovo Regolamento privacy Ue, si evidenziano due elementi concettuali:

- **Il sistema di gestione e controllo** sul trattamento dei dati personali costituito dai seguenti elementi: **valutazione del rischio; accountability; misure giuridiche, organizzative e tecniche; sistema sanzionatorio a protezione dei dati personali; audit e monitoraggio;**
- **La governance sul sistema di gestione privacy.**

Tali concetti possono essere individuati nei seguenti profili normativi:

- il **principio dell'accountability** inteso come responsabilità e prova della responsabilità che il trattamento dei dati personali effettuato è conforme al Regolamento;
- i titolari del trattamento, sia pubblici che privati, dovranno dimostrare di aver effettuato analisi di privacy risk assessment a tutela dei dati **(*Data Protection Impact Assessment*);**
- i titolari del trattamento dovranno dimostrare di aver adottato misure tecniche ed organizzative adeguate per la tutela dei dati e di aver effettuato una valutazione preventiva ex ante su nuovi prodotti, tecnologie…sin dalla loro progettazione **(P*rivacy by design*);**
- I titolari del trattamento dovranno dimostrare di aver adottato misure tecniche e organizzative capaci di garantire che vengano trattati solo i dati personali necessari (pertinenti e non eccedenti) rispetto alle finalità perseguite **(P*rivacy by default*);**
- il ruolo di sorveglianza e la responsabilità del ***protection officer***, che diventa obbligatorio in tutta una serie di casistiche, avrà un ruolo significativo anche nella dialettica della responsabilità giuridica ascrivibile al titolare del trattamento, sotto il profilo della *culpa in eligendo* e in vigilando;
- il nuovo **quadro sanzionatorio** caratterizzato da sanzioni che potranno arrivare sino al 4% del fatturato mondiale annuo, in caso di violazioni particolarmente gravi;
- codici di condotta **come linea guida per la corretta applicazione del Regolamento, in funzione delle specificità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese;**
- **la certificazione** (ancora non disciplinata) per la corretta applicazione del Regolamento intesa come verifica ex post della conformità delle misure adottate.

La Governance ed il Sistema di Gestione Privacy: introduzione

A distanza di circa 5 anni dalla entrata in vigore del Reg. (UE) 2016/679 (“GDPR”), ed a seguito delle modifiche al Codice Privacy di cui al D.lgs. 101/2018, le tematiche della Governance e dei Controlli in materia di protezione dei dati personali hanno acquisito un'importanza sempre maggiore nella definizione delle strategie e dei contenuti dei Sistemi di Gestione della Privacy (nel seguito anche SGP), imponendo una specifica valutazione sul “Governo del Dato”, attenzionandone le modalità operative e la trasparenza delle regole in ottica di adeguatezza e proporzionalità in relazione alle dimensioni e complessità degli specifici contesti aziendali.

La Governance ed il Sistema di Gestione Privacy: il governo del dato

Con l'espressione "Governo del Dato" riferita al trattamento dei dati personali possiamo intendere il sistema di regole che deve essere definito per determinare nella propria struttura organizzativa: ruoli, compiti, responsabilità, procedure e policy, controlli e monitoraggi, flussi informativi, e rendicontazione delle attività. In sostanza si tratta di introdurre e definire un SGP in modo che sia chiaro:

a. quali siano i contenuti del SGP in relazione allo specifico contesto aziendale;

b. quale siano la metodologia e la logica di risk-based da adottare;

c. quale sia la leadership, quali siano i ruoli e le responsabilità, ovvero:

- chi può prendere decisioni;
- chi deve conformarsi alle decisioni;
- quale sia il processo che governa le suddette decisioni dalla fase della progettazione alla fase dell'implementazione e successiva verifica;
- quali siano, infine, le responsabilità sia in capo a colui che decide sia in capo a colui che deve eseguire le decisioni;

a. quali siano i livelli di controllo;

b. come viene gestito l'esercizio del potere di controllo datoriale;

c. quali siano i flussi informativi tra gli attori del SGP;

d. come attuare la rendicontazione delle attività svolte e implementare le azioni di miglioramento.

La Governance ed il Sistema di Gestione Privacy: accountability e SGP

Un ulteriore campo di applicazione dei principi di data governance è sicuramente da individuarsi in relazione al principio di accountability.

Con tale principio si costituisce un vero e proprio meccanismo di responsabilità in capo ai titolari, i quali dovranno intervenire nella definizione dei processi e nell'attuazione delle misure o procedure da adottare e, in più, dovranno anche poter dimostrare il fondamento delle scelte effettuate e la loro implementazione.

Si può quindi ritenere che il primo obiettivo dell'accountability sia la formalizzazione di scelte che sono demandate al titolare affinché questi possa implementare gli elementi di governance ritagliati sulla propria realtà concreta. Questa lettura del principio, tuttavia, ha anche il pregio di trasferire in politiche concrete, attraverso il SGP, i principi che sono contenuti nella normativa, personalizzandole sulla realtà nella quale andranno operativamente a ricadere.

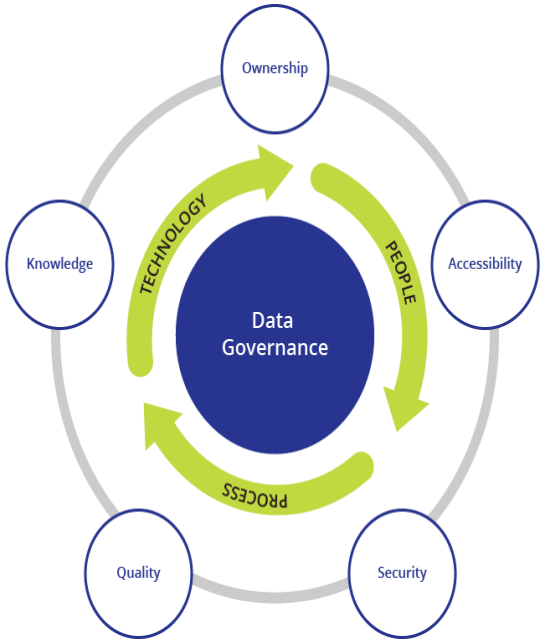
La Governance ed il Sistema di Gestione Privacy: framework

In sintesi, per governance dei dati si intende un insieme di processi, ruoli, policy, standard e metriche finalizzato a garantire un uso efficace ed efficiente delle informazioni, che permetta a un'organizzazione di raggiungere gli obiettivi prefissati.

Stabilisce processi e responsabilità che assicurano la qualità e la sicurezza dei dati impiegati all'interno di un'organizzazione aziendale.

La governance dei dati definisce chi può intraprendere determinate azioni, su quali dati, in quali situazioni e utilizzando quali metodi.

Una strategia di Governance dei dati ed il conseguente SGP se ben concepito è fondamentale per la gestione di ogni trattamento dei dati, in quanto aiuta a definire come l'azienda può trarre vantaggio da processi e responsabilità coerenti e comuni.



La Governance ed il Sistema di Gestione Privacy: dati e processi aziendali

Processi aziendali e di gestioni dati

L'attuazione di una data governance dovrà quindi necessariamente passare attraverso una preliminare fase di studio e individuazione delle caratteristiche **tipiche della propria struttura** e dei **processi** che sovrintendono alla gestione dei dati per tutto il loro ciclo di vita (raccolta, trattamento, trasferimento, messa in sicurezza e distruzione del dato stesso).

Processo Aziendale	Processo Dati
➢ HR ➢ Sales ➢ IT ➢ E-Commerce ➢ Marketing ➢ Product Customization ➢ Finance and Amministration	➢ Raccolta ➢ Trattamento ➢ Trasferimento ➢ Messa in sicurezza ➢ Distruzione

N.B. Ad ogni processo aziendale corrisponde un Processo dei dati.

