UNIONE FIDUCIARIA S.p.A.

In collaborazione con:
Il Sole 24 ORE

WHISTLEBLOWING FORUM

Tutela dell'azienda e lotta alla corruzione a un anno dall'emanazione della Legge

Milano, 30 novembre 2018

WHISTLEBLOWING ITALIA

OFFICIAL SPONSOR

CAGNOLA & ASSOCIATI STUDIO LEGALE

GRIMALDI STUDIO LEGALE

MAZARS

CON IL PATROCINIO DI

Milano Comune di Milano

Ordine dei Giornalisti Consiglio regionale della Lombardia

ASSOHOLDING Associazione Holding di Partecipazione

AODV 231 Associazione dei Componenti degli Organismi di Vigilanza ex D.Lgs. 231/2001

Fondazione Studi Consulenti del Lavoro Consiglio Nazionale dell'Ordine

eventi.ilsole24ore.com

24ORE EVENTI

24ORE BUSINESS SCHOOL

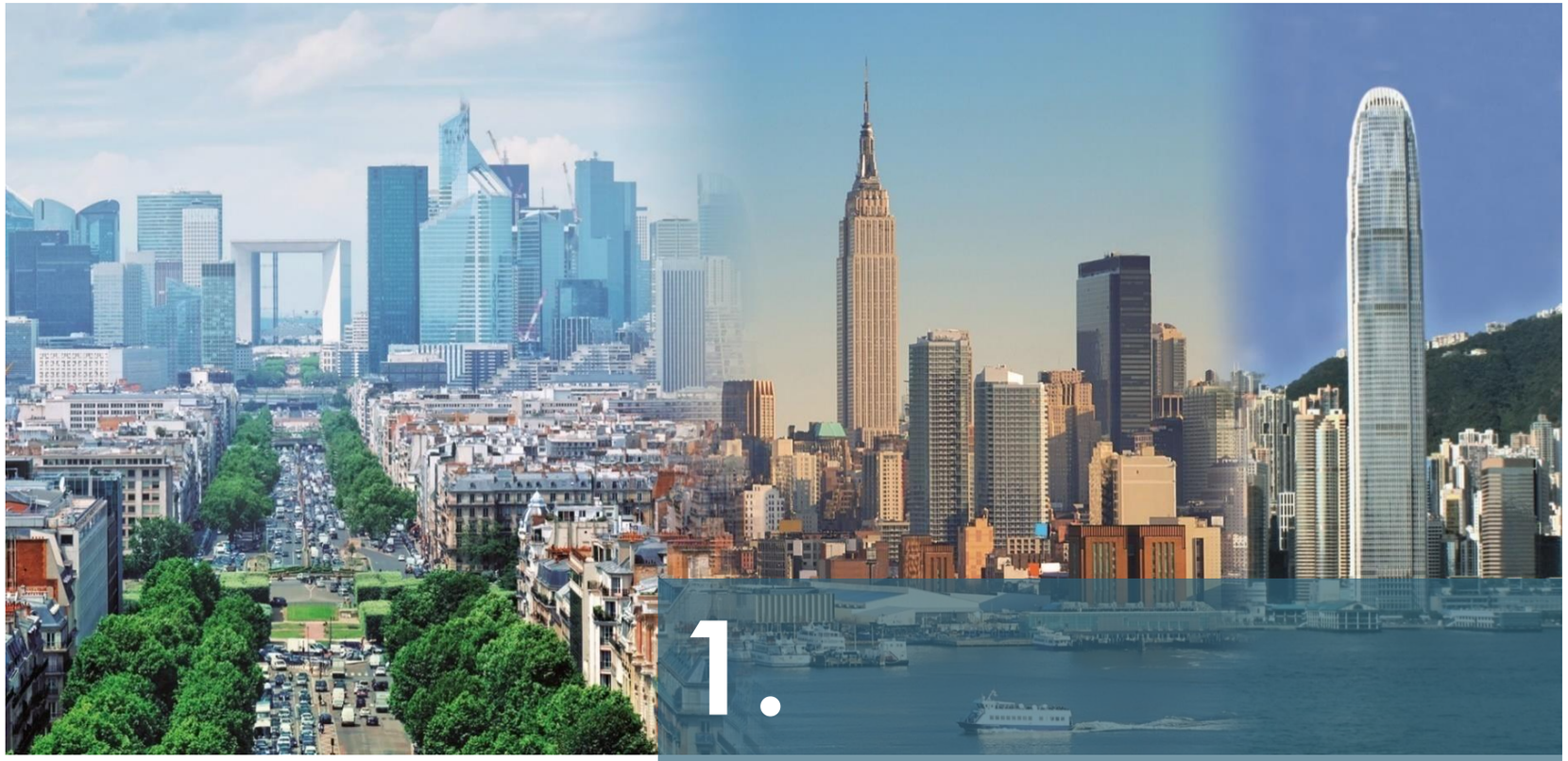
WHISTLEBLOWING E PRIVACY – MODELLO, METODOLOGIA E STRUMENTI

30/11/2018

MAZARS

AGENDA

- Mazars
- La normativa Privacy e il Whistleblowing
- L’informatizzazione del Whistleblowing
- La definizione di misure idonee a tutelare la riservatezza dell’identità del segnalante
- La tutela del segnalato
- Le fasi di progetto del Whistleblowing

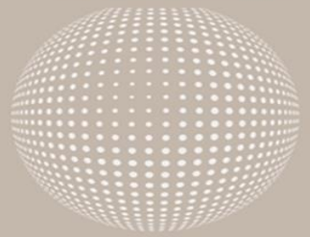


1.

Panoramica di Mazars

UNO SGUARDO SU MAZARS NEL MONDO ED IN ITALIA

20,000
Professionisti



980
Soci

- Europa → 10,138
- Asia Pacifico → 3,806
- America → 2,635
- Africa & Medio Oriente → 3,421

102
Paesi integrati
International Reach

>100
Fortune 500 Global

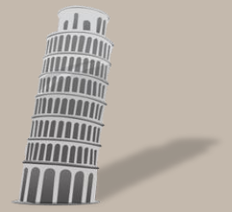
Global Coverage
300
uffici

Growth X 2
in size in 10 years

1,5 bn €
Turnover

- Mazars è un'organizzazione internazionale, integrata e indipendente
  ……..
- Specializzata nei servizi Audit e Assurance, Accounting, Consulting, Financial Advisory, Tax e Legal
- ……..
- Costituita da professionisti e esperti internazionali che condividono le medesime visione e mentalità collaborativa

