ORDINE DEGLI INGEGNERI DI BERGAMO

16/04/2024

Quadro normativo e regolamentare

La normativa di riferimento

Con la Legge del 6 novembre 2012, n. 190 (c.d. Legge Severino), l'Italia ha introdotto nel proprio ordinamento norme a tutela della persona che segnala condotte illecite (attività c.d. ***whistleblowing***).

La Legge 190/2012 integra il Testo Unico del pubblico impiego (D.Lgs. 30 marzo 2001, n. 165) con l'articolo 54-bis, in base al quale: "*…il dipendente che denuncia all'autorità giudiziaria o alla Corte dei conti, ovvero riferisce al proprio superiore gerarchico condotte illecite di cui è venuto a conoscenza in ragione del rapporto di lavoro, non può essere sanzionato, licenziato o sottoposto ad una misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia*".

Il D.lgs. 24/2023, attuativo della Direttiva UE 2019/1937, in vigore dal 15 luglio 2023, raccoglie in un unico testo normativo l'intera disciplina dei canali di segnalazione e delle tutele riconosciute ai segnalanti sia del settore pubblico che privato.
Con particolare riferimento , il D.lgs. 24/2023:

- ha ampliato la possibilità di segnalare condotte illecite sia da parte dei dipendenti, sia dei privati;
- fornisce una maggiore tutela della persona che segnala condotte illecite (il c.d. *whistleblower*), tramite apposite misure di sostegno volte alla limitazione della responsabilità, alla protezione dalle ritorsioni e alla tutela della riservatezza.

Con Delibera n. 311 del 12 luglio 2023 ANAC ha adottato le «***Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne***»

Le tipologie di segnalazione

COMPORTAMENTI, ATTI O OMISSIONI CHE LEDONO L'INTERESSE PUBBLICO O L'INTEGRITÀ DELL'AMMINISTRAZIONE PUBBLICA O DELL'ENTE PRIVATO

- illeciti **amministrativi**, **contabili**, **civili** o **penali**;
- **condotte illecite** rilevanti ai sensi del **decreto legislativo 231/2001**, o **violazioni dei modelli** di organizzazione e gestione ivi previsti;
- Illeciti che rientrano nell'ambito di applicazione degli **atti dell'Unione europea** o **nazionali** relativi ai seguenti settori:
  - **appalti pubblici**;
  - **servizi**, **prodotti** e **mercati finanziari** e prevenzione del **riciclaggio** e del finanziamento del **terrorismo**;
  - **sicurezza** e **conformità** dei **prodotti**; **sicurezza** dei **trasporti**; tutela dell'**ambiente**;
  - **radioprotezione** e **sicurezza nucleare**;
  - sicurezza degli **alimenti** e dei **mangimi** e **salute** e **benessere** degli **animali**;
  - **salute pubblica**;
  - **protezione** dei **consumatori**;
  - tutela della **vita privata** e **protezione** dei **dati personali** e **sicurezza** delle **reti** e dei **sistemi informativi**.
- atti o omissioni che **ledono** gli **interessi finanziari** dell'Unione;
- atti o omissioni riguardanti il **mercato interno**;
- atti o comportamenti che **vanificano** l'**oggetto** o la **finalità** delle **disposizioni** di cui agli atti dell'**Unione**.

Le tutele per i whistleblowers

GLI AUTORI DELLE SEGNALAZIONI NON POSSONO SUBIRE RITORSIONI DI ALCUN TIPO

Esempi di comportamenti ritorsivi:

- il **licenziamento**, la **sospensione**;
- la **retrocessione di grado** o la **mancata promozione**;
- il **mutamento** di funzioni, il **cambiamento** del luogo di lavoro, la **riduzione** dello stipendio, la **modifica** dell'orario di lavoro;
- la **sospensione** della formazione;
- le **note di merito negative**;
- l'adozione di **misure disciplinari** o di altra **sanzione** anche pecuniaria;
- la **coercizione**, l'**intimidazione**, le **molestie** o l'**ostracismo**;
- la **discriminazione** o comunque il **trattamento sfavorevole**;
- la **mancata conversione** di un contratto di lavoro a termine in un contratto di lavoro a **tempo indeterminato**, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- il **mancato rinnovo** o la **risoluzione anticipata** di un contratto di lavoro a termine;
- i danni, anche alla **reputazione della persona**, in particolare sui social media, o i **pregiudizi economici** o **finanziari**, comprese la **perdita di opportunità economiche** e la **perdita di redditi**;
- l'annullamento di una **licenza** o di un **permesso**;
- la richiesta di **sottoposizione ad accertamenti** psichiatrici o medici.