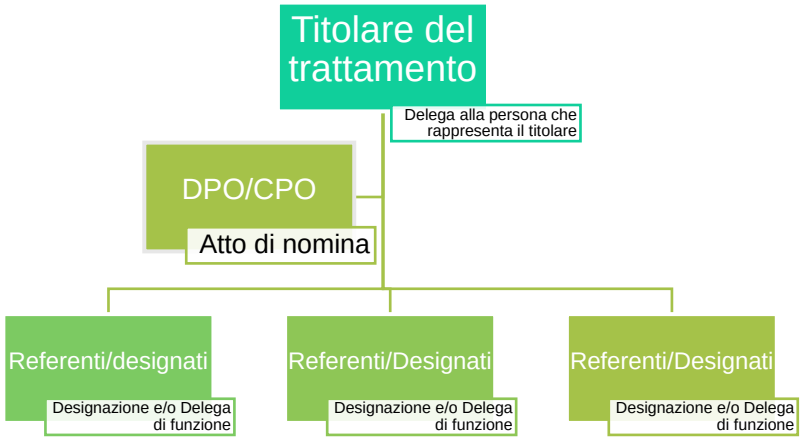
La Governance ed il Sistema di Gestione Privacy: il processo e gli elementi che definiscono il SGP

La Governance ed il Sistema di Gestione Privacy: focus governance

Con il D.Lgs 101/2018 il legislatore Italiano ha voluto far chiarezza sulla punto della previsione di ruoli interni alle organizzazioni per la gestione dei dati personali. Questo provvedimento integra il Codice della privacy con la disposizione dell' Art. 2 quaterdecies "Attribuzione di funzioni e compiti ai soggetti designati".

Tale disposizione ribadisce l'importanza dell'implementazione di una organizzazione interna ai fini privacy in conformità al principio di *accountability* e, quindi, l'importanza di una corretta distribuzione di ruoli e responsabilità.

D. Lgs 101/2018	
Art. 2 quaterdecies "Attribuzione di funzioni e compiti ai soggetti designati"	Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalita' piu' opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.



La Governance ed il Sistema di Gestione Privacy: focus governance

Ai sensi dell'articolo 4 del GDPR, il Titolare del trattamento (soventemente chiamato in lingua inglese "*data controller*") è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*" (art. 4. par. 1, n. 7 GDPR).

Nel caso di società il Titolare del trattamento dei dati è la persona giuridica, che agisce tramite il suo rappresentate legale.

Compiti e Responsabilità

- adotta le misure tecniche e organizzative adeguate per garantire, sin dalla fase della progettazione, la tutela dei diritti dell'interessato (privacy by design) e per garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente;
- dispone di vincoli al dovere di riservatezza dei dati, inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento operato;
- fornisce l'informativa ex art. 13 GDPR agli interessati;
- procede a valutazioni d'impatto (c.d. DPIA);
- procede alla designazione dei responsabili, designati ed autorizzati del trattamento;
- redige il registro di trattamenti;
- forma il personale;
- documenta la violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio;
- svolge ulteriori compiti ad esso attribuiti dalla normativa di riferimento.

La Governance ed il Sistema di Gestione Privacy: focus governance

Il Responsabile del trattamento è definito dall'art. 4, par. 8 del GDPR come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*". L'art. 28 disciplina nel dettaglio i requisiti di tale figura affermando che "*qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato*".

La nomina del Responsabile deve, quindi, essere effettuata dal Titolare per iscritto mediante contratto od altro atto giuridico vincolante, finalizzato a regolare il rapporto in essere, con specifiche istruzioni e relative responsabilità. Per tali ragioni, data la sua figura centrale nel trattamento dei dati per conto del Titolare, il Responsabile deve quindi essere individuato tra i soggetti – persone fisiche o giuridiche – che per esperienza, capacità ed affidabilità forniscano idonee garanzie del pieno rispetto delle disposizioni del GDPR.

Compiti e Responsabilità

- il Responsabile deve trattare i dati personali secondo le istruzioni impartite dal Titolare. Qualora non dovesse rispettare le istruzioni, determinando autonomamente le finalità e i mezzi del trattamento, viene considerato esso stesso Titolare del trattamento in questione;
- garantire che le persone autorizzate o designate al trattamento si impegnino alla riservatezza;
- deve inoltre adottare misure tecniche ed organizzative adeguate, come richieste dal Titolare;
- deve assistere il Titolare del trattamento in tutte le attività per cui è stato nominato, rendendosi disponibile anche per eventuali audit di verifica effettuati dal Titolare stesso;
- su scelta del Titolare, al termine del trattamento deve cancellare o restituire i dati personali ad esso comunicati;
- deve dimostrare al Titolare di aver rispettato gli obblighi e le istruzioni ad esso impartite;
- deve tenere un registro del trattamento nel quale illustra i trattamenti effettuati per conto del Titolare;
- deve avvertire tempestivamente il Titolare in caso di data breach;
- deve cooperare con l'Autorità di Vigilanza;
- non può ricorrere ad un altro responsabile (sub-responsabile) in assenza di previa autorizzazione scritta specifica o generale del Titolare.

La Governance ed il Sistema di Gestione Privacy: focus governance

Il referente privacy è una figura, seppur non espressamente contemplata dal GDPR, di supporto designata dal Titolare, per fini organizzativi, come punto chiave per la gestione operativa delle operazioni di trattamento caratterizzate da una rischiosità intrinseca dovuta alla tipologia dei dati trattati (gestione del personale, risorse informatiche, etc.).

Il Referente o "designato", introdotto dall' art. 2 quaterdecies del D.Lgs 101/2018, è una figura eventuale che non deve essere prevista obbligatoriamente dalle aziende. Per la funzione che svolge (supporto organizzativo-gestionale al Titolare) è logico pensare che con maggior probabilità esso sia previsto all'interno delle società complesse, piuttosto che all'interno di quelle semplici.

Sulla scorta del principio di responsabilizzazione del Titolare (cd. *accountability*) il referente privacy costituisce a tutti gli effetti il soggetto delegato di riferimento dell'impresa per le tematiche connesse al trattamento di dati personali.

Nel caso in cui un'azienda preveda al suo interno questa figura, questi sono i suoi compiti.

Compiti e Responsabilità

- cura l'attuazione delle misure di protezione per i dati personali;
- fornisce indicazioni/istruzioni operative agli autorizzati al Trattamento sulle modalità di trattamento e presidio dei dati personali e ne coordina le attività;
- cura le revisioni periodiche della mappatura dei trattamenti dati personali riferite alla propria area di competenza;
- gestisce, anche mediante propri collaboratori, i rapporti con i soggetti esterni in materia di privacy;
- si rivolge al DPO per avere chiarimenti in caso di eventuali nuove operazioni di trattamento, nonché in caso di dubbi sui trattamenti esistenti;
- riporta al titolare eventuali irregolarità riscontrate nell'ambito di trattamenti di dati personali;
- gestisce il flusso informativo in materia privacy all'interno della società.

La Governance ed il Sistema di Gestione Privacy: focus governance

Il DPO è il soggetto cui competono le responsabilità di indirizzare, sensibilizzare e sorvegliare il rispetto della normativa sul trattamento di dati personali.

Gli artt. 37, 38, 39 del GDPR introducono tale figura che deve essere nominata in tutti i casi in cui l'azienda Titolare svolge trattamenti che prevedano il controllo regolare e sistematico degli interessati, ovvero la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Ai sensi del GDPR, è possibile designare un DPO anche in casi diversi da quelli sopra indicati ovvero per un gruppo di imprese purché abbia risorse necessarie per coprire il proprio ruolo e riesca a garantire effettività al suo ruolo e disponibilità e copertura per tutte le società che sono tenute alla nomina.

Compiti e Responsabilità

- svolge un ruolo centrale, interagendo con i vari soggetti per l'emanazione di politiche e linee guida a livello societario;
- sorveglia l'attuazione e l'applicazione delle politiche privacy all'interno delle società;
- indirizza l'applicazione in azienda di quanto richiesto dalla normativa con particolare riguardo ai requisiti concernenti la protezione dei dati (progettazione, informazione all'interessato);
- informa le società e i dipendenti che eseguono trattamenti in merito agli obblighi derivanti dal GDPR e dalla normativa in materia di protezione dei dati;
- cura la formazione e l'informazione al personale;
- funge da punto di contatto per il Garante Privacy nel caso di richieste di informazioni/verifiche ispettive/procedimenti autorizzativi e sanzionatori;
- funge da punto di contatto per gli Interessati per l'esercizio dei loro diritti o per fornire informazioni;
- verifica l'attuazione e l'applicazione del Regolamento;
- fornisce, se richiesto dal Titolare, pareri in merito alla valutazione d'impatto e/o alla Data Breach.