240 Professionisti



33
Partners

- Milano
- Roma
- Padova
- Firenze
- Torino
- Verona

Advisory & Compliance
25+ staff

Bookkeeping Outsourcing & Payroll
60 staff

Audit & Assurance
120 staff

Corporate Finance & Transaction Services
25+ staff

20m €
fee income

MAZARS

LE COMPETENZE IN AMBITO IT RISK&ADVISORY

IT Strategy & Governance

- Assessment maturità processi
- Assessment competenze
- Strategia IT
- Ottimizzazione dei processi IT
- Demand Management
- Customer Satisfaction ICT

COBIT 5 AN ISACA® FRAMEWORK

ITIL®

IT Assurance & Compliance

- IT Audit / IT Assessment
- Compliance di settore
- Software Asset Management
- Dematerializzazione documentale
- Compliance Integrata
- Report Assurance (ISAE3402)
- Adeguamento sistemi IFRS/OIC
- Industry 4.0

AICPA SOC

IFRS

IT Solution

- Analisi Sistemi informativi
- Software Selection
- Implementazione Sistemi Informativi (con Partner Certificati)
- Robotization
- Data Analytics
- Quality Assurance
- Migrazione e verifica dei dati

Security e Gestione Rischi

- Cyber Security Services
- IT Risk Assessment & Management
- Segregation of Duties
- Servizi ISO27001/ISO27002
- Business Continuity e Disaster Recovery
- Travel Security

ISO

Privacy & Whistleblowing

- Privacy Compliance (GDPR)
- Servizi di Data Protection Officer
- Data Breach management
- Data Protection Impact Assessment (DPIA)
- Whistleblowing Compliance
- Modelli ISO 37001

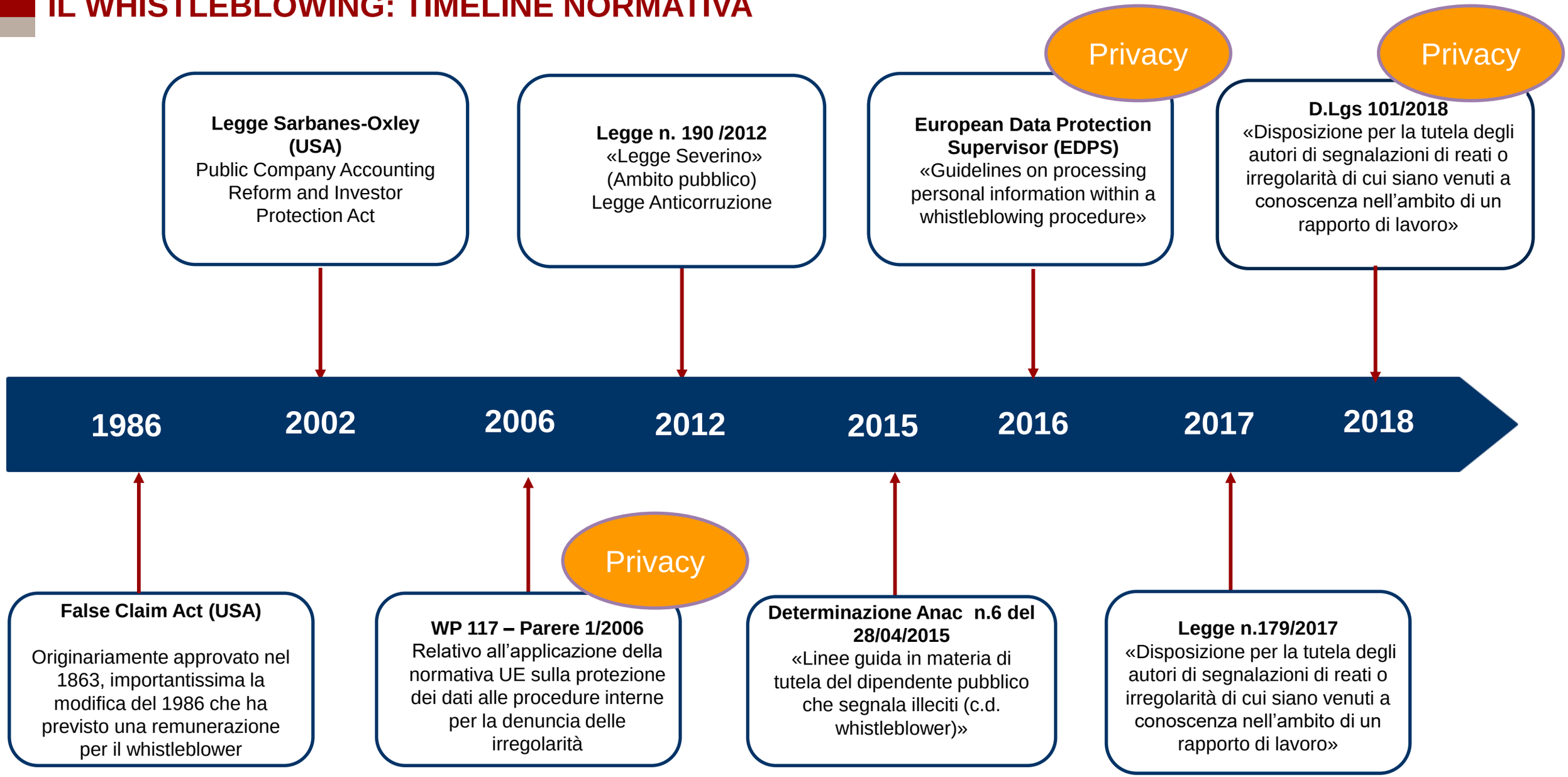
GDPR

MAZARS

2.

