REGOLAMENTO UE SULLA PROTEZIONE DEI DATI PERSONALI

GLI IMPATTI PER LE AZIENDE

INDICE DEI TEMI – I PARTE

PROGRAMMA

- **III GIORNATA INFORMATIVA**
- L'ADEGUAMENTO AL REGOLAMENTO (UE) N. 679/2016 E LE NOVITÀ DEL D.LGS. 101/2018
- COSA FARE PER ADEGUARSI
- **15 NOVEMBRE 2018, ORE 9.00**
- SALA CONVEGNI, CONFINDUSTRIA SALERNO

- **INTERVENTI**

- **ORE 9.45 AVV. RICCARDO IMPERIALI DI FRANCAVILLA - PARTNER GRUPPO IMPERIALI**
- L'ADEGUAMENTO AL REGOLAMENTO (UE) 679/2016 E LE NOVITÀ DEL D.LGS. 101/2018

- **ORE 11.45 DR.SSA ANNA IRACE - RESPONSABILE *COMPLIANCE* GRUPPO IMPERIALI**
- IL RAPPORTO TRA IL TITOLARE E LE TERZE PARTI
- L'IMPORTANZA DELL'ADEGUATEZZA DELLE MISURE TECNICHE ORGANIZZATIVE E DI SICUREZZA
- L'OPPORTUNITÀ DI INTEGRAZIONE DEL MODELLO GDPR CON GLI ALTRI MODELLI ORGANIZZATIVI (TUTELA DEL *KNOW- HOW* E MO 231)

AGGIORNAMENTI NORMATIVI

D.LGS. 101/2018

- IL 19 SETTEMBRE ENTRA IN VIGORE IL D.LGS. 101/2018 DI ARMONIZZAZIONE DEL CODICE PRIVACY CON I PRINCIPI DEL REGOLAMENTO UE 2016/679
- IL LEGISLATORE INTERVIENE COL BISTURI E PER OGNI ARTICOLO DEL CODICE CHE VA MODIFICATO NE STABILISCE LA RISCRITTURA O L'INTEGRAZIONE, CONTEMPORANEAMENTE ALL'ABROGAZIONE DI AMPIE PARTI, IN QUANTO GIÀ AFFRONTATE DAL GDPR.

COSA SUCCEDE CON LE AUTORIZZAZIONI GENERALI DEL GARANTE?

AUTORIZZAZIONI GENERALI

IL GARANTE, CON PROPRIO PROVVEDIMENTO DA ADOTTARE ENTRO 90 GIORNI DALLA VIGENZA DEL DECRETO, INDIVIDUA LE PRESCRIZIONI CONTENUTE NELLE AUTORIZZAZIONI GENERALI GIÀ ADOTTATE, RIGUARDO AI DATI PARTICOLARI E GIUDIZIARI, NONCHÉ SULLE MATERIE RIMESSE ALLA COMPETENZA REGOLATORIA DEGLI STATI MEMBRI, CHE RISULTANO COMPATIBILI CON IL GDPR E, QUINDI, CONTINUANO AD AVERE VALIDITÀ.

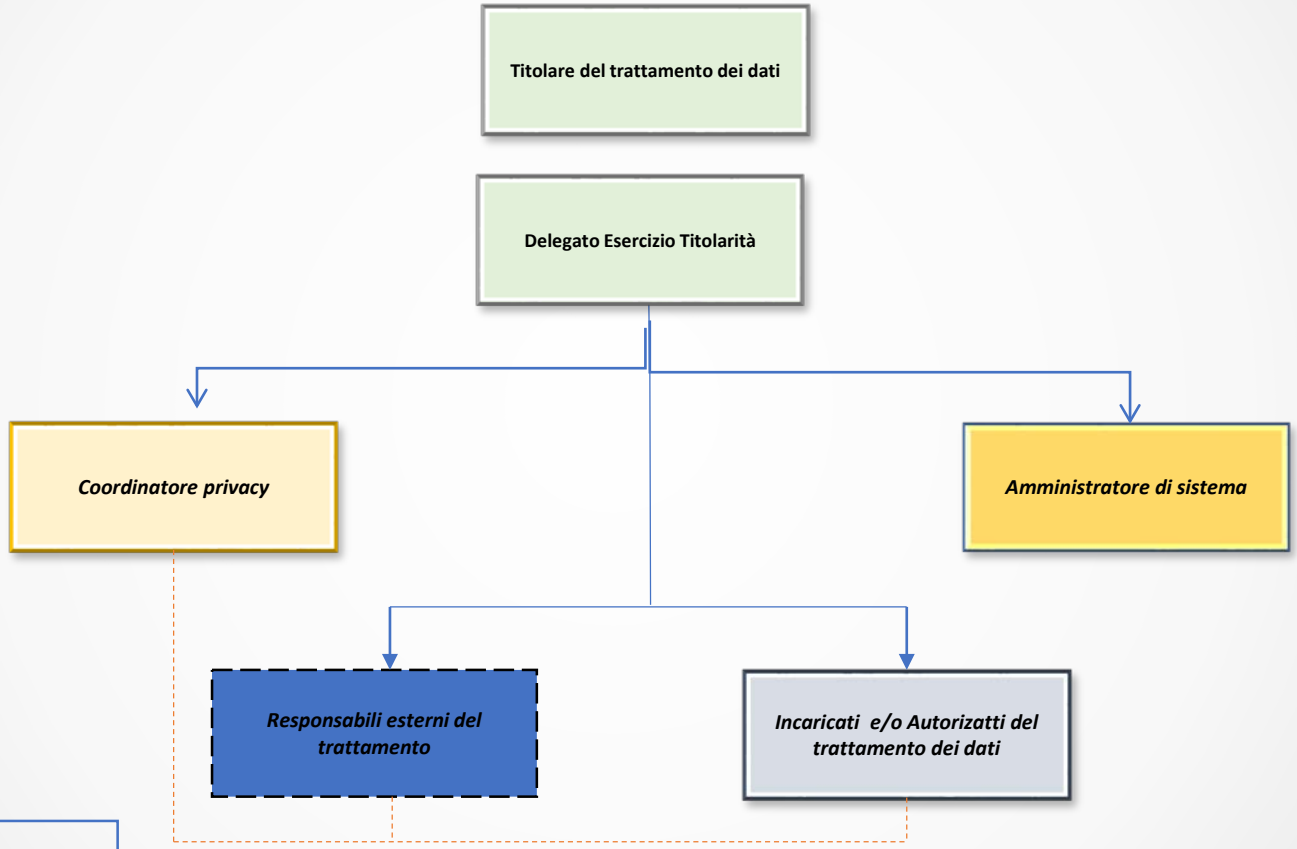
AUTONOMIA DEL TITOLARE

ASSETTO ORGANIZZATIVO

TITOLARE E RESPONSABILI SONO LIBERI DI ATTRIBUIRE SPECIFICI COMPITI E FUNZIONI CONNESSI AL TRATTAMENTO DI DATI PERSONALI NELL'AMBITO DEL PROPRIO ASSETTO ORGANIZZATIVO. CIOÈ SPETTA ALL'AZIENDA DEFINIRE IL MODELLO ORGANIZZATIVO DATA PROTECTION RITENUTO PIÙ ADEGUATO

PROPOSTA DI MODELLO ORGANIZZATIVO

DATA PROTECTION



AGGIORNAMENTI NORMATIVI

TRATTAMENTO DI DATI PARTICOLARI PER MOTIVI DI INTERESSE PUBBLICO RILEVANTE

I REGOLAMENTI DELLA PA PER L'USO DI DATI SENSIBILI RIMANGONO VALIDI.

L'USO DI DATI PARTICOLARI O GIUDIZIARI È AMMESSO QUANDO È NECESSARIO PER MOTIVI DI INTERESSE PUBBLICO RILEVANTE, A CONDIZIONE CHE SIA PREVISTO DALLA LEGGE O, NEI CASI PREVISTI DALLA LEGGE, DI REGOLAMENTO CHE SPECIFICHINO I TIPI DI DATI CHE POSSONO ESSERE TRATTATI, LE OPERAZIONI ESEGUIBILI E IL MOTIVO DI INTERESSE PUBBLICO RILEVANTE

LE FAQ DEL GARANTE SUL REGISTRO TRATTAMENTI

L'art. 30 del **Regolamento (EU) n. 679/2016** (di seguito "RGPD") prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del **registro delle attività di trattamento**.