La Governance ed il Sistema di Gestione Privacy: focus governance

L'autorizzato ed il designato sono le persone fisiche che effettuano materialmente le operazioni di trattamento sui dati personali su istruzioni del Titolare del trattamento. Il D.lgs. 101/2018, all'art. *2-quaterdecies*, riporta testualmente che "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità.*" Ai fini del rispetto del principio dell'*accountability* e di efficienza del sistema di gestione privacy, il Titolare può prevedere la nomina di specifici soggetti a designati del trattamento in virtù delle specifiche mansioni a loro assegnate che prevedono il coordinamento e la gestione di numerose figure interne e di conseguenza precisazioni maggiori, in relazione agli obblighi connessi alla protezione dei dati personali, tendenzialmente identificati nelle figure dei responsabili di funzione. Autorizzati invece dovranno essere tutti i dipendenti che trattano dati, raccogliendo la loro firma per presa visione.

Compiti e Responsabilità

- deve rispettare ed adempiere agli obblighi introdotti dal rispettivo atto di nomina predisposto dal titolare del trattamento;
- deve trattare i dati personali nel rispetto delle istruzioni impartite dal Titolare e dal Referente interno;
- deve rispettare le adeguate misure di sicurezza predisposte dal Titolare;
- deve informare il titolare e il Referente Interno di qualsiasi incidente di sicurezza fisica o informatica che possa aver coinvolto – anche solo potenzialmente – i dati personali cui ha accesso o di cui comunque venga a conoscenza;
- non deve operare alcuna comunicazione e/o diffusione dei dati personali ai quali ha accesso salvo preventiva autorizzazione del Titolare;
- non deve avere alcuna autonomia decisionale nel trattamento dei dati.

La Governance ed il Sistema di Gestione Privacy: focus governance

Il Provvedimento del 23 novembre 2008 del Garante per la Protezione dei Dati Personali ha introdotto per la prima volta nel nostro impianto normativo gli Amministratori di Sistema ("ADS"), definendoli come le "*figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi".*

Il GDPR non prevede una disciplina *ad hoc* per l'ADS, richiamandolo tuttavia implicitamente dalla lettura dell'art. 32 GDPR in quanto l'adozione di misure di sicurezza adeguate richiede necessariamente la partecipazione di personale specializzato e competente. Di conseguenza si assumono tuttora valide le prescrizioni del Garante presenti nel citato Provvedimento.

Compiti e Responsabilità

- deve adottare nel rispetto delle istruzioni del Titolare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici che devono garantire caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, la pseudonimizzazione e la cifratura dei dati personali, la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico nonché una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

- sorveglia l'attuazione e l'applicazione misure di sicurezza tecnologiche introdotte dal titolare;
- le registrazioni dei dati di log degli amministratori devono essere conservate per un congruo periodo di tempo non inferiore ai sei mesi;
- l´operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un´attività di verifica da parte del Titolare del trattamento o del responsabile.

La Governance ed il Sistema di Gestione Privacy: focus governance

Le caratteristiche principali della delega di funzione per i designati/referenti privacy

Dimensioni della società	▪ Secondo alcune pronunce la delega di funzioni è da ritenersi ammissibile solo allorquando le dimensioni dell'impresa sono tali da rendere impossibile il controllo dell' attività in capo ad una sola persona
Data Certa e Forma Scritta	▪ Da un punto di vista formale è senz'altro necessario che la delega di funzioni in materia abbia data certa e forma scritta
Idoneità del soggetto delegato	▪ E' necessaria l'idoneità del soggetto delegato quali requisiti indispensabili per il corretto esercizio dei poteri delegati: in difetto, la responsabilità per la scelta di persona tecnicamente non capace e non dotata delle necessarie cognizioni tecniche ricadrebbe comunque in capo al delegante
Autonomia ed effettivi poteri	▪ Il delegato dev'essere dotato di autonomia gestionale e capacità di spesa nella materia delegata in modo da poter esercitare in maniera effettiva la responsabilità assunta.
Accettazione	▪ Il delegato deve accettare espressamente per iscritto la delega conferita in quanto deve essere consapevole delle responsabilità amministrative e penali che gli vengono conferite
Divieto di ingerenza	▪ E' vietata al delegante ogni intromissione sia tecnica che decisionale nella sfera di operatività attribuita al delegato; in caso contrario la condotta posta in essere dovrebbe essere imputata direttamente al primo

La Governance ed il Sistema di Gestione Privacy: focus governance : principali elementi

COSA FARE?

1. Predisporre o Revisionare il Funzionigramma Privacy implementato prevedendo "persone designate" interne;
2. Prevedere specifici atti di designazione per le "persone designate" ove siano dettagliati compiti e responsabilità relativi al trattamento dei dati personali in modo chiaro e preciso;
3. Prevedere specifiche deleghe di funzione in materia di Privacy;
4. Prevedere gli specifici compiti privacy nelle Job descriptions o nei mansionari.

La Governance ed il Sistema di Gestione Privacy: monitoraggio e controlli

Monitoraggio › Audit

Un elemento fondamentale del Regolamento 679/2016 ("GDPR") è rappresentato dagli obblighi di continuo **monitoraggio** e **verifica** della effettiva implementazione del proprio Sistema di Gestione della Privacy posti a carico di Titolari del Trattamento e, ove nominato, anche a carico del Data Protection Officer dell'azienda o del Gruppo, quali ad esempio:

GDPR - Art. 32 (Misure di sicurezza

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, che comprendono: […] d) una **procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento.

GDPR - Art. 24 (Accountability)

Tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il **titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare**, che il trattamento dei dati personali è effettuato conformemente al Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

GDPR - Art. 39 (DPO)

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: b) **sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali,** compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati **considera debitamente i rischi inerenti al trattamento**, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

La Governance ed il Sistema di Gestione Privacy: monitoraggio e controlli

Il Sistema adottato deve avere una propria solidità non solamente formale ma effettiva, ovvero deve dimostrare di essere concretamente e continuamente in grado di fornire una **compliance day by day** su ogni tematica privacy che inerisce la conduzione giornaliera dell'attività dell'impresa.

In questo contesto si inserisce la necessità di **eseguire attività di verifica di compliance in ambito Privacy** per:

- ✓ verificare l'adeguata strutturazione formale del Sistema di Gestione Privacy (Privacy by Design e Privacy by Default)
- ✓ verificare la effettiva implementazione sostanziale del proprio sistema di Sistema di Gestione Privacy
- ✓ valutare lo stato di compliance operativa (day by day compliance) effettiva raggiunto;
- ✓ valutare la compliance con le decisioni specifiche del Garante e con eventuali ;
- ✓ identificare, gestire e mitigare i rischi di non conformità sanzionabili sul piano amministrativo e/o penale;
- ✓ identificare potenziali non conformità formale o sostanziale;
- ✓ rendere effettivo e tracciabile il monitoraggio periodico eseguito (principio di accountability).

La Governance ed il Sistema di Gestione Privacy: monitoraggio e controlli

Ambiti di verifica

Principi
Liceità e correttezza: rispetto delle norme generali e specifiche dell'ordinamento in materia di data protection
Trasparenza: assicurare la consapevolezza dell'interessato; modalità operative di accessibilità dei dati da parte degli interessati
Integrità e riservatezza: assicurare misure tecniche ed organizzative adeguate al fine di proteggere i dati personali da trattamenti non autorizzati
Limitazione alla conservazione: i dati devono essere conservati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità
Minimizzazione dei dati: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto ale finalità del trattamento

- Protezione dei dati fin dalla progettazione
- Mappatura dei dati e dei trattamenti effettuati per processo aziendale
- Ridurre al minimo l'utilizzo dei dati personali mediante misure tecniche ed organizzative

- Tutela della protezione del dato per impostazione predefinita
- Misure tecniche ed organizzative adeguate per garantire che siano trattati per impostazione predefinita solo i dati personali necessari per ogni specifica finalità
- Predisposizione di procedure e policy per disciplinare l'accessibilità dei dati e i tempi di conservazione..

- Responsabilizzazione e rendicontazione dei titolari e dei responsibili per quell che attiene al rispetto delle norme del Regolamento e, in generale, della normativa in materia di data protection.