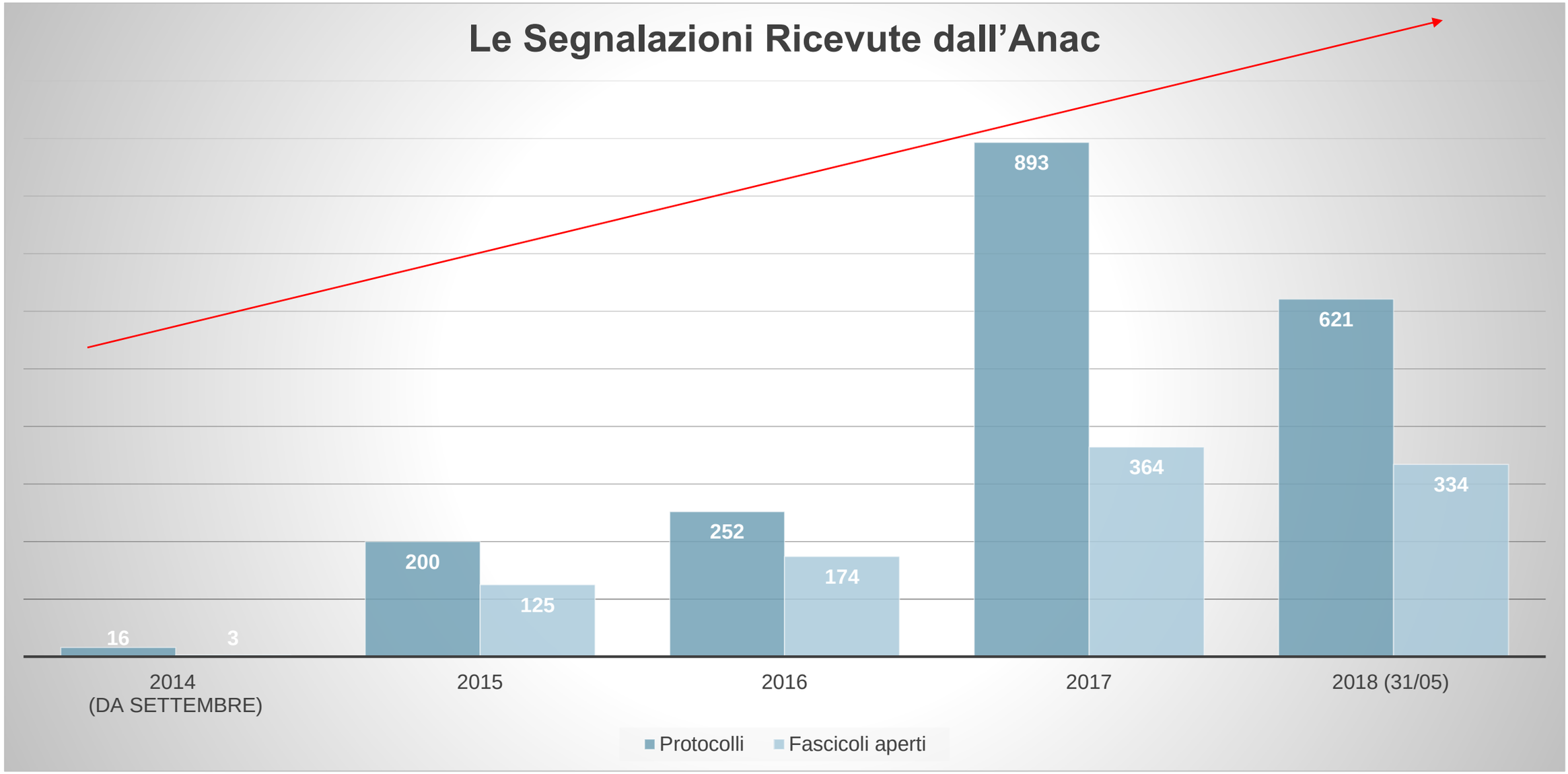
La normativa Privacy e il Whistleblowing

IL WHISTLEBLOWING: TIMELINE NORMATIVA



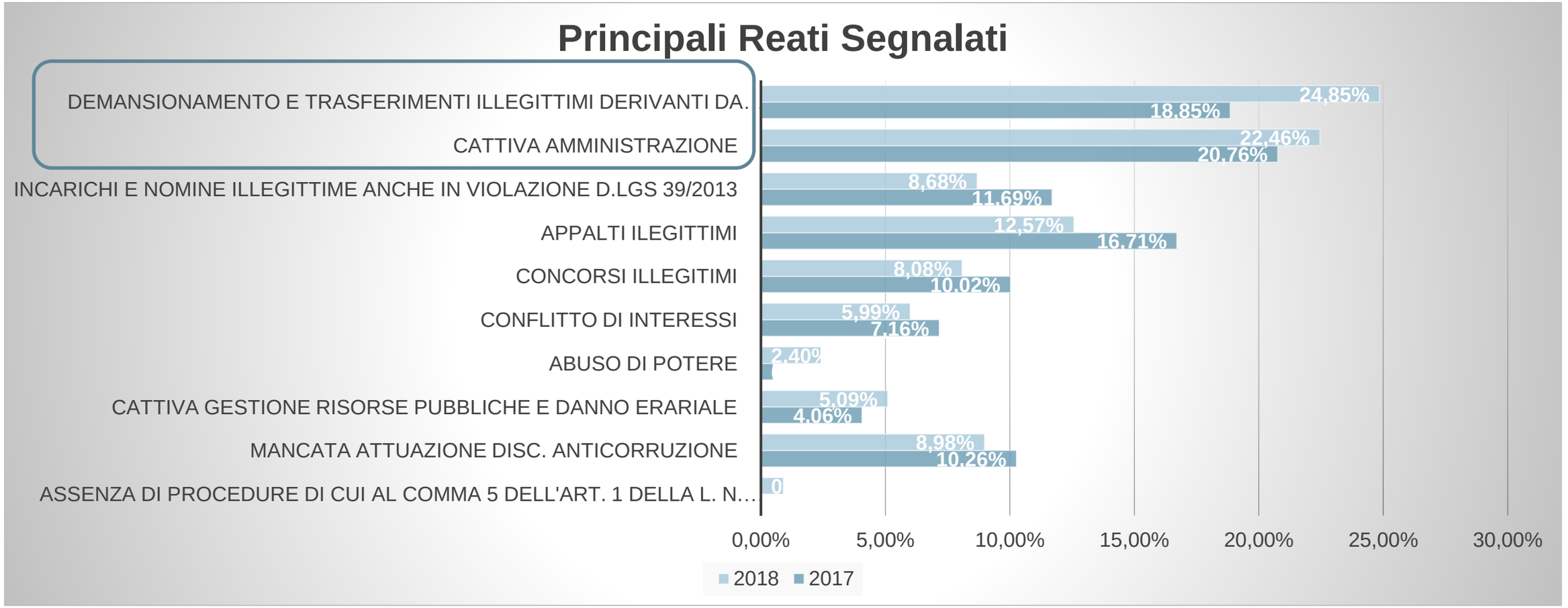
MAZARS

DATI ANAC – ANDAMENTO DELLE SEGNALAZIONI IN AMBITO PUBBLICO



MAZARS

DATI ANAC – PRINCIPALI REATI SEGNALATI



Demansionamento e cattiva amministrazione sono esempi che potrebbero interessare anche il settore privato.

MAZARS

LE PRINCIPALI CARATTERISTICHE DEL WHISTLEBLOWING (DAL WP 117 AL D. LGS. 101/2018)

Necessità di definire sistemi interni volti a **permettere la segnalazione (tramite canali specifici)** da parte del personale di atti o fatti che possano costituire una violazione

Tutelare adeguatamente il soggetto segnalante contro **condotte ritorsive, discriminatorie o comunque sleali** conseguenti alla segnalazione

Garantire la **riservatezza dell'identità del segnalante**, che può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato o motivi di sicurezza, **limitando, ritardando o eventualmente eludendo il diritto di accesso (e gli altri diritti privacy)** per mezzo di una comunicazione motivata.