E' un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del RGPD) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento (sul registro del responsabile, vedi, in particolare, il **punto 6**).

Costituisce uno dei principali elementi di accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante

CHI È TENUTO A REDIGERLO?

Tutti **i titolari** e i **responsabili** del trattamento sono tenuti a redigere il Registro delle attività di trattamento (v. art. 30, par. 1 e 2 del RGPD).

In particolare, in ambito privato, i soggetti obbligati sono così individuabili:

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

CHI È TENUTO A REDIGERLO?

RIENTRANO NELLA CATEGORIA DELLE "ORGANIZZAZIONI" DI CUI ALL'ART. 30, PAR. 5 ANCHE LE ASSOCIAZIONI, FONDAZIONI E I COMITATI.

ALLA LUCE DI QUANTO DETTO SOPRA, SONO TENUTI ALL'OBBLIGO DI REDAZIONE DEL REGISTRO, AD ESEMPIO:

- **ESERCIZI COMMERCIALI, ESERCIZI PUBBLICI O ARTIGIANI** CON ALMENO UN DIPENDENTE (BAR, RISTORANTI, OFFICINE, NEGOZI, PICCOLA DISTRIBUZIONE, ECC.) E/O CHE TRATTINO DATI SANITARI DEI CLIENTI (ES. PARRUCCHIERI, ESTETISTI, OTTICI, ODONTOTECNICI, TATUATORI ECC.);

- **LIBERI PROFESSIONISTI** CON ALMENO UN DIPENDENTE E/O CHE TRATTINO DATI SANITARI E/O DATI RELATIVI A CONDANNE PENALI O REATI (ES. COMMERCIALISTI, NOTAI, AVVOCATI, OSTEOPATI, FISIOTERAPISTI, FARMACISTI, MEDICI IN GENERALE);

- ASSOCIAZIONI, FONDAZIONI E COMITATI OVE TRATTINO "CATEGORIE PARTICOLARI DI DATI" E/O DATI RELATIVI A CONDANNE PENALI O REATI (I.E. ORGANIZZAZIONI DI TENDENZA; ASSOCIAZIONI A TUTELA DI SOGGETTI C.D. "VULNERABILI" QUALI AD ESEMPIO MALATI, PERSONE CON DISABILITÀ, EX DETENUTI ECC.; ASSOCIAZIONI CHE PERSEGUONO FINALITÀ DI PREVENZIONE E CONTRASTO DELLE DISCRIMINAZIONI DI GENERE, RAZZIALI, BASATE SULL'ORIENTAMENTO SESSUALE, POLITICO O RELIGIOSO ECC.; ASSOCIAZIONI SPORTIVE CON RIFERIMENTO AI DATI SANITARI TRATTATI; PARTITI E MOVIMENTI POLITICI; SINDACATI; ASSOCIAZIONI E MOVIMENTI A CARATTERE RELIGIOSO);

- **IL CONDOMINIO** OVE TRATTI "CATEGORIE PARTICOLARI DI DATI" (ES. DELIBERE PER INTERVENTI VOLTI AL SUPERAMENTO E ALL'ABBATTIMENTO DELLE BARRIERE ARCHITETTONICHE AI SENSI DELLA L. N. 13/1989; RICHIESTE DI RISARCIMENTO DANNI COMPRENSIVE DI SPESE MEDICHE RELATIVI A SINISTRI AVVENUTI ALL'INTERNO DEI LOCALI CONDOMINIALI).

Misure semplificative

Infine, si precisa che le **imprese e organizzazioni con meno di 250 dipendenti** obbligate alla tenuta del registro potranno comunque beneficiare di **alcune misure di semplificazione**, potendo circoscrivere l'obbligo di redazione del registro alle sole specifiche attività di trattamento sopra individuate (es. ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti un solo lavoratore dipendente, il registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento).

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

Si invita altresì a consultare il documento interpretativo del 19 aprile 2018 del Gruppo ex art. 29 (Ora Comitato europeo per la protezione dei dati) reperibile al seguente link: **http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045**

QUALI SONO LE MODALITÀ DI CONSERVAZIONE E DI AGGIORNAMENTO?

IL REGISTRO DEI TRATTAMENTI È UN DOCUMENTO DI CENSIMENTO E ANALISI DEI TRATTAMENTI EFFETTUATI DAL TITOLARE O RESPONSABILE. IN QUANTO TALE, IL REGISTRO DEVE ESSERE MANTENUTO COSTANTEMENTE AGGIORNATO POICHÉ IL SUO CONTENUTO DEVE SEMPRE CORRISPONDERE ALL'EFFETTIVITÀ DEI TRATTAMENTI POSTI IN ESSERE. QUALSIASI CAMBIAMENTO, IN PARTICOLARE IN ORDINE ALLE MODALITÀ, FINALITÀ, CATEGORIE DI DATI, CATEGORIE DI INTERESSATI, DEVE ESSERE IMMEDIATAMENTE INSERITO NEL REGISTRO, DANDO CONTO DELLE MODIFICHE SOPRAVVENUTE.

IL REGISTRO PUÒ ESSERE COMPILATO SIA IN FORMATO CARTACEO CHE ELETTRONICO MA DEVE IN OGNI CASO RECARE, IN MANIERA VERIFICABILE, LA DATA DELLA SUA PRIMA ISTITUZIONE (O LA DATA DELLA PRIMA CREAZIONE DI OGNI SINGOLA SCHEDA PER TIPOLOGIA DI TRATTAMENTO) UNITAMENTE A QUELLA DELL'ULTIMO AGGIORNAMENTO. IN QUEST'ULTIMO CASO IL REGISTRO DOVRÀ RECARE UNA ANNOTAZIONE DEL TIPO:

"- SCHEDA CREATA IN DATA XY"

"- ULTIMO AGGIORNAMENTO AVVENUTO IN DATA XY"

I DATI CHE DEVE CONTENERE

TITOLARE E RESPONSABILE DEVONO MANTENERE UN REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO, DISPONIBILE SU RICHIESTA DEL GARANTE (ART. 30)



- Dati Identificativi
- Finalità Trattamento
- Flussi transfrontalieri
- Categorie soggetti interessati e dati
- Categorie di destinatari
- Tempi di conservazione
- Descrizione misure di sicurezza tecnico-organizzative

PUNTI DI ATTENZIONE

NEL CAMPO "**DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA**" ANDRANNO INDICATE LE MISURE TECNICO-ORGANIZZATIVE ADOTTATE DAL TITOLARE AI SENSI DELL'ART. 32 DEL RGDP TENENDO PRESENTE CHE L'ELENCO IVI RIPORTATO COSTITUISCE UNA LISTA APERTA E NON ESAUSTIVA, ESSENDO RIMESSA AL TITOLARE LA VALUTAZIONE FINALE RELATIVA AL LIVELLO DI SICUREZZA ADEGUATO, CASO PER CASO, AI RISCHI PRESENTATI DALLE ATTIVITÀ DI TRATTAMENTO CONCRETAMENTE POSTE IN ESSERE.

TALE LISTA HA DI PER SÉ **UN CARATTERE DINAMICO** (E NON PIÙ STATICO COME È STATO PER L'ALLEGATO B DEL D. LGS. 196/2003) DOVENDOSI CONTINUAMENTE CONFRONTARE CON GLI SVILUPPI DELLA TECNOLOGIA E L'INSORGERE DI NUOVI RISCHI. LE MISURE DI SICUREZZA POSSONO ESSERE DESCRITTE IN FORMA RIASSUNTIVA E SINTETICA, O COMUNQUE IDONEA A DARE UN QUADRO GENERALE E COMPLESSIVO DI TALI MISURE IN RELAZIONE ALLE ATTIVITÀ DI TRATTAMENTO SVOLTE, CON POSSIBILITÀ DI FARE RINVIO PER UNA VALUTAZIONE PIÙ DETTAGLIATA A DOCUMENTI ESTERNI DI CARATTERE GENERALE (ES. PROCEDURE ORGANIZZATIVE INTERNE; SECURITY POLICY ECC.).