Principali aree di rischio				
	Management & Governance	Processo HR	Marketing & CRM	Salute e sicurezza luoghi di lavoro
	Processo Legale & compliance	Internal audit	Produzione qualità vendite	Amministrazione e contabilità

La Governance ed il Sistema di Gestione Privacy: monitoraggio e controlli

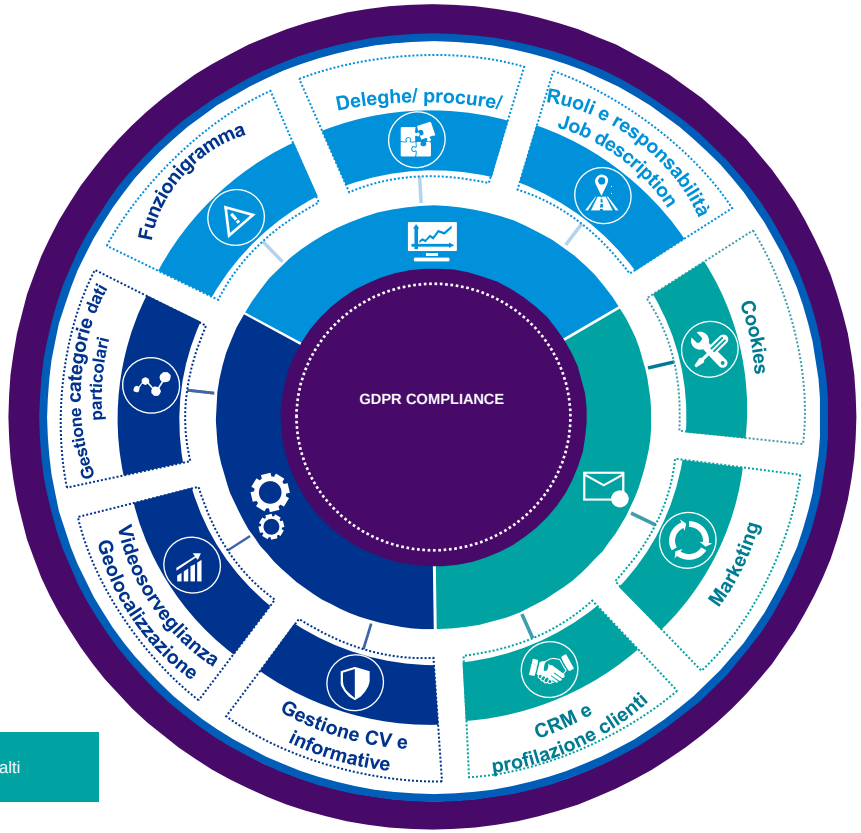
I processi a rischio Privacy

Il framework di controlli che verrà utilizzato consente di identificare i vari componenti e le parti interessate di un Sistema di Gestione Privacy completo.

I controlli applicati integrati garantiscono una identificazione dei rischi tempestiva ed efficace, la valutazione, la mitigazione e, in alcuni casi, l'accettazione degli stessi purché coerentemente motivati secondo i corretti principi di accountability.

Questo framework offre i seguenti vantaggi:

- Progettazione, sviluppo e aggiornamento continuo del Sistema di Gestione Privacy implementato;
- Dimostrazione concreta di efficacia del principio di autoresponsabilizzazione in ordine all'implementazione di misure tecniche ed organizzative adeguate non solo per garantire ma anche per essere in grado di dimostrare che il trattamento è effettuato in maniera conforme al Regolamento UE ed al Codice della privacy, per come recentemente modificato dal D.Lgs. n. 101/2018
- Dimostrazione concreta da parte del titolare dell'adeguatezza delle misure tecniche ed organizzative in base alla natura, all'ambito, al contesto, alle finalità ed alle probabilità dei rischi



Esempi di processi a rischio

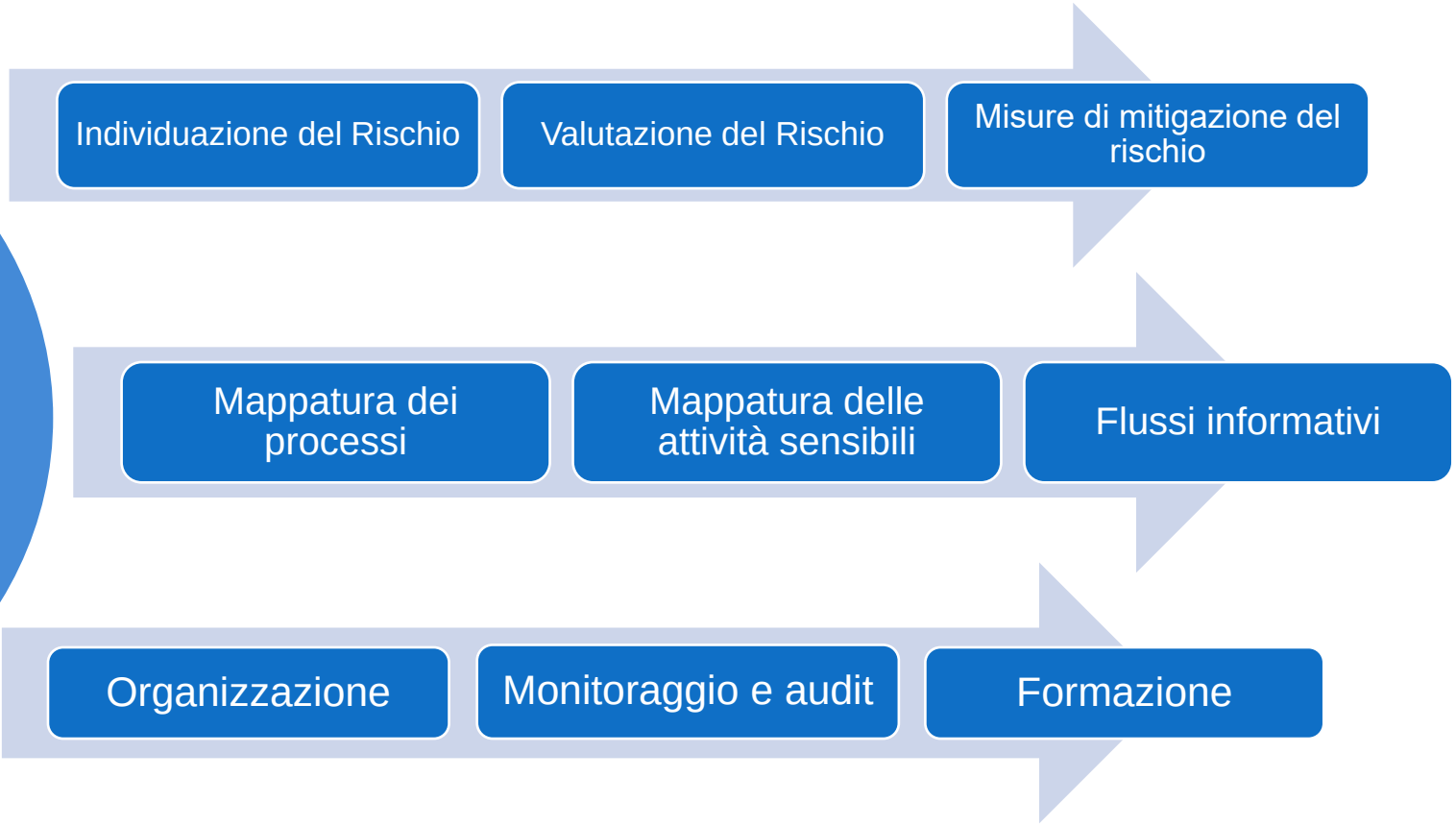
Gestione CV e informative	Videosorveglianza	Categorie particolari	
CRM	Profilazione	Marketing	Appalti

La Governance ed il Sistema di Gestione Privacy: sistema di gestione integrato

La *compliance* richiesta alle aziende dai contesti normativi in cui operano si sta dimostrando sempre più stringente e articolata, rendendo complesse e onerose le attività per la gestione dei rischi di conformità.
Solo a titolo di esempio, recentemente il Nuovo Codice della crisi di Impresa e dell'Insolvenza **(D.Lgs 14/2019** ha fatto rientrare i **modelli 231** tra le disposizioni societarie dirette a garantire l'adeguatezza di governo come strumento di rilevazione preventiva dell'emersione dello stato di crisi, il **D.lgs. 97/2016 modificando l'art. 1 comma 2 bis l. 190/2012 "Legge Anticorruzione"** ha introdotto per le società controllate o partecipate **oneri anticorruzione in forma semplificata.**
L'impegno del imprese oggi si focalizza, da un lato nel costruire e mantenere un sistema di controllo efficiente in grado di garantire la conformità alle leggi, regolamenti e standard, in modo integrato con i processi operativi e la gestione dei rischi; dall'altro nel coniugare queste esigenze con gli obiettivi, ancora più pressanti, di performance.