E' necessario stabilire delle procedure di **data retention**

Nomina di un **responsabile** dei **sistemi interni di segnalazione** che assicura il corretto svolgimento del procedimento e riferisce direttamente e senza indugio agli organi aziendali le informazioni oggetto di segnalazione, ove rilevanti

Garanzia di **misure di sicurezza adeguate** per permettere a **tutti i soggetti coinvolti** nel processo di segnalazione la confidenzialità e la riservatezza dei dati.

DECRETO 101/2018 E WHISTLEBLOWING - COSA INTRODUCE

Esempio di indice Policy di gestione dei diritti interessati

- **Introduce limitazione ai diritti degli interessati in caso di segnalazioni ai sensi della Legge 179.**
- **Suggeriamo di integrare la procedura di gestione dei diritti degli interessati** sulla base delle limitazioni introdotte dal D.Lgs. 101/2018.
- **Dare informativa allegata alla procedura di Whistleblowing:**
  - E' assicurata la riservatezza dell'identità dei segnalanti;
  - L'informativa sia facilmente reperibili da tutti gli interessati (Internet e intranet)
  - Il Diritto di accesso e gli altri diritti possono essere limitati, ritardati o eventualmente elusi (a meno del consenso, ecc.)

MAZARS

IMPATTI PRIVACY

- La disciplina del whistleblowing, entrata in vigore in seguito alla pubblicazione in Gazzetta Ufficiale della **Legge del 30 Novembre 2017 n.179**, recante «Disposizione per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato», si integra con il Regolamento UE 679/2016 su diversi aspetti.

	Privato	Pubblico	Impatti Privacy
Soggetto abilitato alla segnalazione	• Soggetti con funzioni di rappresentanza/amministrazione o direzione dell'ente • Soggetti che esercitano, anche di fatto, la gestione ed il controllo dell'ente • Soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti precedenti	• Dipendenti pubblici • Dipendenti di enti pubblici economici • Dipendenti di diritto privato sottoposti a controllo pubblico • Dipendenti e collaboratori di imprese fornitrici di beni o servizi alla pubblica amministrazione	• Persone Fisiche: possibilità di rendere anonimo l'accesso • Tutela del segnalante
Oggetto della segnalazione	• Segnalazioni circostanziate di condotte illecite, rilevanti e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente	• Condotte illecite di cui è venuto a conoscenza in ragione del proprio rapporto di lavoro	• Potrebbero contenere sia dati personali che particolari • Registro dei trattamenti (whistleblowing) • Interpellare DPO su misure organizzative e di sicurezza da adottare in tali casi • Informativa a tutti i soggetti interessati • Tutela del segnalato
Canale informatico di segnalazione	• Previsto almeno un canale alternativo informatico per le segnalazioni	• Previsto l'utilizzo di modalità anche informatiche	• Analisi dei rischi • DPIA (art. 35 GDPR) – Allegato 1 Provvedimento Garante Privacy n. 469 • Suggerimento: ISAE 3402 - ISAE 3000 specifico sui controlli GDPR calati sul software
Criptazione del canale di segnalazione	• Non specificato	• Previsto	• Consigliato un canale cifrato
Responsabile del sistema di segnalazione	• Potrebbe essere esterno	• Responsabile anticorruzione e trasparenza (RPCT) – interno	• Se esterno va nominato Responsabile Esterno ai sensi del Regolamento UE 2016/679 con la relativa clausola • Se interno come «referente privacy» la nomina va fatta specifica

3.

Informatizzazione del Whistleblowing

INFORMATIZZAZIONE DEL WHISTLEBLOWING: PERIMETRO

Il Macro-perimetro delle segnalazioni comprende:

1. Segnalazione o chiarimenti di comportamenti propri o altrui relativamente ai temi del Codice Etico e di Condotta delle più generali Policy per il Rispetto dei Diritti Umani (es: violazione di divieti e disposizioni aziendali, controlli sull'operato dei fornitori);
2. Comunicazioni di presunte violazioni di norme di legge o regolamenti (es: inosservanza di clausole contrattuali, diffamazione, minacce, violazione della privacy, frodi, improprio utilizzo di dotazioni aziendali);
3. Comunicazioni di presunte violazioni del Modello Organizzativo 231/2001;
4. Denunce provenienti da Terzi aventi ad oggetto presunti rilievi, irregolarità e fatti censurabili;
5. Esposti riguardanti tematiche di contabilità, controlli.

Destinatari del whistleblowing sono:

1. Vertici aziendali ed i componenti degli organi sociali;
2. Tutti i dipendenti;
3. Tutti i partner, clienti, fornitori, consulenti, collaboratori, soci e, più in generale, chiunque sia in relazioni d'interessi.

PERIMETRO E DESTINATARI DEL WHISTLEBLOWING – COSA E' ESCLUSO

Dal perimetro del modello di whistleblowing sono escluse le seguenti segnalazioni:

- Segnalazione di **incidenti di security** che riguardano le risorse umane, materiali ed immateriali (quali, ad esempio, malfunzionamenti software, guasti alla rete aziendale, smarrimento o distruzione accidentale di documenti, incidenti di sicurezza ICT, furti);
- **Reclami commerciali**
- **Data Breach**
- Altre segnalazioni in base alle specifiche procedure già in essere nella Società

ELEMENTI ESSENZIALI NELLA INFORMATIZZAZIONE DEL WHISTLEBLOWING

Procedura di Whistleblowing – Matrice RACI

R=Responsible (Resp. Della realizzazione dell'attività); **A= Accountable** (Resp. Dell'approvazione/ validazione); **C=Consulted** (Coinvolto nell'attività**); I=Informed** (informato dell'attività)

Attori / Attività	Whistleblower	Comitato Whistleblowing / Responsabile Whistleblowing	Altre Funzioni (es: Compliance, Legale, Risorse Umane, ecc.)	Vertice Aziendale
Invio delle Segnalazioni	**R**	**I**		
Analisi Preliminare		**A,R**	**C**	
Approfondimenti specifici		**A,R**	**C,R**	
Comunicazione Risultati		**A,R**	**I**	
Reportistica		**A,R**		

Al fine di garantire la gestione e la tracciabilità delle segnalazioni e delle relative attività si suggerisce di implementare nelle procedure di whistleblowing dei flow chart disegnati ad hoc per le società e gli enti pubblici