PUNTI DI ATTENZIONE

NEL CAMPO "**TERMINI ULTIMI PREVISTI PER LA CANCELLAZIONE DELLE DIVERSE CATEGORIE DI DATI**" DOVRANNO ESSERE INDIVIDUATI I TEMPI DI CANCELLAZIONE PER TIPOLOGIA E FINALITÀ DI TRATTAMENTO (AD ES. "IN CASO DI RAPPORTO CONTRATTUALE, I DATI SARANNO CONSERVATI PER 10 ANNI DALL'ULTIMA REGISTRAZIONE – V. ART. 2220 DEL CODICE CIVILE"). AD OGNI MODO, OVE NON SIA POSSIBILE STABILIRE A PRIORI UN TERMINE MASSIMO, I TEMPI DI CONSERVAZIONE POTRANNO ESSERE SPECIFICATI MEDIANTE IL RIFERIMENTO A CRITERI (ES. NORME DI LEGGE, PRASSI SETTORIALI) INDICATIVI DEGLI STESSI (ES. "IN CASO DI CONTENZIOSO, I DATI SARANNO CANCELLATI AL TERMINE DELLO STESSO")

REGISTRO DEL RESPONSABILE DEL TRATTAMENTO

IL RESPONSABILE DEL TRATTAMENTO TIENE UN REGISTRO DI "TUTTE LE CATEGORIE DI ATTIVITÀ RELATIVE AL TRATTAMENTO SVOLTE PER CONTO DI UN TITOLARE" (ART. 30, PAR. 2 DEL RGPD).

IN MERITO ALLE MODALITÀ DI COMPILAZIONE DELLO STESSO SI RAPPRESENTA QUANTO SEGUE:

A) NEL CASO IN CUI UNO STESSO SOGGETTO AGISCA IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO PER CONTO DI PIÙ CLIENTI QUALI AUTONOMI E DISTINTI TITOLARI (ES. SOCIETÀ DI SOFTWARE HOUSE), LE INFORMAZIONI DI CUI ALL'ART. 30, PAR. 2 DEL RGPD DOVRANNO ESSERE RIPORTATE NEL REGISTRO CON RIFERIMENTO A CIASCUNO DEI SUDDETTI TITOLARI. IN QUESTI CASI IL RESPONSABILE DOVRÀ SUDDIVIDERE IL REGISTRO IN TANTE SEZIONI QUANTI SONO I TITOLARI PER CONTO DEI QUALI AGISCE; OVE, A CAUSA DELL'INGENTE NUMERO DI TITOLARI PER CUI SI OPERI, L'ATTIVITÀ DI PUNTUALE INDICAZIONE E DI CONTINUO AGGIORNAMENTO DEI NOMINATIVI DEGLI STESSI NONCHÉ DI CORRELAZIONE DELLE CATEGORIE DI TRATTAMENTI SVOLTI PER OGNUNO DI ESSI RISULTI ECCESSIVAMENTE DIFFICOLTOSA, IL REGISTRO DEL RESPONSABILE POTREBBE RIPORTARE IL RINVIO, AD ES., A SCHEDE O BANCHE DATI ANAGRAFICHE DEI CLIENTI (TITOLARI DEL TRATTAMENTO), CONTENENTI LA DESCRIZIONE DEI SERVIZI FORNITI AGLI STESSI, FERMA RESTANDO LA NECESSITÀ CHE COMUNQUE TALI SCHEDE RIPORTINO TUTTE LE INDICAZIONI RICHIESTE DALL'ART. 30, PAR. 2 DEL RGPD.

REGISTRO DEL RESPONSABILE DEL TRATTAMENTO

B) CON RIFERIMENTO ALLA "DESCRIZIONE DELLE CATEGORIE DI TRATTAMENTI EFFETTUATI" (ART. 30, PAR. 2, LETT. B) DEL RGPD) È POSSIBILE FAR RIFERIMENTO A QUANTO CONTENUTO NEL CONTRATTO DI DESIGNAZIONE A RESPONSABILE CHE, AI SENSI DELL'ART. 28 DEL RGPD, DEVE INDIVIDUARE, IN PARTICOLARE, LA NATURA E LA FINALITÀ DEL TRATTAMENTO, IL TIPO DI DATI PERSONALI E LE CATEGORIE DI INTERESSATI OGGETTO DEL TRATTAMENTO, NONCHÉ LA DURATA DI QUEST'ULTIMO;

C) IN CASO DI SUB-RESPONSABILE, PARIMENTI, IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO SVOLTE DA QUEST'ULTIMO POTRÀ SPECIFICATAMENTE FAR RIFERIMENTO AI CONTENUTI DEL CONTRATTO STIPULATO TRA LO STESSO E IL RESPONSABILE AI SENSI DELL'ART. 28, PARAGRAFI 2 E 4 DEL RGPD.

APPROCCIO BASATO SUL RISCHIO E MISURE DI ACCOUNTABILITY (RESPONSABILIZZAZIONE) DI TITOLARI E RESPONSABILI

IL REGOLAMENTO PONE CON FORZA L´ACCENTO SULLA "RESPONSABILIZZAZIONE" (ACCOUNTABILITY NELL´ACCEZIONE INGLESE) DI TITOLARI E RESPONSABILI – OSSIA, SULL´**ADOZIONE DI COMPORTAMENTI PROATTIVI E TALI DA DIMOSTRARE LA CONCRETA ADOZIONE DI MISURE FINALIZZATE AD ASSICURARE L´APPLICAZIONE DEL REGOLAMENTO** *(SI VEDANO ARTT. 23-25, IN PARTICOLARE, E L´INTERO CAPO IV DEL REGOLAMENTO)*. SI TRATTA DI UNA GRANDE NOVITÀ PER LA PROTEZIONE DEI DATI IN QUANTO VIENE AFFIDATO AI TITOLARI IL COMPITO DI DECIDERE AUTONOMAMENTE LE MODALITÀ, LE GARANZIE E I LIMITI DEL TRATTAMENTO DEI DATI PERSONALI – NEL RISPETTO DELLE DISPOSIZIONI NORMATIVE E ALLA LUCE DI ALCUNI CRITERI SPECIFICI INDICATI NEL REGOLAMENTO.

DATA PROTECTION BY DEFAULT AND BY DESIGN"

IL PRIMO FRA TALI CRITERI È SINTETIZZATO DALL´ESPRESSIONE INGLESE **"DATA PROTECTION BY DEFAULT AND BY DESIGN"** *(SI VEDA ART. 25)*, OSSIA DALLA NECESSITÀ DI CONFIGURARE IL TRATTAMENTO PREVEDENDO FIN DALL´INIZIO LE GARANZIE INDISPENSABILI "AL FINE DI SODDISFARE I REQUISITI" DEL REGOLAMENTO E TUTELARE I DIRITTI DEGLI INTERESSATI – TENENDO CONTO DEL CONTESTO COMPLESSIVO OVE IL TRATTAMENTO SI COLLOCA E DEI **RISCHI** PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI. TUTTO QUESTO DEVE AVVENIRE A MONTE, PRIMA DI PROCEDERE AL TRATTAMENTO DEI DATI VERO E PROPRIO ("SIA AL MOMENTO DI DETERMINARE I MEZZI DEL TRATTAMENTO SIA ALL´ATTO DEL TRATTAMENTO STESSO", SECONDO QUANTO AFFERMA L´ART. 25(1) DEL REGOLAMENTO) E RICHIEDE, PERTANTO, UN´ANALISI PREVENTIVA E UN IMPEGNO APPLICATIVO DA PARTE DEI TITOLARI CHE **DEVONO SOSTANZIARSI IN UNA SERIE DI ATTIVITÀ SPECIFICHE E DIMOSTRABILI.**

IL CONCETTO DI «RESPONSABILIZZAZIONE» O «ACCOUNTABILITY»

LE RESPONSABILITÀ DEL TITOLARE DEL TRATTAMENTO (ART. 24)

1. TENUTO CONTO DELLA NATURA, DELL'AMBITO DI APPLICAZIONE, DEL CONTESTO E DELLE FINALITÀ DEL TRATTAMENTO, NONCHÉ DEI RISCHI AVENTI PROBABILITÀ E GRAVITÀ DIVERSE 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 È EFFETTUATO CONFORMEMENTE AL PRESENTE REGOLAMENTO. DETTE MISURE SONO **RIESAMINATE E AGGIORNATE** QUALORA NECESSARIO.