La Governance ed il Sistema di Gestione Privacy: sistema di gestione integrato

Sinergie Metodologiche



La Governance ed il Sistema di Gestione Privacy: SCI e Privacy

Impatto e correlazioni tra il SCI e il "Privacy Compliance"	
Sintesi dei principali elementi del SCI	**Sintesi dei principali elementi del Privacy Compliance**
Obiettivo: ➢ Conformità dei comportamenti aziendali alla legge.	L'obiettivo del Privacy Compliance è garantire il rispetto e la conformità al Regolamento Europeo.
Ambiente di controllo: elementi socio/organizzativi/culturale ➢ Valori etici, stile manageriale, politiche di gestione delle risorse umane.	Il Privacy Compliance presuppone una cultura diversa rispetto alla precedente normativa e prevede il coinvolgimento di tutti i processi e responsabili di funzione. La "Persona" deve essere al centro delle valutazioni in ogni progettualità sin dall'origine (Privacy by design).
Valutazione dei rischi ➢ Valutazione dei rischi (nella sua globalità) che impediscono il raggiungimento degli obbiettivi: analisi dei fattori e stima dell'impatto.	Il Privacy Compliance prevede un approccio basato sul rischio: ➢ Valutazione d'impatto; ➢ Data Protection Impact Assessment.
Attività di controllo ➢ Azioni e misure per la mitigazione del rischio ➢ Esempio di controlli: verifiche di compliance normativa (privacy; riciclaggio, 231, antitrust, codice autodisciplina, ecc..).	Il Privacy Compliance prevede adeguate misure per la protezione dei dati: ➢ Misure organizzative e procedurali; ➢ Misure informatiche; ➢ Misure legali/giuridiche .
Sistema informativo ➢ Flussi informativi sulle componenti del sistema di controllo e tra i livelli della struttura organizzativa.	Il Privacy Compliance prevede: ➢ Flussi informativi tra il DPO e il Titolare, il Responsabile al trattamento, i dipendeti, i terzi, l'Autorità garante; ➢ Segnalazioni di violazione del sistema e del Trattamento 8Data Breach).
Monitoraggio ➢ Supervisione sul sistema di controllo per la verifica dell'efficacia dello stesso: adeguatezza, aggiornamento e miglioramenti.	I Privacy Compliance prevede: ➢ Autorità garante che sorveglia ed assicura l'applicazione del regolamento; ➢ DPO verifica che la normativa e le policy privacy siano attuate.

La Governance ed il Sistema di Gestione Privacy: 231 e privacy

Nello specifico, alcuni dei comportamenti che costituiscono una minaccia alla **sicurezza informatica**, sono stati qualificati all'interno del nostro ordinamento come condotte penalmente perseguibili ed inseriti tra i "reati presupposto" della responsabilità degli enti di cui al D.Lgs. n. 231/2001:

Delitti informatici e trattamento illecito dei dati (Art. 24-bis del D.Lgs. 231/2001)

Art. 24-*bis* del D.Lgs. 231/2001, introdotto dalla Legge 18 marzo 2008, n. 48:

- Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.)
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)
- Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)
- Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)

La Governance ed il Sistema di Gestione Privacy: 231 e privacy

Delitti in materia di privacy: prima inseriti nel D.Lgs. 231/2001, poi estromessi

Nell'agosto 2013* il legislatore aveva inserito nel novero dei reati presupposto ex D.Lgs. 231/2001 i seguenti ***delitti privacy*:**

- trattamento illecito dei dati personali;
- falsità nelle dichiarazioni notificazioni al Garante;
- inosservanza dei provvedimenti del Garante.

LA PENA PREVISTA

In assenza/insufficienza dei Modelli organizzativi previsti dalla normativa 231, se i vertici dell'impresa avessero commesso uno dei delitti previsti in materia di privacy, la Società sarebbe stata soggetta ad una sanzione **da 100 a 500 quote** (una quota singola può variare da un minimo di 258 fino a un massimo di 1.549 euro).

RETRO-FRONT

Il Decreto Legge n. 93/2013 è stato convertito in legge, ma con l'esclusione dei reati relativi alla privacy.
L'estromissione dei reati privacy dal D.Lgs. 231/2001 potrebbe far pensare ad una scarsa attenzione che le Istituzioni danno alla tutela e riservatezza dei dati personali.
Tuttavia ciò è smentito dalla tendenza europea, che ha visto la recente pubblicazione del nuovo **Regolamento Europeo in materia di Protezione dei Dati**.

* **Decreto Legge 14/8/2013 n. 93**, intitolato "*Norme urgenti in materia di sicurezza e per il contrasto della violenza di genere*" in vigore dal **17 agosto 2013** e da convertire in legge entro 3 mesi, aveva modificato ed aggiornato l'articolo ***24 bis comma 1*** del Decreto legislativo 231 del 2001 (*Delitti informatici e trattamento illecito di dati – in vigore dall'aprile 2008*)

Michele Luigi Giordano
Partner

Governance, Compliance & Organisation
Studio Associato KPMG – Consulenza legale e tributaria

E: michelegiordano@kpmg.it

Mob. +39 3486561052

Sistema di Gestione Privacy

Il Sistema di Gestione Privacy

Il Sistema di Gestione della Protezione dei dati personali costituisce un efficace strumento per la messa in sicurezza dei dati personali, per la loro valorizzazione e per la tutela dell'intero del patrimonio informativo aziendale.

Un Sistema di Gestione è un insieme di elementi correlati di un'organizzazione finalizzato a stabilire politiche e processi per conseguire obiettivi.

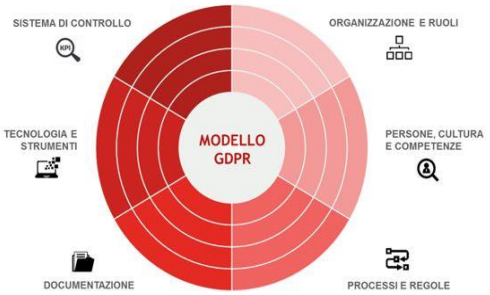
E' uno strumento di carattere organizzativo e gestionale utilizzato per rispettare, in modo dimostrabile da parte del Titolare o del Responsabile del Trattamento («Accountability»), i criteri ed i requisiti della previsti dalla norma di riferimento.

Il Sistema di Gestione Privacy

Formazione

+

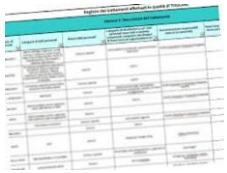
Monitoraggio



1 Assessment

2 Gap Analysis

3 Registro attività di Trattamento

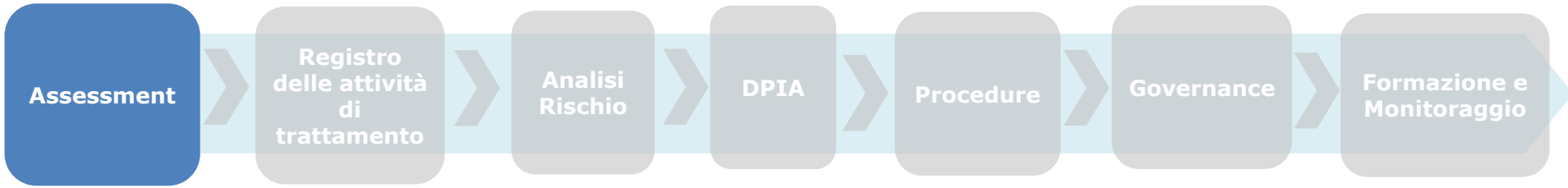


4 Risk Analysis e DPIA

5 Procedure e Informative Privacy

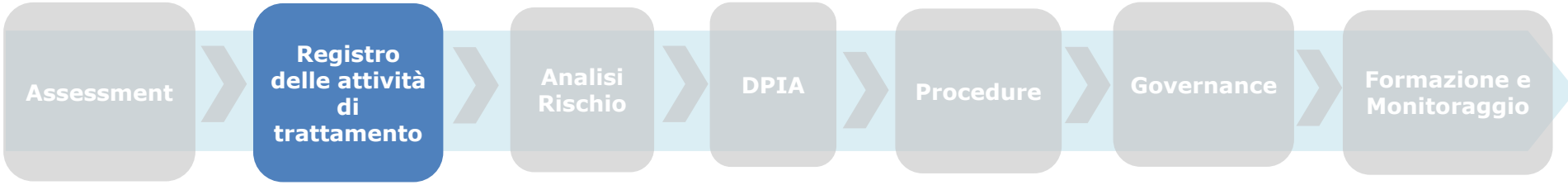
6 Governance Privacy e Nomine

Il Sistema di Gestione Privacy



1. **Rilevazione dello stato della Società in materia di compliance alla Privacy**
2. **Rilevazione dei «*gap*» rispetto alla Normativa Privacy (Gdpr, Codice della Privacy, D. Lgs. 101/08, Codici deontologici, Provvedimenti del Garante della Protezione dei Dati personali, Linee Guida anche dell'EDPB, *best practice*)**
3. **Definizione di una «*Road Map*» di azioni correttive e di miglioramento in riferimento ai «*gap*» di compliance rilevati**