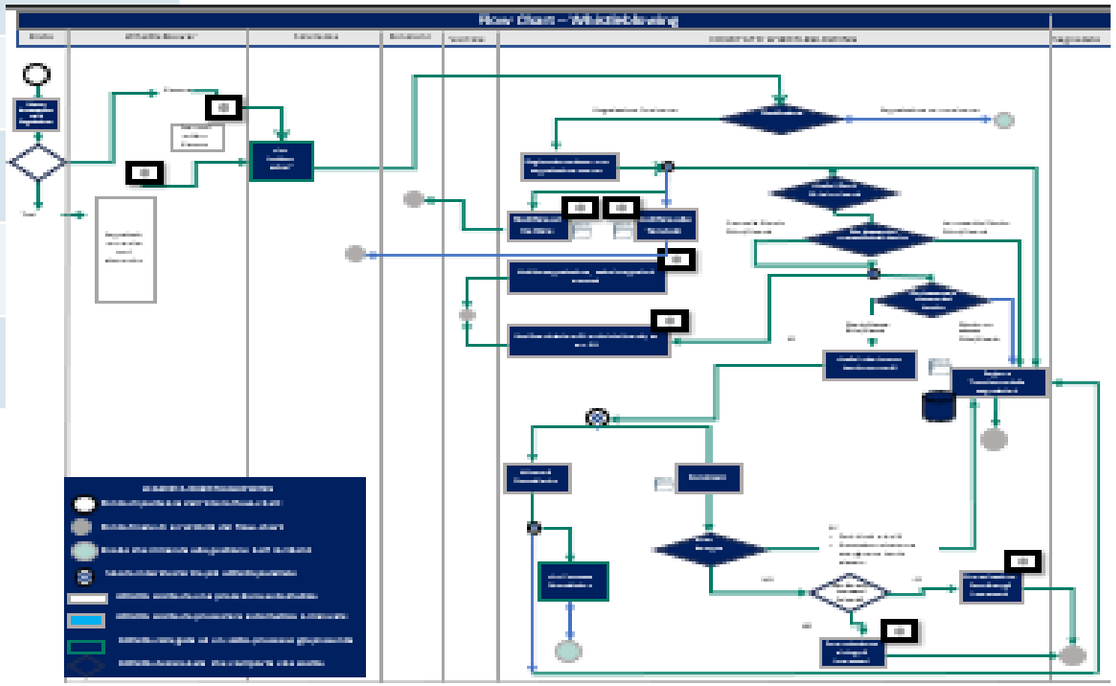


TABELLA ILLECITI – DATA RETENTION POLICY

DEFINIRE POLICY DI DATA RETENTION IN BASE AI TEMPI DI PRESCIZIONE DEI REATI/ILLECITI E CONSEGUENTI PROCEDURE DI CANCELLAZIONE DEI DATI

MAZARS

Descrizione Reato	Rif. Artt. 231	Data di introduzione	Anno di introduzione	Fonte Originale	Artt. Fonte originale	Sanzione Amministrativa Min (quota)	Sanzione Amministrativa Max (quota)	Tempo di conservazione	Note
Corruzione per l'esercizio della funzione	25 Concussione, induzione indebita a dareo promettere utilità e corruzione (art. sostituito dalla Legge Anticorruzione del Novembre 2012)	04/07/2001	2001	C.P.	318	100	200	6 anni	Le sanzioni pecuniarie previste si applicano all'ente anche quando t sono stati commessi dalle persone indicate negli articoli 320 e 32
False comunicazioni sociali delle societa' quotate	25 ter Reati societari [Articolo aggiunto dal D.Lgs. 11 aprile 2002 n. 61, art. 3 e modificato dalla Legge 69/15, in vigore dal 14/06/2015].	16/04/2002	2002	C.C.	2622	400	600	8 anni	-

COSA DEVE CONTENERE IL SOFTWARE

L'utente può decidere se effettuare una segnalazione anonima oppure inserire le proprie generalità.

Qualora il segnalante volesse inserire le proprie generalità (**riservatezza**), deve inserire i seguenti dati:

a) Paese
b) Società
c) Funzione aziendale
d) Area aziendale
e) Luogo
f) Data
g) Soggetto segnalato
h) Tipologia di illecito segnalato

Il segnalante ha la possibilità di scrivere in chiaro il proprio nome e **poter dare il consenso** all'utilizzo dei propri dati

Il segnalante dovrà inoltre descrivere la tipologia di condotta illecita:

a) La tipologia di reato commesso;
b) La tipologia di illecito commesso;
c) Se viola il codice di comportamento / codice etico
d) Danno reputazionale per la società
e) Se viola le norme ambientali o di sicurezza sul lavoro
f) Altre

Key Code

Per tracciare la segnalazione, all'utente verrà rilasciato **un codice dal software** per poter accedere e verificare lo stato di avanzamento.

4.

La definizione di misure idonee a tutelare la riservatezza dell'identità del segnalante

LE MISURE IDONEE A TUTELARE LA RISERVATEZZA DEL SEGNALANTE: LE ORIGINI

La Legge n. 190/2012 “Disposizioni per la prevenzione e la repressione della corruzione e dell’illegalità nella pubblica amministrazione” (c.d. Legge Severino) introduce per la prima volta in Italia una norma specificamente diretta alla regolamentazione del whistleblowing e la conseguente **protezione del segnalante**.

Viene introdotto l’**art. 54 bis** al D.lgs. 165/2001, norma che regola l’attività lavorativa dei dipendenti della P.A.:

regime di garanzia contro tre possibili ipotesi di ritorsioni quali il **licenziamento**, le **sanzioni disciplinari** e **misure discriminatorie** dirette o indirette

Criticità:

- **Tutela insufficiente del segnalante**: manca il riferimento alla tutela verso la calunnia, la diffamazione e la responsabilità civile
- Il riferimento alle «condotte illecite» è eccessivamente generico (ANAC è dovuta intervenire per dettagliare le fattispecie incluse)

LE MISURE IDONEE A TUTELARE LA RISERVATEZZA DEL SEGNALANTE: LA L. 179/2017

L. n. 179/2017 ha introdotto alcune rilevanti novità soprattutto in tema di tutela del segnalante

- **Ampliamento tutele** verso il segnalante
- **Inversione dell'onere della prova** in caso di controversie per sanzioni al whistleblower
- Almeno un **canale alternativo di segnalazione** idoneo a garantire, **con modalità informatiche**, la riservatezza dell'identità del segnalante (best practice: **segnalazione anonima**)
- Copertura della riservatezza del segnalante durante tutta la fase delle indagini per procedimenti penali e della Corte dei Conti (c.d. **segreto istruttorio**)

Criticità:

- Il segnalato poteva appellarsi al diritto accesso ai sensi del D.lgs 196/2003 ai fini di ottenere informazioni sul segnalante

LE MISURE IDONEE A TUTELARE LA RISERVATEZZA DEL SEGNALANTE: IL D.LGS. 101/2018

Art. 2-undecies (**Limitazioni ai diritti dell'interessato**)

I diritti di cui agli articoli da 15 a 22 del 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:

f) alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio.