2. SE CIÒ È PROPORZIONATO RISPETTO ALLE ATTIVITÀ DI TRATTAMENTO, LE MISURE DI CUI AL PARAGRAFO 1 INCLUDONO **L'ATTUAZIONE DI POLITICHE ADEGUATE** IN MATERIA DI PROTEZIONE DEI DATI DA PARTE DEL TITOLARE DEL TRATTAMENTO.

3. L'ADESIONE AI CODICI DI CONDOTTA DI CUI ALL'ARTICOLO 40 O A UN MECCANISMO DI CERTIFICAZIONE DI CUI ALL'ARTICOLO 42 PUÒ ESSERE UTILIZZATA COME ELEMENTO PER DIMOSTRARE IL RISPETTO DEGLI OBBLIGHI DEL TITOLARE DEL TRATTAMENTO.

CONTITOLARI E RESPONSABILI

IL REGOLAMENTO:

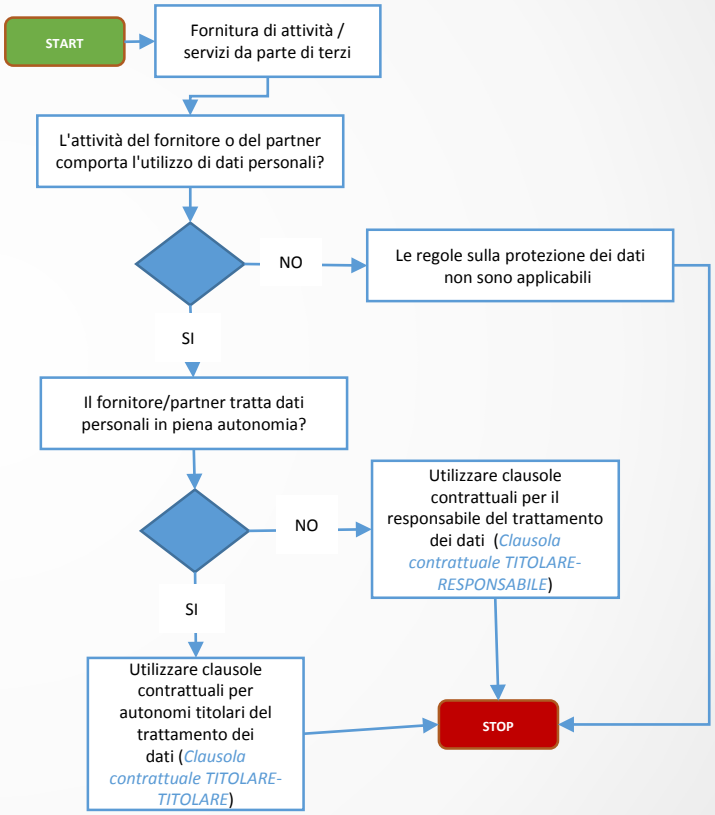
- DISCIPLINA LA **CONTITOLARITÀ DEL TRATTAMENTO** *(ART. 26)* E IMPONE AI TITOLARI DI DEFINIRE SPECIFICAMENTE (CON UN ATTO GIURIDICAMENTE VALIDO AI SENSI DEL DIRITTO NAZIONALE) IL RISPETTIVO AMBITO DI RESPONSABILITÀ E I COMPITI **CON PARTICOLARE RIGUARDO ALL´ESERCIZIO DEI DIRITTI DEGLI INTERESSATI**, CHE HANNO COMUNQUE LA POSSIBILITÀ DI RIVOLGERSI INDIFFERENTEMENTE A UNO QUALSIASI DEI TITOLARI OPERANTI CONGIUNTAMENTE;
- PREVEDE **OBBLIGHI SPECIFICI IN CAPO AI RESPONSABILI DEL TRATTAMENTO**, IN QUANTO DISTINTI DA QUELLI PERTINENTI AI RISPETTIVI TITOLARI. CIÒ RIGUARDA, IN PARTICOLARE, LA TENUTA DEL **REGISTRO DEI TRATTAMENTI** SVOLTI *(EX ART. 30, PARAGRAFO 2)*; L´ADOZIONE DI IDONEE **MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA** DEI TRATTAMENTI *(EX ART. 32 REGOLAMENTO)*; LA **DESIGNAZIONE DI UN RPD-DPO** (SI SEGNALANO, AL RIGUARDO, LE LINEE-GUIDA IN MATERIA DI RESPONSABILI DELLA PROTEZIONE DEI DATI ADOTTATE DAL GRUPPO "ARTICOLO 29", DISPONIBILI QUI ANCHE NELLA VERSIONE IN ITALIANO: WWW.GARANTEPRIVACY.IT/REGOLAMENTOUE/RPD), NEI CASI PREVISTI DAL REGOLAMENTO O DAL DIRITTO NAZIONALE *(SI VEDA ART. 37 DEL REGOLAMENTO)*.

GESTIONE TERZE PARTI

AL FINE DI INDIVIDUARE SE IL RAPPORTO CON LA TERZA PARTE DEBBA PREVEDERE L'ADOZIONE DI CLAUSOLE CONTRATTUALI DATA PROTECTION AD HOC, L'AZIENDA DEVE PRIMA DI TUTTO DOMANDARSI:

1. SE IL CONTRATTO COMPORTA TRASFERIMENTI DI DATI PERSONALI VERSO LA TERZA PARTE.

2. POI, QUALE SIA IL MODO IN CUI LA TERZA PARTE TRATTA I DATI PERSONALI (AUTONOMAMENTE O SU ISTRUZIONI DELL'AZIENDA).



Nell'ambito di servizi che comportano il trasferimento di dati personali ai fornitori

La Società è TITOLARE del trattamento

Valuta l'autonomia del fornitore nel trattamento dei dati trasferiti ai fini della definizione del suo ruolo e sottoscrive con questi uno dei seguenti accordi:

A

Contratto Titolare/Titolare

Il fornitore tratta i dati in modo autonomo.

- Assume il ruolo di **Titolare** del trattamento ex art. 4 c. 7 del GDPR;
- Ha **autonomia** in:

a) verifica conformità del trattamento
b) predisposizione misure tecniche e organizzative
c) responsabilità verso i soggetti interessati

- **Notifica** eventuali violazioni nel trattamento dallo stesso effettuato.

B

Contratto Titolare/Responsabile

Il fornitore tratta i dati in modo non autonomo.

- Assume il ruolo di **Responsabile** del trattamento ex art. 4 c. 8 del GDPR;
- Rispetta le **istruzioni scritte** ricevute dal Titolare;
- Garantisce **competenza** nell'adozione di misure tecniche e organizzative;
- Rispetta obblighi di **collaborazione, informazione e notifica** verso il Titolare;
- Nomina **sub-responsabili** se autorizzato dal Titolare.

Il GDPR prevede una nuova figura, eventuale, nell'ambito del trattamento di dati personali :

IL SUB- RESPONSABILE DEL TRATTAMENTO

L'art. 28 del GDPR ai commi 2 e 4 espressamente prevede oggi la figura del sub-responsabile, ovvero del ricorso ad un altro/i responsabile/i da parte del responsabile nominato dal titolare, al fine di svolgere specifiche attività di trattamento.

Il sub-responsabile, secondo quanto disposto dal GDPR, è tenuto a rispettare i medesimi obblighi contrattuali che legano il titolare al primo responsabile, prevedendo in particolare garanzie sufficienti e la messa in atto di misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento.
Il responsabile è in ogni caso tenuto ad informare previamente il titolare del fatto che intende avvalersi di un altro soggetto nell'ambito del trattamento per cui è stato designato e il titolare ha diritto di opporsi ex ante alla designazione del sub-responsabile e di revocare ex post la sua adesione.

1

Il Titolare deve fornire al Responsabile :

- **Clausola contrattuale Titolare-Responsabile con Autorizzazione Generale alla nomina dei Sub- Responsabili o**
- **Clausola contrattuale Titolare-Responsabile con Autorizzazione Specifica Sub-Responsabile**

2

Il Responsabile deve fornire al Titolare la **Clausola contrattuale Responsabile - Sub Responsabile**

AMMINISTRATORE DI SISTEMA

L'amministratore di sistema è una figura professionale preposta alla gestione, alla sicurezza e alla manutenzione delle banche dati e dei sistemi e delle infrastrutture informatiche di un ente o un'impresa.