Il Sistema di Gestione Privacy



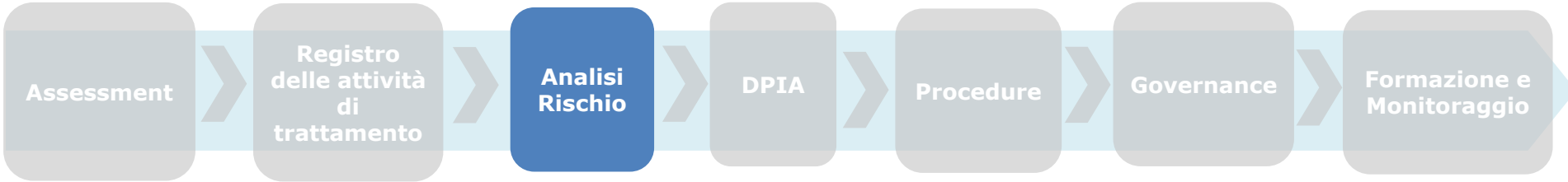
L'obbligo di redigere il Registro delle attività di trattamento (art. 30 del GDPR) è uno dei principali elementi di «*Accountability*» del Titolare poiché rappresenta uno strumento necessario a fornire un quadro aggiornato dei trattamenti effettuati dalla Società.

È suggeribile redigere un Registro delle attività di trattamento per ciascun processo aziendale che possa costituire una mappatura completa di tutti i trattamenti per ogni specifica funzione aziendale.

Il Registro deve avere forma scritta, anche elettronica e deve essere esibito su richiesta del Garante, e contenere, fra le altre informazioni obbligatorie:

- **Finalità del trattamento**
- **Categorie di dati personali trattati**
- **Modalità di trattamento**
- **Responsabili ex art. 28**
- **Categorie di destinatari**
- **Categorie di interessati**
- **Trasferimenti dei dati extra Ue**
- **Data retention**
- **Misure di sicurezza tecniche e organizzative**

Il Sistema di Gestione Privacy



Il Considerando 75 del GDPR con riferimento al concetto di rischio stabilisce che : *"I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale […]".*

Con tale valutazione si determina la misura di responsabilità del titolare o del responsabile del trattamento, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli interessati.

Il Sistema di Gestione Privacy

«Per "rischio" si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità» per i diritti e le libertà degli interessati»

(Linee guida del Gruppo di lavoro Articolo 29 WP248rev.1)

Il Sistema di Gestione Privacy

Analisi del Rischio: il Rischio inerente

I Rischi inerenti al trattamento dei dati rispetto alla sicurezza dei dati stessi (C83):

- Distruzione accidentale o illegale dei dati
- Perdita dei dati, modifica, rilevazione
- Accesso non autorizzato
- Trattamento non conforme o non consentito

Potenziale danno fisico materiale o immateriale

Da effettuarsi su tutti i trattamenti, sia ex ante sia ex post (valutazione dell'efficacia delle misure attuate per ridurre i rischi rilevati)

Il Titolare dovrà operare le proprie scelte sulla base di un processo di valutazione del rischio oggettivo

Il Sistema di Gestione Privacy

Analisi del Rischio: Rischio inerente

ESEMPI DI INDICI DI VALUTAZIONE DELLA PROBABILITÀ

- Profilazione sistematica e globale: Il trattamento dei dati su salute, preferenze personali, interessi, affidabilità, comportamento, ubicazione e spostamenti della persona fisica è svolto in maniera automatizzata?
- Criticità precedenti: Si sono verificate nel passato irregolarità/violazioni nel trattamento dei dati?
- Specificità rispetto al business: Il trattamento oggetto di valutazione è specifico in relazione al settore di appartenenza della Società? (esempio: farmaceutico/bancario/marketing)
- Nuove tecnologie: Per il trattamento vengono utilizzate nuove tecnologie per esempio Cloud?
- Trattamento di dati su larga scala: sono trattati relativi ad un elevato numero di soggetti o comprendenti enormi quantità di dati stessi?
- Categoria di dato: Il trattamento comprende dati particolari o giudiziari oppure dati comuni?
- Trasferimenti di dati all'estero: E' previsto il trasferimento di dati fuori UE?
- Controllo sistematico dei dati: E' effettuato un monitoraggio dei soggetti interessati?

EINDICI DI VALUTAZIONE DELL'IMPATTO

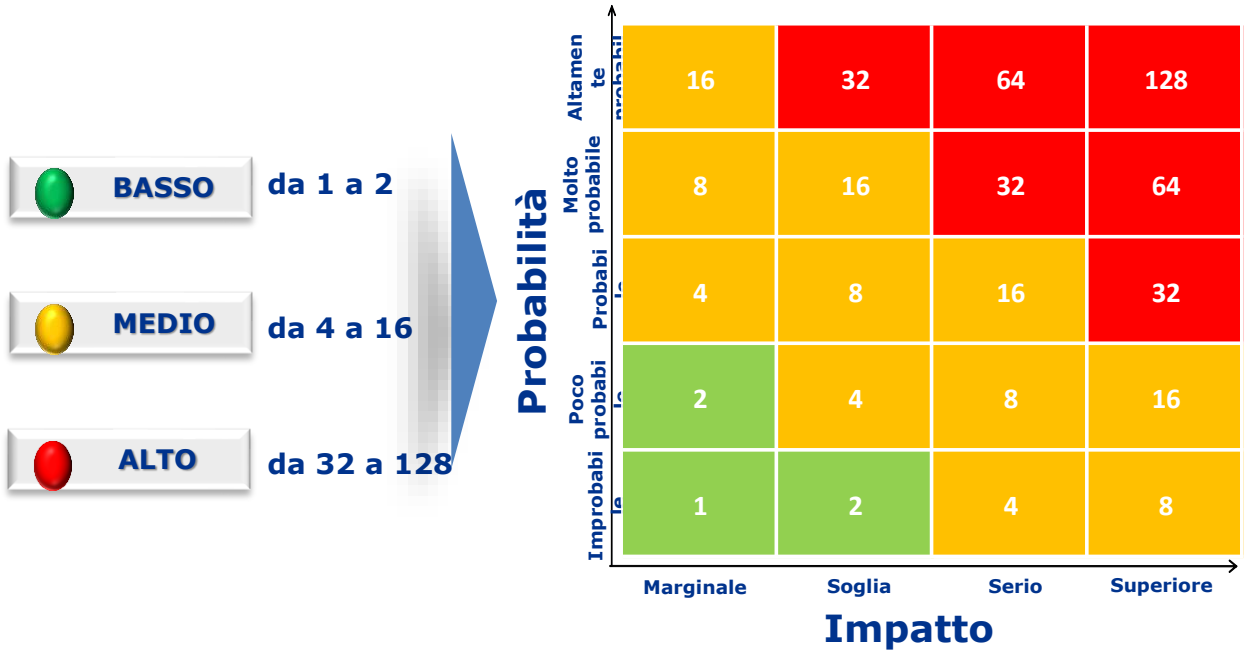
- Impatto sanzionatorio: Qual è l'entità massima delle sanzioni pecuniarie e penali previste dal D.Lgs. 196/2003 e dal Regolamento UE applicabili?
- Provvedimenti del Garante: Esistono provvedimenti del Garante in merito al trattamento in oggetto?
- Impatto reputazionale: Qual è l'impatto all'immagine aziendale derivante della diffusione di eventuali notizie di commissione del reato privacy?