Il D.lgs 101/2018 introduce un livello ulteriore di protezione nei confronti dell'identità del segnalante:

I diritti dell'interessato previsti dal GDPR non si applicheranno per il soggetto coinvolto in una procedura di whistleblowing

BENEFICI DEL WHISTLEBLOWING NEGLI STATI UNITI – PREMIO WHISTLEBLOWER

Negli Stati Uniti, esiste una legislazione a livello statale, ma la regolamentazione più importante è a livello federale. Innanzitutto, il **False Claim Act,** originariamente approvato nel 1863. Importantissima la modifica del 1986 che ha previsto una remunerazione per il *whistleblower* con una **percentuale (25-30%) sul totale che il Governo recupera grazie alle informazioni denunciate.**

Inoltre, la **Security Exchange Commission** ha previsto un **«whistleblower award»** tramite il Regolamento 240 per poter incentivare le segnalazioni. La **ratio** della ricompensa è che il *whistleblower* assuma i rischi professionali e personali (es. licenziamento) nel denunciare l'illecito, ma la detta ricompensa rappresenta sicuramente un formidabile incentivo alla presentazione di denunce. Si pensi, per esempio, alla cospicua remunerazione in denaro **($14 milioni**) che un *whistleblower* ha ricevuto dalla SEC nel 2013.

In Italia si è tentato di introdurre tale sistema tramite la **proposta di legge** AC 3365, presentata il 15 ottobre 2015 dalla Deputata Francesca Businarolo. Se dovesse mai essere adottata, la scelta di premiare i whistleblower non graverebbe sui contribuenti, ma come per il modello americano, le ricompense pecuniarie sarebbero corrisposte da un **fondo finanziato** dalle sanzioni comminate ai trasgressori.

BENEFICIO A SEGNALARE - CASI CONCRETI DI SUCCESSO DEL WHISTLEBLOWING

Ferrovie Nord

SCIENZA E FILOSOFIA

Buone nuove per il whistleblower

–di **Guido Romeo** | 20 ottobre 2017

Il paradosso della vicenda al centro de *Il Disobbediente*, è che Franzoso fa ciò che è esattamente pagato per fare. Nel 2015, da incaricato dell'audit interno di Ferrovie Nord, rileva le gravissime irregolarità della gestione a dir poco disinvolta dell'allora presidente Norberto Achille, il quale aveva utilizzato a fini personali e familiari carte di credito, telefoni e auto dell'azienda partecipata per oltre 400mila euro. Quando le segnalazioni interne non sembrano sortire nessun effetto, Franzoso, ex-carabiniere e novizio dei gesuiti, denuncia tutto agli ex-colleghi dell'Arma. Nel farlo commette un'imprudenza dettata forse dall'orgoglio o da un pizzico di quello che a molti colleghi può apparire narcisismo moralista. Invece di fare una denuncia anonima per venire poi convocato a rispondere come gli altri suoi colleghi, sceglie di metterci la faccia. Una scelta che gli costerà mesi di *mobbing*, di spese in avvocati un po' troppo ambiziosi e infine il posto, ma soprattutto molte amicizie e un fortissimo scontro con la sua stessa famiglia. Quella di Franzoso è una scelta

Articolo Sole24Ore – 20/10/2017 - entrato nel Cda

SERVIZIO | SCANDALO IN DANIMARCA

Danske Bank incriminata per il maxiriciclaggio da 200 miliardi di euro

–di **Angelo Mincuzzi** | @Angelo_Mincuzzi | 28 novembre 2018

The Trust Project

Articolo Sole24Ore – 28/11/2018 – ha consentito di portare alla luce flussi di riciclaggio.

5.

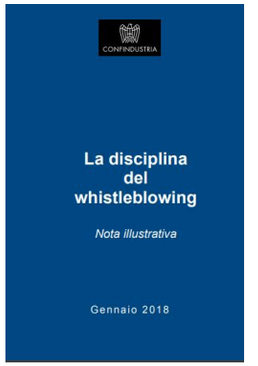
La tutela del segnalato

LA TUTELA DEL SEGNALATO: LE LINEE GUIDA CONFINDUSTRIA 2018

La nota illustrativa inerente la disciplina del whistleblowing redatta da Confindustria ha affrontato la tematica della **tutela del segnalato** nell'ottica di contemperare le esigenze di trasparenza con il diritto di difesa ex art. 24 della Costituzione.

Ricordando che emerge una disciplina di favor nei confronti del segnalante, viene segnalato che:

In ogni caso, permane un'impostazione tesa a proteggere il soggetto segnalante in misura prevalente rispetto a quello segnalato. Per evitare eccessivi squilibri in fase applicativa, ad esempio, l'esigenza di tutelare la riservatezza dell'identità del primo dovrebbe essere contemperata con quella di ***salvaguardare il diritto di difesa del segnalato****, nel caso in cui la segnalazione sia abusiva. Infatti, il diritto di difesa del segnalato potrà essere pienamente esercitato solo dopo aver individuato l'identità del denunciante e accertato l'eventuale natura abusiva della segnalazione; tuttavia, nelle more della definizione del giudizio, la posizione del soggetto segnalato rischia di essere compromessa, quanto meno sul piano reputazionale.*



CONFINDUSTRIA

Gennaio 2018

Stante la lacuna della norma è compito delle aziende prevedere delle misure idonee a consentire la **difesa del segnalato**, anche mantenendo traccia di tutto il flusso informativo del whistleblowing

N.B. Il segnalato in caso di segnalazione non veritiera potrebbe rivalersi anche sull'azienda in caso di danno qualora gli sia impedito di difendersi immotivatamente.

MAZARS

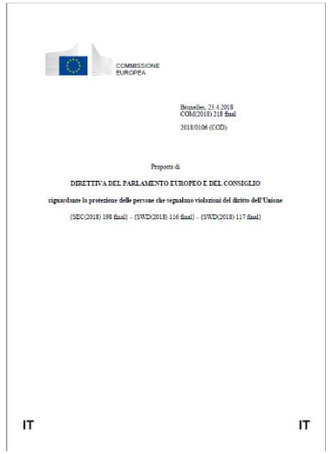
LA TUTELA DEL SEGNALATO: PROPOSTA DIRETTIVA EUROPEA «WHISTLEBLOWING»

E’ la proposta di direttiva riguardante la protezione delle persone che segnalano violazioni del diritto dell’Unione (23 Aprile 2018)

Articolo 16

Misure per la protezione delle persone coinvolte

1. Gli Stati membri garantiscono che le persone coinvolte godano pienamente del diritto a un ricorso effettivo e a un giudice imparziale, della presunzione di innocenza e dei diritti della difesa, compreso il diritto di essere sentiti e il diritto di accedere al fascicolo, in conformità con la Carta dei diritti fondamentali dell’Unione europea.
2. Se l’identità della persona coinvolta non è nota al pubblico, le autorità competenti provvedono a che sia **tutelata fintanto che sono in corso gli accertamenti.**
3. Le procedure di cui agli articoli 9 e 11 si applicano anche alla tutela dell’identità della persona coinvolta.