Tale figura, pur non essendo in alcun modo menzionata dal Regolamento GDPR, ma già prevista agli albori della *privacy* nella disciplina di protezione dei dati preesistente al Codice del 2003, è tutt'oggi regolamentata dal provvedimento dell'autorità Garante del 2008 intitolato "**Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".**

Con il provvedimento del 2008 il Garante impone una serie di accorgimenti circa le modalità di svolgimento delle funzioni assegnate agli amministratori di sistema e il loro rapporto con il titolare del trattamento, quali ad esempio le idonee misure volte a prevenire eventuali accessi non consentiti ai dati personali.

Precisa altresì il provvedimento che la funzione svolte dall'amministratore di sistema può tuttavia anche essere affidata ad un responsabile del trattamento (persona fisica o giuridica), od anche rappresentare una specifica qualifica di un incaricato (persona fisica).

Formalizzare nomina AdS Interni
e/o
Clausola Ads Esterni

OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO DEI DATI (ART. 28)



SONO RESPONSABILI DEL TRATTAMENTO TUTTI COLORO CHE EFFETTUANO UN TRATTAMENTO DATI PER CONTO DEL TITOLARE.

I RESPONSABILI DEL TRATTAMENTO DEI DATI DEVONO:

- TRATTARE I DATI SOLTANTO SU **ISTRUZIONE DOCUMENTATA** DEL TITOLARE DEL TRATTAMENTO
- GARANTIRE CHE LE PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI PERSONALI SIANO IMPEGNATE ALLA RISERVATEZZA O ABBIANO UN OBBLIGO LEGALE DI RISERVATEZZA.
- ADOTTARE TUTTE LE MISURE DI SICUREZZA ADEGUATE AL RISCHIO AI SENSI DELL'ART ART. 32 (PSEUDONIMIZZAZIONE, CAPACITÀ DI RIPRISTINARE TEMPESTIVAMENTE LA DISPONIBILITÀ E L'ACCESSO AI DATI PERSONALI IN CASO DI INCIDENTE FISICO O TECNICO.)
- **ASSISTERE IL TITOLARE** PER DARE SEGUITO ALLE RICHIESTE PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO

OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO DEI DATI (ART. 28)



- **ASSISTERE IL TITOLARE** NEL GARANTIRE IL RISPETTO DEGLI OBBLIGHI DI CUI ALL'ART. 32 (SICUREZZA) E 36 (CONSULTAZIONE PREVENTIVA) E IL RISPETTO DEL REGOLAMENTO
- **CONSENTIRE E CONTRIBUIRE ALLE ATTIVITÀ DI REVISIONE** COMPRESE LE ISPEZIONI, REALIZZATE DAL TITOLARE O DA UN ALTRO SOGGETTO DA QUESTI INCARICATO.
- **CANCELLARE O RESTITUIRE, SU SCELTA DEL TITOLARE** TUTTI I DATI PERSONALI DOPO CHE È TERMINATA LA PRESTAZIONE DEI SERVIZI RELATIVI AL TRATTAMENTO E CANCELLI LE COPIE ESISTENTI.

LA FIGURA DEL SUB- RESPONSABILE(ART. 28.2)

IL RE NON RICORRE AD **ALTRO RESPONSABILE** (PER L'ESECUZIONE DI SPECIFICHE ATTIVITÀ DI TRATTAMENTO PER CONTO DEL TITOLARE) SENZA **PREVIA AUTORIZZAZIONE SCRITTA**, SPECIFICA O GENERALE, DEL TITOLARE DEL TRATTAMENTO. NEL CASO DI AUTORIZZAZIONE SCRITTA GENERALE, IL RE INFORMA IL TI DI EVENTUALI MODIFICHE PREVISTE RIGUARDANTI L'AGGIUNTA O LA SOSTITUZIONE DI ALTRI RESPONSABILI AL TRATTAMENTO, DANDO COSÌ L'OPPORTUNITÀ AL TITOLARE DI OPPORSI A TALI MODIFICHE.

AL SUB-RESPONSABILE E/O RESPONSABILE DI II LIVELLO, CON CONTRATTO SONO IMPOSTI GLI STESSI OBBLIGHI IN MATERIA DP, CONTENUTI NEL CONTRATTO TRA TI E RE.

QUALORA IL SUB-RESPONSABILE OMETTA DI ADEMPIERE AGLI OBBLIGHI DEL TRATTAMENTO **IL RE INIZIALE CONSERVA NEI CONFRONTI DEL TITOLARE L'INTERA RESPONSABILITÀ DELL'ADEMPIMENTO DEGLI OBBLIGHI DEL SUB- RESPONSABILE**

VALUTAZIONE D'IMPATTO: SUSSISTENZA DI RISCHIO ELEVATO





Registro dei Trattamenti punto di partenza per…

Il Registro dei Trattamenti rappresenta una parte fondamentale del Sistema di Gestione DP in quanto, se fatto bene, consente al Titolare di :

- ❑ Definire un Organigramma DP
- ❑ Mappatura delle Terze Parti (Contitolari e Responsabili Esterni)
- ❑ Individuare Trattamenti che potrebbero presentare rischi elevati per i diritti e libertà delle persone fisiche

Quindi è un valido strumento per il Titolare per iniziare a individuare se ci sono trattamenti per i quali è necessario procedere con una DPIA.

VALUTAZIONE D'IMPATTO: SUSSISTENZA DI RISCHIO ELEVATO



Quando fare la Valutazione d'impatto ?

Altra novità del GDPR è la DPIA che il Titolare deve fare soltanto quando il trattamento *«può presentare un rischio elevato per i diritti e le libertà delle persone fisiche» (art. 35 par.1).* Essa è particolarmente importante quando viene introdotta una nuova tecnologia di trattamento dei dati.

Il **Gruppo di Lavoro articolo 29** – (Organo Consultivo dell'UE per la protezione dei dati personali) ha adottato le ***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.***

Linee Guida WP 248 rev.01

IL RISCHIO INERENTE IL TRATTAMENTO



LL **RISCHIO INERENTE AL TRATTAMENTO** È DA INTENDERSI COME **RISCHIO DI IMPATTI NEGATIVI SULLE LIBERTÀ E I DIRITTI DEGLI INTERESSATI** *(SI VEDANO CONSIDERANDO 75-77)*; TALI IMPATTI DOVRANNO ESSERE ANALIZZATI ATTRAVERSO UN APPOSITO PROCESSO DI VALUTAZIONE *(SI VEDANO ARTT. 35-36)* TENENDO CONTO DEI **RISCHI** NOTI O EVIDENZIABILI E DELLE MISURE TECNICHE E ORGANIZZATIVE (ANCHE DI SICUREZZA) CHE IL TITOLARE RITIENE DI DOVER ADOTTARE PER MITIGARE TALI **RISCHI** (SI SEGNALANO, AL RIGUARDO, LE LINEE-GUIDA IN MATERIA DI VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI ADOTTATE DAL GRUPPO "ARTICOLO 29", QUI DISPONIBILI: **WWW.GARANTEPRIVACY.IT/REGOLAMENTOUE/DPIA**). ALL´ESITO DI QUESTA VALUTAZIONE DI IMPATTO IL TITOLARE POTRÀ DECIDERE IN AUTONOMIA SE **INIZIARE IL TRATTAMENTO** (AVENDO ADOTTATO LE MISURE IDONEE A MITIGARE SUFFICIENTEMENTE IL **RISCHIO**) OVVERO **CONSULTARE L´AUTORITÀ DI CONTROLLO** COMPETENTE PER OTTENERE INDICAZIONI SU COME GESTIRE IL **RISCHIO** RESIDUALE; L´AUTORITÀ NON AVRÀ IL COMPITO DI "AUTORIZZARE" IL TRATTAMENTO, BENSÌ DI INDICARE LE MISURE ULTERIORI EVENTUALMENTE DA IMPLEMENTARE A CURA DEL TITOLARE E POTRÀ, OVE NECESSARIO, ADOTTARE TUTTE LE MISURE CORRETTIVE AI SENSI DELL´ART. 58: DALL´AMMONIMENTO DEL TITOLARE FINO ALLA LIMITAZIONE O AL DIVIETO DI PROCEDERE AL TRATTAMENTO.