VALORI DELL'IMPATTO
1 marginale 2 soglia
4 serio 8 superiore

VALORI DELLA PROBABILITÀ
1 improbabile 2 poco probabile 4 probabile
8 molto probabile 16 altamente probabile

Il Sistema di Gestione Privacy

La matrice dei rischi



Il Sistema di Gestione Privacy

SISTEMA DI CONTROLLO INTERNO PRIVACY

Il sistema di controllo interno è un altro driver su cui si basa la valutazione del rischio privacy ed è calcolato prendendo in considerazione le attività poste in essere dalle aziende per rendersi conformi alla normativa di riferimento

Indici di valutazione del sistema di controllo interno

- **Consenso ed informative appropriate al trattamento;**
- **Presenza di nomine adeguate e specifiche;**
- **Presenza di procedure e istruzioni operative specifiche per la protezione dei dati personali;**
- **Misure di sicurezza adeguate;**
- **Formazione su tematiche specifiche;**

Il Sistema di Gestione Privacy

Analisi del Rischio: Rischio Residuo

Il **rischio privacy inerente (RI)** connesso ad un determinato trattamento indica il livello di rischio associato al trattamento stesso a prescindere dall'azione del sistema di controllo interno posto in essere.

Il **sistema di controllo interno privacy** è costituito dall'insieme della documentazione, delle procedure e delle misure tecniche e organizzative volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi.

Il valore del **rischio privacy residuo (RR)** è ottenuto riducendo il valore iniziale del rischio inerente in misura proporzionale alla forza del sistema di controllo che caratterizza l'attività in questione.

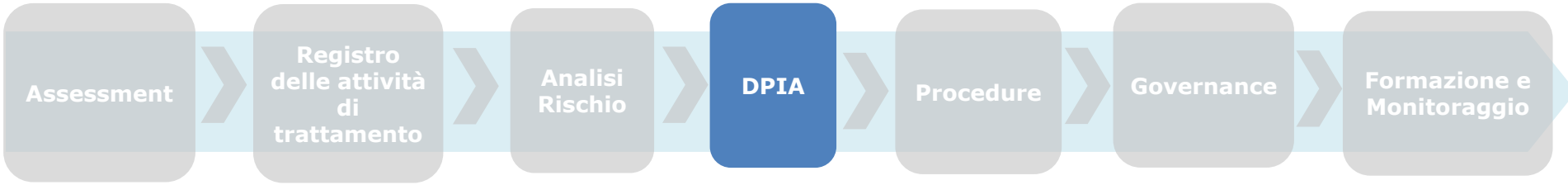
Valutazione Rischio Privacy Residuo

=

Valutazione Rischio Privacy Inerente **–** Adeguatezza Sistema di Controllo Interno Privacy

- ALTO
- MEDIO
- BASSO

Il Sistema di Gestione Privacy



L'art. 35 e l'EDBP offrono dei criteri in base ai quali si individuano i casi in cui sia necessaria una Valutazione d'Impatto del trattamento.

A norma dell'art. 35, comma 7, la valutazione contiene almeno:

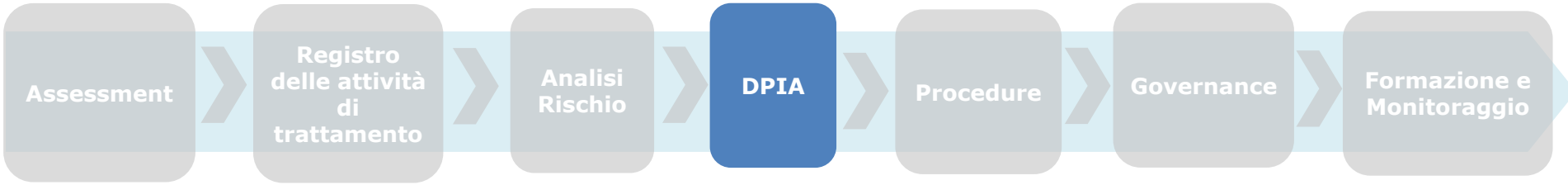
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il Sistema di Gestione Privacy

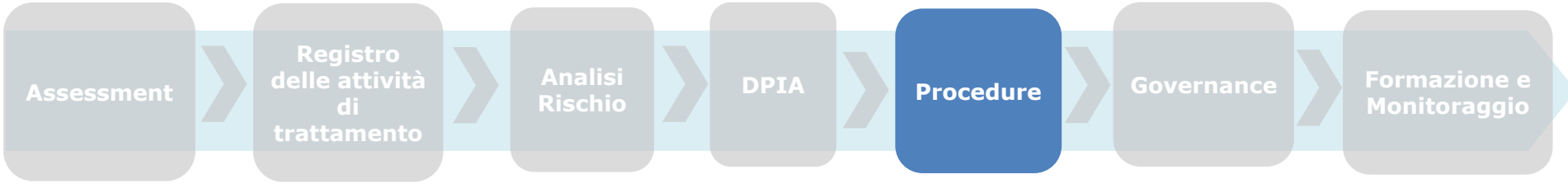


L'Autorità Garante Italiana, col Provvedimento 11 ottobre 2018, ha previsto un elenco di trattamenti per i quali è obbligatorio svolgere una Valutazione d'Impatto. Questo elenco è vincolante ma non è esaustivo, poiché resta fermo l'obbligo di adottare una DPIA laddove ricorrano due o più dei criteri individuati dalle Linee Guida.

Il CNIL (autorità di controllo francese) ha messo a disposizione un software open source per la valutazione di impatto sia nella versione *standalone* (da scaricare sul computer) che in quella online.

Anche il Garante italiano segnala questo software come tool per realizzare la valutazione.

Il Sistema di Gestione Privacy



Al fine di una corretta *compliance* al Regolamento europeo in materia di Protezione dei Dati è importante dare rilevanza all'interno della propria organizzazione alla redazione di specifiche procedure in conformità al principio della Privacy by default. Le principali procedure da implementare sono:

- **Procedura Data Breach**
- **Procedura Data Retention**
- **Procedura gestione istanze interessati**
- **Procedura flussi al DPO;**
- **Procedura visite ispettive;**
- **Procedura utilizzo dispositivi mobili – Regolamento informatico**

Il Sistema di Gestione Privacy

Assessment → Registro delle attività di trattamento → Analisi Rischio → DPIA → Procedure → **Governance** → Formazione e Monitoraggio

E' necessario per un corretto Sistema d Gestione Privacy la predisposizione di una Governance Privacy.

Esempio di Governance in società complessa

Titolare del Trattamento

DPO/manager Privacy

Responsabili ex Art. 28

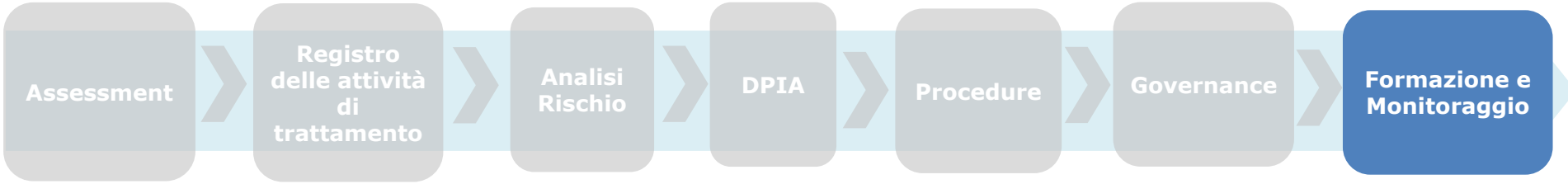
Designati del trattamento

- Dott.ssa XXXX – MKTG
- Dott. XXXX – OPERATION
- Dott.ssa XXXX – HR
- Dott.ssa XXXX – CRM
- Responsabile IT – Amministratori di Sistema

Autorizzati al trattamento dei dati

Tutti i dipendenti

Il Sistema di Gestione Privacy



Formazione

- Il GDPR prevede l'obbligo della formazione in materia di protezione dei dati personali per tutte le figure presenti nell'organizzazione (sia dipendenti che collaboratori).
- L'art. 29 del Regolamento dispone, infatti, che "[...] il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali non può trattare tali dati se non è istruito in tal senso dal titolare".
- Il WP 29, nel proprio parere n. 3/2010 ha individuato, tra le misure comuni concernenti la responsabilità "un'adeguata formazione ed istruzione del personale in materia di protezione dei dati. Il personale in questione dovrebbe includere gli incaricati (o responsabili) del trattamento dei dati personali, ma anche dirigenti e sviluppatori in campo informatico e direttori di unità commerciali".
- La centralità della formazione è confermata, poi, anche dall'art. 32 del GDPR "Sicurezza del trattamento" paragrafo 4 ove si prevede espressamente che "il titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso ai dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".