COMMISSIONE EUROPEA

Bruxelles, 23.4.2018
COM(2018) 218 final
2018/0106 (COD)

Proposta di

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione

{SEC(2018) 198 final} - {SWD(2018) 116 final} - {SWD(2018) 117 final}

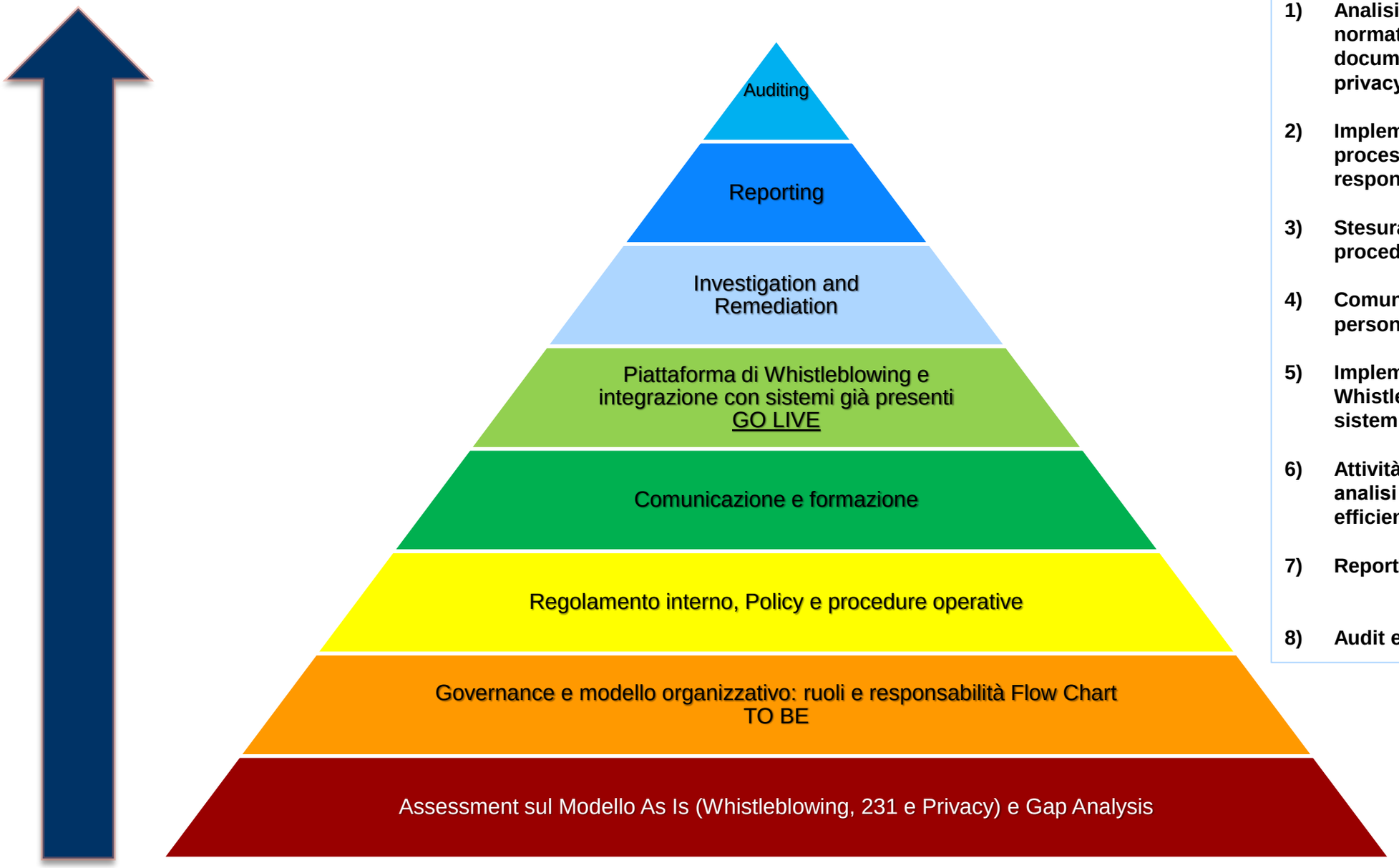
IT IT

- un termine ragionevole, non superiore a **tre mesi o sei mesi** in casi debitamente giustificati, per dare **un riscontro alla persona segnalata**
- il regime di ri**servatezza applicabile alle segnalazioni**, in particolare alle informazioni relative al trattamento dei dati personali conformemente all’articolo 13 del regolamento (UE) 2016/679 (informativa)
- Gli Stati membri provvedono affinché le autorità competenti **conservino** la documentazione inerente a ogni segnalazione ricevuta (… anche registrazioni delle conversazioni o verbalizzazioni).

6.

Le fasi di progetto del Whistleblowing

LE PRINCIPALI FASI



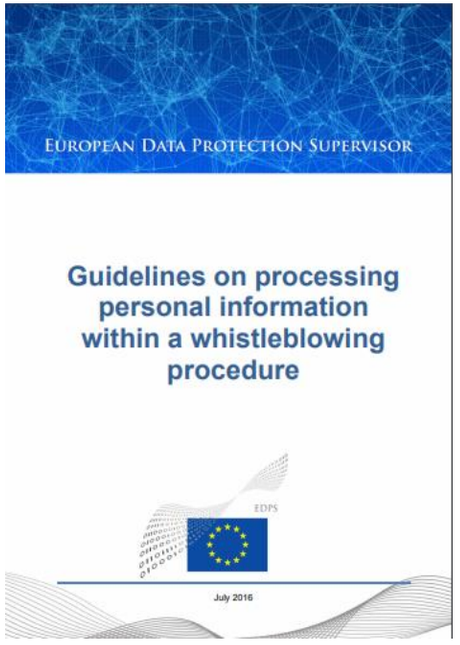
1) **Analisi volta ad individuare i gap normativi e procedurali, analisi documentale (modello 231/2001, privacy,…);**
2) **Implementazione del flusso di processo, definizione dei ruoli e delle responsabilità;**
3) **Stesura ed implementazione delle procedure operative;**
4) **Comunicazione delle procedure al personale e formazione;**
5) **Implementazione della piattaforma di Whistleblowing ed integrazione con i sistemi IT/ Security già presenti;**
6) **Attività di Remediation ed ulteriore analisi volta a verificare l'efficacia ed efficienza del modello;**
7) **Reporting e deliverable finale;**
8) **Audit e monitoraggio del modello**

MAZARS

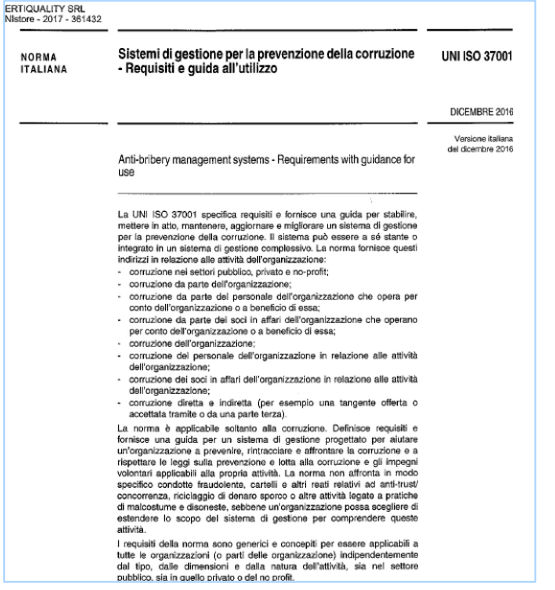
FRAMEWORK GENERALE

Approccio al whistleblowing: si suggerisce di definire un Modello specifico basato non solo sulle normative vigenti ma anche su standard riconosciuti INTERNAZIONALMENTE.