VALUTAZIONE D'IMPATTO: CONSULTAZIONE PREVENTIVA



TITOLARE

- ✓ **Se DPIA attesta** che, in assenza di misure, meccanismi, garanzie di riduzione del rischio, **permangono rischi elevati**, ragionevolmente non mitigabili

Assistito su richiesta dal Responsabile

Consultazione preventiva

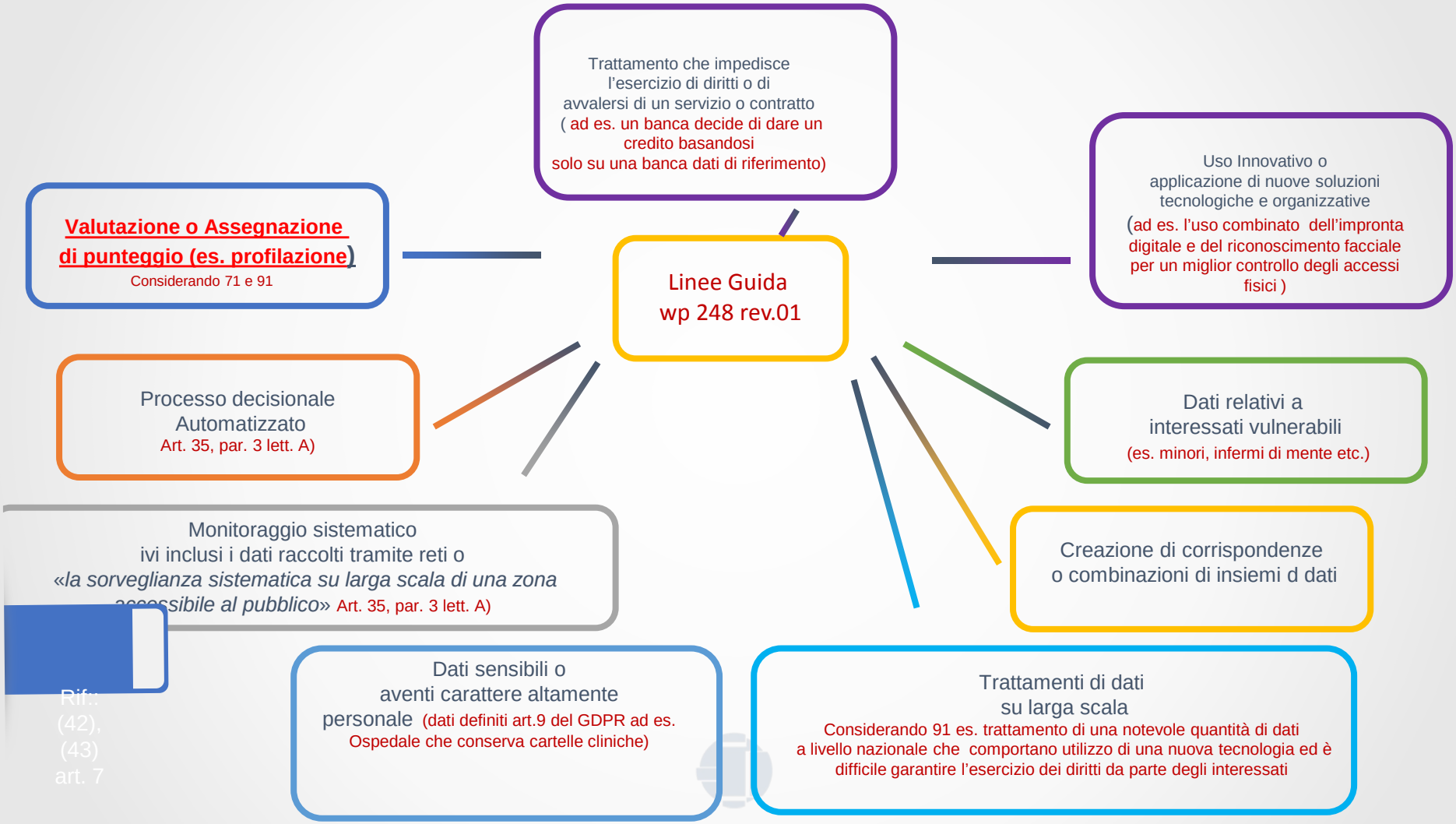
GARANTE

- ✓ **Risponde entro 8+6 settimane** al Titolare o Responsabile per iscritto

Rif::
(94)
Art. 36

9 Criteri per determinare il rischio elevato (Linee Guida wp 248 rev.01)

GRUPPOIMPERIALI



Misure tecnico-organizzative: Esempi e utilità



Misure Tecniche

Credenziali, Sistema autorizzazione, Cifratura, Antivirus, etc.



Misure Organizzative

Clausole DP, Contratti con Responsabili, Vincoli riservatezza, Istruzioni, Registro

- Sistema di **protezione e reazione alle violazioni** *(data breach)*
- Strumento di **verifica e dimostrazione di conformità**
- Strumento di **riduzione e valutazione del risc**
- **Modello organizzativo**
- Supporto e facilitazione **all'esercizio del diritti**

DPO

Responsabile della protezione dei dati (DPO)

- Il DPO deve essere prontamente coinvolto in tutte le questioni che interferiscono con la protezione dei dati personali (art. 38.1)
- Il DPO è indipendente e deve ricevere adeguato supporto in termini di risorse e accessibilità (art. 38.2)
- La nomina del DPO è obbligatoria (art. 37.1) per:
  - **Enti pubblici** eccetto le autorità giudiziarie per le funzioni giurisdizionali
  - Quando le «attività principali» «consistono in trattamenti» «che richiedono» (a) **monitoraggio di interessati** (b) regolare e sistematico (c) su larga scala
  - Quando l'attività principale consiste nel trattamento «su larga scala» di **dati sensibili e giudiziari**
- Un gruppo imprenditoriale può nominare anche un solo DPO purchè «sia facilmente raggiungibile da ciascuno stabilimento» (art. 37.2)

Implicazioni per le aziende

- La nomina, la posizione nell'organizzazione e le attività del DPO richiedono l'utilizzo di valutazioni innovative per l'ambiente della protezione dei dati

DPO

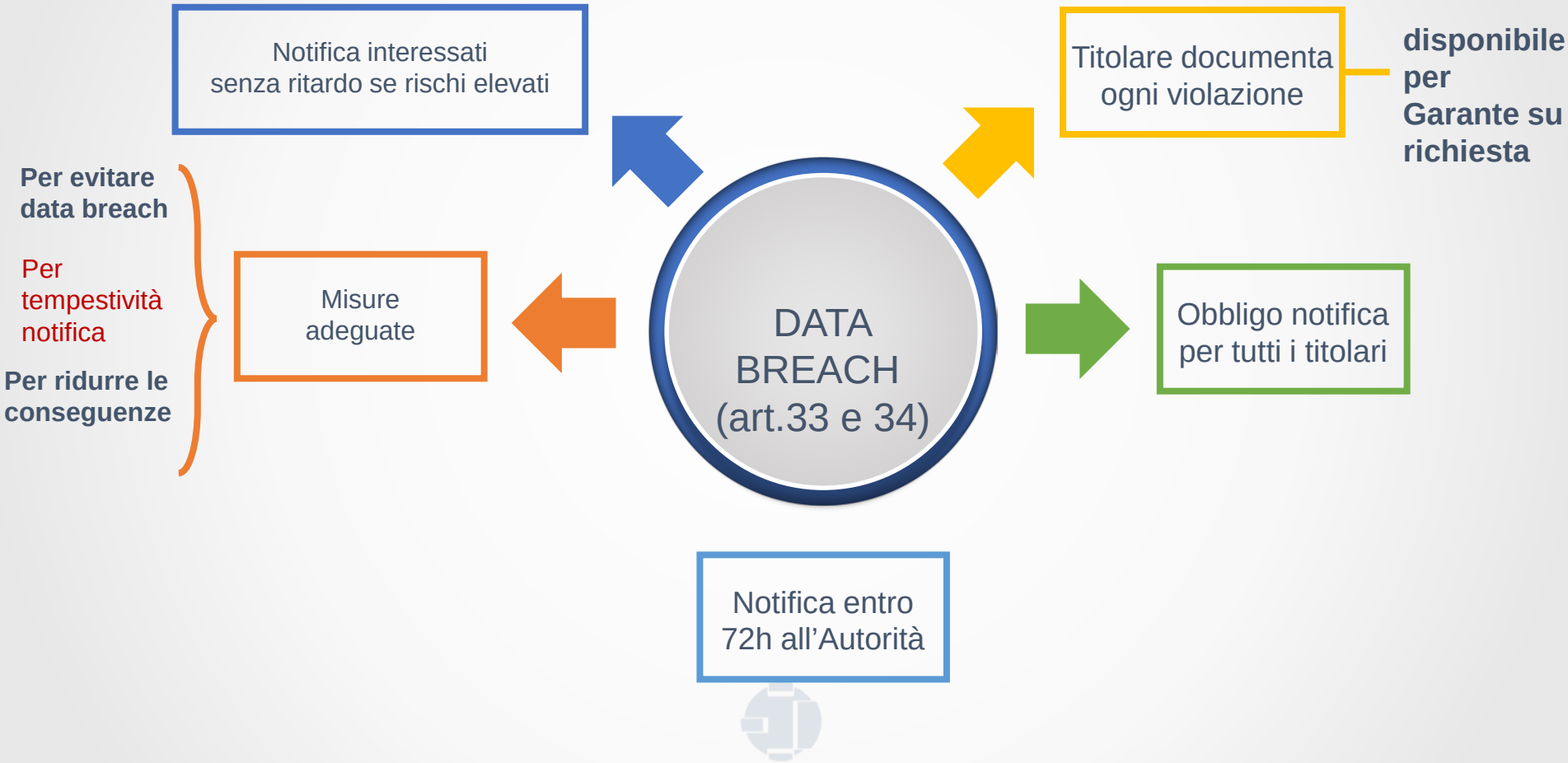
Responsabilità e accountability dei Titolari