Il Sistema di Gestione Privacy

Assessment › Registro delle attività di trattamento › Analisi Rischio › DPIA › Procedure › Governance › **Formazione e Monitoraggio**

Monitoraggio

GDPR - Art. 32 (Misure di sicurezza)

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, che comprendono: […] d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

GDPR - Art. 39 (DPO)

Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

Le sanzioni amministrative e penali derivanti dal mancato rispetto della normativa in materia di protezione dei dati

Il Nuovo Quadro Sanzionatorio

Il nuovo e pervasivo quadro sanzionatorio in riferimento a non conformità con il nuovo framework legislativo in materia di Data Protection si struttura su 3 aree di illeciti, come di seguito evidenziato:

Condotte illecite di minore gravità	Sanzione amministrativa pecuniaria fino a 10 milioni di euro o, se superiore, fino al 2% del fatturato mondiale totale annuo	6 Condotte tipiche
Condotte illecite di particolare gravità	Sanzione amministrativa pecuniaria fino a 20 di milioni di euro o, se superiore, fino al 4% del fatturato mondiale totale annuo	26 Condotte tipiche
Illeciti Penali	Reclusione da 1 a 6 anni	4 Fattispecie di reato

Le sanzioni amministrative pecuniarie

Condotte di minor gravità

Sanzione

Sanzione amministrativa pecuniaria fino a **10 milioni di euro** o, per le imprese, fino al **2% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore.

CONDOTTE

1. Violazione degli obblighi imposti al titolare (e, se nominato, al responsabile) del trattamento in relazione al consenso dei minori per i servizi della società dell'informazione
2. Violazione delle misure a garanzia introdotte dal Garante con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che può presentare rischi particolarmente elevati
3. Violazione delle modalità di redazione e conservazione di cartelle cliniche Violazione delle disposizioni sulla redazione del certificato di assistenza al parto Violazione, da parte del titolare, degli obblighi di informativa all'utente sulla natura dei dati di traffico telefonico e telematico e sulla durata del trattamento
4. Violazione, da parte del fornitore del servizio di comunicazione elettronica, degli obblighi relativi al trasferimento automatico della chiamata
5. Violazione del provvedimento del Garante di individuazione delle modalità di manifestazione del consenso all'inclusione negli elenchi telefonici cartacei e elettronici e all'utilizzo dei relativi dati per marketing
6. Violazione degli obblighi relativi alla sicurezza del trattamento

Le sanzioni amministrative pecuniarie

Sanzione

CONDOTTE

Condotte illecite di particolare gravità (1/3)

Sanzione amministrativa pecuniaria fino a **20 milioni di euro** o, per le imprese, fino al **4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore

1. Violazione delle disposizioni relative alla comunicazione e diffusione di dati personali da parte di titolari che effettuato il trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri
2. Violazione, da parte del titolare del trattamento, delle disposizioni sul consenso dei minori in relazione ai servizi della società dell'informazione
3. Violazione delle norme sul trattamento di particolari categorie di dati personali per rilevanti motivi di interesse pubblico rilevante
4. Diffusione in dati genetici, biometrici e relativi alla salute
5. Violazione delle norme sul trattamento dei dati relativi a condanne penali
6. Violazione delle disposizioni relative all'esercizio dei diritti delle persone decedute da parte di chi ve ne abbia interesse
7. Indicazione dei dati identificativi degli interessati in provvedimenti giurisdizionali in violazione della disciplina che consente all'interessato di precludere tale indicazione nella riproduzione dei provvedimenti
8. Violazione della disciplina sul trattamento dei dati sanitari
9. Violazione delle disposizioni sull'informativa da fornire all'interessato nell'ambito dei trattamenti sanitari, anche d'emergenza

Le sanzioni amministrative pecuniarie

CONDOTTE

Condotte illecite di particolare gravità (2/3)

10. Violazione delle disposizioni sulla presa visione e il rilascio di cartella clinica a soggetto diverso dall'interessato
11. Rilascio a terzi di certificato di assistenza al parto Violazione delle disposizioni sulla comunicazione e diffusione di dati relativi a studenti Violazione delle disposizioni sulla durata del trattamento in caso di trattamento a fini di archiviazione nel pubblico interesse o di ricerca scientifica
12. Diffusione di dati per fini di studio da parte di università ed enti di ricerca Modalità di trattamento di dati per scopi storici, per scopi statistici e scientifici
13. Violazione delle disposizioni che attengono al trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici
14. Violazione delle regole deontologiche nei trattamenti in materia di lavoro e previdenza Violazione della disciplina sull'informativa all'interessato nel primo contatto dopo la ricezione del curriculum
15. Violazione delle disposizioni sul trattamento dei dati da parte degli istituti di patronato
16. Comunicazione di dati all'istituto di vigilanza sulle assicurazioni a fini di contrasto delle frodi assicurative
17. Violazione delle disposizioni sul trattamento di informazioni nell'apparecchio terminale del contraente o utente di servizi di comunicazione elettronica

Le sanzioni amministrative pecuniarie

Condotte illecite di particolare gravità (3/3)

CONDOTTE

18. Mancata cancellazione di dati relativi al traffico telefonico telematico, conservazione degli stessi a finii di fatturazione oltre i sei mesi, mancato consenso al trattamento dei dati a fini di commercializzazione di servizi e trattamento da parte di soggetti diversi dal delegato
19. Violazione, da parte del fornitore del servizio di comunicazione elettronica, degli obblighi relativi alla fatturazione dettagliata dei dati di traffico
20. Violazione dell'obbligo, a richiesta, di impedire l'identificazione della linea
21. Violazione delle disposizioni sui dati relativi all'ubicazione diversi dai dati del traffico Violazione delle disposizioni sulle comunicazioni indesiderate
22. Violazione delle disposizioni su informazioni a contraenti e utenti Violazione delle disposizioni sulla conservazione dei dati di traffico telefonico e telematico
23. Violazione degli obblighi per i fornitori dei servizi di comunicazione elettronica di fornire al Garante le informazioni sulle procedure interne
24. Violazione delle disposizioni sulle informazioni del fornitore ad abbonati e utenti sui rischi di violazioni della sicurezza
25. Violazione delle regole deontologiche
26. Violazione delle misure di garanzia e delle misure tecniche introdotte dal Garante in relazione ai dati

Le sanzioni penali

Articolo	Condotte illecite	
Art. 167 Trattamento illecito dei dati	E' punito, salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, arreca nocumento all'interessato in violazione di specifiche disposizioni di legge (come quelle che regolamentano il trattamento di dati ex art. 9 e il trasferimento internazionale dei dati personali). L'aggiunta del "danno" consente di ricomprendere tra le fattispecie punibili anche condotte quali il "revenge porn". E' altresì punito chi, al fine di trarre per sè o per altri profitto o di arrecare danno all'interessato procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti, arreca nocumento all'interessato.	Reclusione da 1 a 3 anni
Art. 167-bis Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala	Comunicazione o diffusione - al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno - di un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies [del Codice di materia di protezione dei dati personali] o senza consenso, ove richiesto.	Reclusione da 1 a 6 anni
Art.167-ter Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala	Acquisizione con mezzi fraudolenti, al fine di trarne profitto ovvero al fine di arrecare danno, di un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala.	Reclusione da 1 a 4 anni

Le sanzioni penali

Articolo	Condotte illecite	
Art. 168 Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante	Dichiarazioni o attestazioni false, in un procedimento o nel corso di un procedimento dinanzi al Garante, di notizie o circostanze o produzione di atti o documenti falsi.	Reclusione da 6 mesi 3 anni
	Intenzionale interruzione o turbamento di un procedimento davanti al Garante o degli accertamenti da questo disposti.	Reclusione fino a 1 anno
Art. 170 Inosservanza di provvedimenti del Garante	Inosservanza dei provvedimenti del Garante	Reclusione da 3 mesi a 2 anni
Art. 171 Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori	Art. 38 della Legge n. 300 del 1970 (cd. "Statuto dei lavoratori")	Pena di cui all'art. 38 della Legge n. 300 del 1970

Avv. Paola Casaccino
Senior Manager, Governance, Compliance & Organisation
Studio Associato (KPMG)
E: pcasaccino@kpmg.it
T: +39 055 261961
M: +39 348 4420380

Alessandro Legnante

Senior Legal Specialist

Governance, Compliance & Organisation
Studio Associato KPMG
E: alegnante@kpmg.it

Mob. +39 3455989855

kpmg.com/it/socialmedia

kpmg.com/app