- **ISO 37001** (dicembre 2016): Sistema di gestione per la prevenzione della corruzione
- WP 117, EDPS, Dlgs. 101
- Legge 190 e Legge 179
- Altre normative di settore (es: Circ. BI 285 per il settore bancario, ecc.)



- Il modello creato da Mazars Italia si adatta a tutte le dimensioni aziendali, piccole medie e grandi.
- La stretta collaborazione con Unione Fiduciaria ha permesso di sviluppare un approccio multidisciplinare e completo
- L'obiettivo è quello di creare e mantenere un efficace sistema di prevenzione dei rischi di corruzione e dei comportamenti illeciti in generale.


ERTIQUALITY SRL
Nistore - 2017 - 361432

NORMA ITALIANA

Sistemi di gestione per la prevenzione della corruzione - Requisiti e guida all'utilizzo

UNI ISO 37001

DICEMBRE 2016

Versione italiana del dicembre 2016

Anti-bribery management systems - Requirements with guidance for use

La UNI ISO 37001 specifica requisiti e fornisce una guida per stabilire, mettere in atto, mantenere, aggiornare e migliorare un sistema di gestione per la prevenzione della corruzione. Il sistema può essere a sé stante o integrato in un sistema di gestione complessivo. La norma fornisce questi indirizzi in relazione alle attività dell'organizzazione:

- corruzione nei settori pubblico, privato e no-profit;
- corruzione da parte dell'organizzazione;
- corruzione da parte del personale dell'organizzazione che opera per conto dell'organizzazione o a beneficio di essa;
- corruzione da parte dei soci in affari dell'organizzazione che operano per conto dell'organizzazione o a beneficio di essa;
- corruzione dell'organizzazione;
- corruzione del personale dell'organizzazione in relazione alle attività dell'organizzazione;
- corruzione dei soci in affari dell'organizzazione in relazione alle attività dell'organizzazione;
- corruzione diretta e indiretta (per esempio una tangente offerta o accettata tramite o da una parte terza).

La norma è applicabile soltanto alla corruzione. Definisce requisiti e fornisce una guida per un sistema di gestione progettato per aiutare un'organizzazione a prevenire, rintracciare e affrontare la corruzione e a rispettare le leggi sulla prevenzione e lotta alla corruzione e gli impegni volontari applicabili alla propria attività. La norma non affronta in modo specifico condotte fraudolenta, cartelli e altri reati relativi ad anti-trust/ concorrenza, riciclaggio di denaro sporco o altre attività legate a pratiche di malcostume e disoneste, sebbene un'organizzazione possa scegliere di estendere lo scopo del sistema di gestione per comprendere queste attività.

I requisiti della norma sono generici e concepiti per essere applicabili a tutte le organizzazioni (o parti delle organizzazione) indipendentemente dal tipo, dalle dimensioni e dalla natura dell'attività, sia nel settore pubblico, sia in quello privato o del no profit.

MAZARS

LA ISO 37001

La norma (UNI) ISO 37001 è stata pubblicata in data 16 ottobre 2016. Analogamente a quanto accade per altre norme ISO sui sistemi di gestione (9001, 14001, 27001,…), la norma prevede i requisiti per pianificare, attuare, mantenere e riesaminare, in ottica di miglioramento, un sistema di gestione per la prevenzione della corruzione.

In sintesi, il Sistema ISO 37001, con approccio analogo a quello delle altre norme ISO (HLS), è articolato come segue:

- Comprensione del contesto (interno ed esterno);
- Identificazione, analisi e valutazione dei rischi;
- Programmazione delle misure e dei controlli in funzione della valutazione dei rischi;
- Leadership e coinvolgimento della direzione (politica, ruoli e responsabilità, compresa una funzione compliance per la prevenzione della corruzione);
- Risorse a supporto del sistema (consapevolezza e formazione, comunicazione interna ed esterna, informazioni documentate);
- Attuazione dei controlli per la prevenzione della corruzione;
- Sorveglianza sul sistema (compresi audit e riesame della direzione) e miglioramento continuo.

SISTEMA DI GESTIONE INTEGRATO

Un approccio integrato tra le diverse norme (BS PAS 99) evidenziano una serie di caratteristiche della gestione del rischio, creando e proteggendo il valore dell'organizzazione. Si vuole in questo modo evidenziare la componente di creazione del valore, accanto a quello della protezione del valore, come finalità di gestione del rischio in modo integrato.

Essa è parte integrante di tutti i processi dell'organizzazione, pertanto, proprio in virtù di una decisione da prendere, la gestione del rischio è parte del processo decisionale e deve necessariamente trattare esplicitamente dell'incertezza, essendo questa una caratteristica intrinseca della gestione del rischio, secondo una metodologia che riducano e tengano sotto controllo tale incertezza

PRINCIPALI DELIVERABLE

Di seguito sono elencati i documenti principali di un progetto Whistleblowing :

- Policy di Whistleblowing (cultura aziendale in riferimento al Whistleblowing e alla compliance);
- Procedura di Whistleblowing (ruoli, responsabilità, attività, diritti di accesso, flow chart, ecc.);
- Procedura di Whistleblowing specifica per le investigazioni (in base al reato) e in compliance con la Privacy;
- Informative ai dipendenti e agli utilizzatori della procedura Whistleblowing;
- Procedura per l'utilizzo del Tool (manuale d'uso);
- Retention Policy (per tipologia di reato/illecito);
- In caso di esternalizzazione: clausola «specifica» e nomina a Resp. Esterno (nel caso di responsabile interno – nomina da «referente privacy» specifica);
- Piano di remediation (controlli aggiuntivi del sistema di controllo interno);
- Piano di Formazione e relativa documentazione.

CONTATTI

Mazars Italia Spa
Largo Augusto 8
20122 Milano
Tel: +39 02 32169300
www.mazars.it

Luca Savoia

Partner

Mobile: +39 348 8217339
Email: luca.savoia@mazars.it