Per assicurare I doveri e le responsabilità previsti per il DPO, i Titolari possono:
- Fare uso dello staff esistente, con training appositi
- Utilizzare contractor esterni
- Assumere nuovo staff

Benefici nel nominare un DPO

- Fornire un collegamento tra il Titolare del trattamento, l'interessato e l'Autorità di Controllo
- Implementare un Sistema di governo dei dati personali, coordinando i doveri e le responsabilità dei diversi ruoli coinvolti nella protezione dei dati personali
- Ridurre i costi amministrativi e di compliance

DATA BREACH: IN SINTESI



NOTIFICA DELLE VIOLAZIONI DI DATI PERSONALI

TUTTI I TITOLARI DEVONO NOTIFICARE ALL´AUTORITÀ DI CONTROLLO LE **VIOLAZIONI DI DATI PERSONALI** DI CUI VENGANO A CONOSCENZA, **ENTRO 72 ORE** E COMUNQUE "SENZA INGIUSTIFICATO RITARDO", MA **SOLTANTO SE RITENGONO PROBABILE CHE DA TALE VIOLAZIONE DERIVINO RISCHI** PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI (SI VEDA CONSIDERANDO 85). PERTANTO, **LA NOTIFICA ALL´AUTORITÀ** DELL´AVVENUTA VIOLAZIONE **NON È OBBLIGATORIA**, ESSENDO SUBORDINATA ALLA VALUTAZIONE DEL **RISCHIO** PER GLI INTERESSATI CHE SPETTA, ANCORA UNA VOLTA, AL TITOLARE. SE LA PROBABILITÀ DI TALE **RISCHIO** È ELEVATA, SI DOVRÀ INFORMARE DELLE VIOLAZIONE ANCHE GLI INTERESSATI, SEMPRE "SENZA INGIUSTIFICATO RITARDO"; FANNO ECCEZIONE LE CIRCOSTANZE INDICATE AL PARAGRAFO 3 DELL´ART. 34 (ADEGUATE MISURE TECNICHE DI SICUREZZA E SFORZO SPROPORZIONATO. **I CONTENUTI DELLA NOTIFICA** ALL´AUTORITÀ E DELLA COMUNICAZIONE AGLI INTERESSATI SONO INDICATI, **IN VIA NON ESCLUSIVA, AGLI ARTT. 33 E 34 DEL REGOLAMENTO**. SI SEGNALANO, AL RIGUARDO, LE LINEE-GUIDA IN MATERIA DI NOTIFICA DELLE VIOLAZIONI DI DATI PERSONALI DEL GRUPPO "ARTICOLO 29", QUI DISPONIBILI **WWW.GARANTEPRIVACY.IT/REGOLAMENTOUE/DATABREACH**.

RACCOMANDAZIONE DEL GARANTE

TUTTI I TITOLARI DI TRATTAMENTO DOVRANNO IN OGNI CASO **DOCUMENTARE LE VIOLAZIONI** DI DATI PERSONALI SUBITE, ANCHE SE NON NOTIFICATE ALL´AUTORITÀ DI CONTROLLO E NON COMUNICATE AGLI INTERESSATI, NONCHÉ LE RELATIVE CIRCOSTANZE E CONSEGUENZE E I PROVVEDIMENTI ADOTTATI *(SI VEDA ART. 33, PARAGRAFO 5).*

SI RACCOMANDA, PERTANTO, AI TITOLARI DI TRATTAMENTO DI ADOTTARE LE MISURE NECESSARIE **A DOCUMENTARE EVENTUALI VIOLAZIONI,** ESSENDO PERALTRO TENUTI A FORNIRE TALE DOCUMENTAZIONE, SU RICHIESTA, AL GARANTE IN CASO DI ACCERTAMENTI.

SANZIONI PREVISTE DAL SOLO REGOLAMENTO

Organizzazione — 2%

Mancata individuazione formale di ruoli e responsabilità nel trattamento dei dati personali

Sicurezza — 2%

Mancata adozione di adeguate misure di sicurezza

Informativa e Consenso — 4%

Non adempiere agli obblighi sul consenso

Accountability

Omessa DPIA quando richiesta, consultazione preliminare Autorità — 2%

Violazione diritti interessati, regole su trasferimenti extra-UE, obblighi Stati Membri, prescrizioni dell'Autorità — 4%

2% Sanzione sino a 10 milioni di euro o, in caso di imprese, sino al 2% del fatturato globale annuo

4% Sanzione sino a 20 milioni di euro o, in caso di imprese, sino al 4% del fatturato globale annuo

TUTELA INFORMAZIONI RISERVATE

CON D. LGS 63/2018 IL GOVERNO ITALIANO HA DATO ATTUAZIONE ALLA DIRETTIVA EUROPEA N. UE 2016/943 SULLA PROTEZIONE DEL KNOW HOW.

GLI ASPETTI SALIENTI DELLA NORMATIVA SONO:

- LA DEFINIZIONE DEL CONCETTO DI SEGRETI COMMERCIALI E TUTELA DEL LEGITTIMO DETENTORE.
- LA DEFINIZIONE DI VIOLAZIONE DEI SEGRETI COMMERCIALI
- ESTESA TUTELA ANCHE CONTRO LE CONDOTTE COLPOSE
- LA PROTEZIONE DEI SEGRETI COMMERCIALI ALL'INTERNO DEL PROCESSO CIVILE
- LA TUTELA PENALE E CIVILE DEI SEGRETI COMMERCIALI

NEL DECRETO EMERGE IL PRINCIPIO SECONDO CUI L'AUTORITÀ GIUDIZIARIA COMPETENTE A GIUDICARE DELLA SUSSISTENZA O MENO DELLA VIOLAZIONE DEL SEGRETO COMMERCIALE DEVE NECESSARIAMENTE VALUTARE SE IL SOGGETTO IL CUI DIRITTO SI RITIENE VIOLATO ABBIA POSTO IN ESSERE LE NECESSARIE E DOVUTE ACCORTEZZE VOLTE A PROTEGGERE IL SEGRETO COMMERCIALE.

È NECESSARIO, INFATTI, CHE SIA POSTO IN ESSERE UN SERIO CRITERIO DI DIFESA ED UNA CORRETTA PROTEZIONE, DIMOSTRABILE E DOCUMENTABILE: AD ESEMPIO UN CRITERIO DI DIFESA PREVEDE CIRCOLARI INTERNE SPECIFICHE, PROCEDURE DI SICUREZZA, ACCORDI DI NON DIVULGAZIONE, CLAUSOLE DI RISERVATEZZA O DI SICUREZZA, CONTRATTI DI SICUREZZA, DI SEGRETAZIONE, ECC. LE MISURE DI SALVAGUARDIA DOVRANNO ESSERE RIVOLTE SIA ALL'INTERNO – E QUINDI VERSO DIPENDENTI O COLLABORATORI - CHE ALL'ESTERNO, VERSO I TERZI, COME, AD ESEMPIO, I FORNITORI, I CLIENTI, PARTNERS.

ALLE AZIENDE È DATA ANCHE LA POSSIBILITÀ DI EMANARE UN PROPRIO **REGOLAMENTO INTERNO PER LA GESTIONE DELLE INFORMAZIONI.**

ALTRA MODALITÀ DI TUTELA VERSO L'INTERNO, SARÀ L'INSERIMENTO DI CLAUSOLE SPECIFICHE NEI CONTRATTI DI LAVORO.

PER QUANTO ATTIENE, INVECE, ALLE MISURE RIVOLTE VERSO L'ESTERNO, UNO DEGLI STRUMENTI GIURIDICI PIÙ UTILIZZATI, IN FASE PREVENTIVA, È QUELLO DEGLI ACCORDI DI RISERVATEZZA.

Tendere verso un Modello Integrato per…

Supportare gli organi di governo societario

a) Valutare l'adeguatezza dell'assetto organizzativo, amministrativo e contabile, con particolare attenzione al sistema di controllo interno
b) Ridurre e monitorare il Rischio di Non Conformità
c) Definire le regole organizzative (policy, etc.), relazionali (es. tra Manager e CdA) e aziendali (deleghe e procure)
d) Mantenere alto il livello di fiducia tra i diversi portatori d'interesse (dipendenti, fornitori, clienti, banche, controllori, etc.)
e) Migliorare il generale rating delle società, soprattutto con riferimento alla valorizzazione degli intangibili, agli investimenti e agli sforzi che la Società fa quotidianamente per il sociale, l'etica, l'ambiente, la sicurezza, in una parola: la sostenibilità.

CREAZIONE DEL VALORE IN AZIENDA GIOCANDO SU ECONOMIE DI SCALA



VANTAGGI ORGANIZZATIVI ULTERIORI. IL SUPPORTO ALLA CORPORATE GOVERNANCE CREA LE BASI PER

a) MIGLIORARE IL SISTEMA DI CONTROLLO INTERNO
b) SVILUPPARE MODELLI ORGANIZZATIVI FINALIZZATI NON SOLO ALLA PROTEZIONE DEL VALORE MA ANCHE ALLA CREAZIONE DEL VALORE IN AZIENDA.
c) INTEGRARE E VALORIZZARE I SISTEMI DI GESTIONE GIÀ ADOTTATI DALL'AZIENDA (FRA CUI QUALITÀ, SICUREZZA, PROTEZIONE DEI DATI, ANTIRICICLAGGIO, AMBIENTE), OTTIMIZZARE I PRESIDI DI CONTROLLO, MIGLIORARE LA CAPACITÀ DELL'AZIENDA DI UTILIZZARE IN MODO EFFICIENTE LE PROPRIE RISORSE RAGGIUNGENDO IN MODO EFFICACE I PROPRI OBIETTIVI.

Scopo della norma Il d.lgs. n. 231/01 introduce nel nostro ordinamento una forma di responsabilità penale diretta a carico di enti ed imprese, in conseguenza di determinati reati commessi dai vertici – soci, amministratori, dirigenti – o anche da semplici funzionari, dipendenti o consulenti esterni, quando sia dimostrato che l'ente abbia avuto interesse o acquisito un vantaggio materiale in seguito alla commissione del reato (ad es. una sovvenzione o un risparmio di imposta derivante da una truffa ai danni della Pubblica Amministrazione, ovvero un incremento di liquidità conseguente a riciclaggio di denaro sporco confluito sui conti aziendali).

Tipi di sanzioni Le sanzioni applicabili sono, necessariamente, di natura pecuniaria - e colpiscono direttamente le disponibilità liquide dell'ente (capitale sociale o fondo comune) – ma, nei casi più gravi, in aggiunta alla pena pecuniaria, il giudice penale può irrogare sanzioni di tipo "chirurgico" (c.d. interdittive) che, ad esempio, revocano il beneficio aziendale fraudolentemente ottenuto per effetto del reato (es. l'aggiudicazione di una gara truccata o la concessione di un finanziamento) o, comunque, pregiudicano il concreto esercizio della gestione dell'ente, impedendo la prosecuzione del ramo di attività nell'ambito della quale è stato commesso il reato.

Modello Organizzativo Per evitare tali conseguenze - o attenuarne la portata afflittiva una volta che il reato sia stato accertato - il Decreto 231 incentiva (ma non obbliga) imprese ed enti ad adottare, in funzione di prova liberatoria nel processo penale, un sistema organizzativo anticrimine che sia idoneo ad impedire la commissione dei reati in generale, ovvero, in caso di adozione post delictum, sia atto, quanto meno ad attestare la diligenza dell'ente nel prevenire reati della specie di quello verificatosi nel contesto aziendale o associativo, onde ottenere lo sconto di pena previsto dalla legge nei casi di ravvedimento operoso.

Organismo di Vigilanza Il concreto funzionamento di questo "modello" - di corretta organizzazione e gestione del rischio crimine - richiede protocolli operativi e presidi di controllo seri e costanti nel tempo, la cui manutenzione va affidata ad apposita entità di verifica della compliance aziendale ai protocolli anti-reato (c.d. organismo di vigilanza), autonoma ed indipendente dall'organo gestorio.

Attraverso la predisposizione e l'implementazione del Modello Organizzativo di Gestione e Controllo integrato con il Modello GDPR, **la società** ha la possibilità - integrando il proprio Sistema di Controllo Interno - di creare un Sistema Integrato, strutturato ed organico, di procedure e attività di controllo, costruito in funzione dei "processi sensibili" della Società al fine di consentire alla stessa di perseguire globalmente i seguenti obiettivi:

- Miglioramento del sistema di *corporate governance*, limitando il rischio di commissione dei reati presupposto ex D.Lgs. 231/01 e incorrere in sanzioni GDPR;
- Creazione di una nuova cultura della gestione del rischio e del relativo controllo;
- Tutela dell'immagine e della reputazione aziendale;
- Promozione del livello di professionalità dei dipendenti;
- Sensibilizzazione dei soggetti che operano per conto o nell'interesse della struttura ai rischi connessi alla violazione del Modello Organizzativo e dei principi e valori contenuti nel Codice Etico, con particolare riguardo al profilo della responsabilità dell'Ente in ipotesi di commissione di reato – presupposto del D.Lgs. 231/01 rafforzando anche l'osservanza dei principi del Regolamento .

In particolare, l'adozione del " Modello 231" integrato con il «Modello GDPR» persegue tre obiettivi fondamentali:

1

a) **Obiettivo giuridico** di ottenere l'esonero da responsabilità da reato dell'ente, qualora siano rilevati e perseguiti dal giudice penale comportamenti criminosi da parte di soggetti che operano per suo conto e ridurre il rischio sanzione GDPR : «**Protezione di valore**».

2

b) **Obiettivo gestionale** di perfezionare il sistema organizzativo e quello dei controlli interni e gestione dei rischi in termini di maggiore formalizzazione, segregazione e chiarezza delle mansioni, delle responsabilità individuali e delle linee di riporto. Valorizzare il proprio Know – How e patrimonio Informativo. Per tale motivo l'adozione del Modello 231 è uno dei primi requisiti richiesto dai **Fondi** o per la **Quotazione in Borsa**.

3

c) **Obiettivo reputazionale** di preservare il buon nome e l'immagine aziendale e consolidare la reputazione di ente rispettoso della legalità, attraverso interventi di comunicazione e formazione del personale sul modello organizzativo anti-reato e la diffusione ed effettiva attuazione di un codice etico calato sulla specificità dell'ente. Consente all'azienda di massimizzare il valore del **Rating di Legalità** «Bollino blu» per le aziende virtuose, potendo usufruire di vantaggi sia per l'accesso al credito che nell'ambito di finanziamenti pubblici o gare.

In conclusione, la conformità al decreto 231 e al GDPR deve essere valutata nella prospettiva più generale di «**Creazione di valore**» aggiunto legato all'etica e alla legalità di impresa.

Grazie

Avv. Riccardo Imperiali di Francavilla

riccardo.imperiali@imperiali.com

Dott.ssa Anna Irace

anna.irace@imperiali.com

Aggiungici su

gruppoimperiali

© 2016 gruppoimperiali