Ambito di applicazione

- Soggetti pubblici
- Soggetti privati con almeno 50 lavoratori subordinati
- Soggetti operanti nei settori dei servizi, prodotti e mercati finanziari, prevenzione del riciclaggio e del finanziamento del terrorismo, nonché sicurezza dei trasporti
- Soggetti dotati di un modello 231

Riferimenti per il calcolo dei dipendenti secondo ANAC

- Per il calcolo della ***media dipendenti*** si deve fare riferimento al valore medio degli addetti (elaborazione dati INPS) al 31/12 dell'anno solare precedente a quello in corso, contenuto nelle visure camerali
- Quando l'impresa è di ***nuova costituzione***, considerato che il dato viene aggiornato trimestralmente, va preso come riferimento il valore medio calcolato nell'ultima visura

Le modalità di segnalazione

2 MODALITÀ DI SEGNALAZIONE

SCRITTA

anche con modalità informatiche (piattaforma online)

ORALE

alternativamente attraverso linee telefoniche, con sistemi di messaggistica vocale o incontro diretto (su richiesta)

In ogni caso deve essere garantita la riservatezza e la protezione dei dati personali.

4 CANALI DI SEGNALAZIONE

- ***CANALI INTERNI NEGLI ENTI PUBBLICI E PRIVATI***
- ***CANALE ESTERNO PRESSO ANAC***
- ***DIVULGAZIONE PUBBLICA (STAMPA, MEZZI ELETTRONICI O ALTRI MEZZI DI DIFFUSIONE)***
- ***DENUNCIA ALL'AUTORITÀ GIUDIZIARIA O CONTABILE***

Informazione rappresentanze sindacali e Regolamento

I soggetti del settore pubblico e del settore privato:

a. **sentite le rappresentanze** o le organizzazioni sindacali, per acquisire **eventuali osservazioni**,
b. definiscono in un **apposito atto organizzativo le procedure** per il ricevimento delle segnalazioni e per la loro gestione, al fine di attivare al proprio interno appositi canali di segnalazione. Nell'atto organizzativo, adottato dall'organo di indirizzo, è opportuno che almeno vengano definiti:

    - il ruolo e i compiti dei soggetti che gestiscono le segnalazioni;

    - le modalità e i termini di conservazione dei dati, appropriati e proporzionati in relazione alla procedura di whistleblowing e alle disposizioni di legge.

Aspetti privacy previsti dalla normativa whistleblowing

Chi sono i soggetti interessati al trattamento del processo?

Segnalatori: **candidati** (se le violazioni sono avvenute durante la selezione e in altri fasi precontrattuali), **lavoratori in forza oppure dimessi** (se le violazioni sono state acquisite durante lo svolgimento della mansione), consulenti, collaboratori, volontari, tirocinanti, azionisti degli stessi soggetti pubblici e privati, ove assumano la forma societaria, persone con funzione di amministrazione, direzione, controllo, vigilanza o rappresentanza

Facilitatori

Segnalati: persona coinvolta o comunque dei soggetti menzionati nella segnalazione

Quali tutele privacy devono essere assicurate?

REQUISITI DI LEGGE
Adempiere agli obblighi informativi
Raccogliere i dati al solo fine di gestire e dare seguito alle segnalazioni, divulgazioni pubbliche o denunce
Assicurare che i dati siano esatti e aggiornati
Conservare i dati per il tempo necessario al trattamento della specifica segnalazione.
Non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione
Effettuare il trattamento in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità, disponibilità e riservatezza»). Nel contesto in esame, caratterizzato da elevati rischi per i diritti e le libertà degli interessati, il ricorso a strumenti di crittografia nell'ambito dei canali interni e del canale esterno di segnalazione, è di regola da ritenersi una misura adeguata a dare attuazione, fin dalla progettazione e per impostazione predefinita, al predetto principio di integrità e riservatezza. Le misure di sicurezza adottate devono, comunque, essere periodicamente riesaminate e aggiornate
Garantire il divieto di tracciamento dei canali di segnalazione
Nel caso in cui l'accesso ai canali interni e al canale esterno di segnalazione avvenga dalla rete dati interna del soggetto obbligato e sia mediato da dispositivi firewall o proxy, deve essere garantita la non tracciabilità – sia sulla piattaforma informatica che negli apparati di rete eventualmente coinvolti nella trasmissione o monitoraggio delle comunicazioni - del segnalante nel momento in cui viene stabilita la connessione a tali canali.
Garantire, ove possibile, il tracciamento dell'attività del personale autorizzato nel rispetto delle garanzie a tutela del segnalante, al fine di evitare l'uso improprio di dati relativi alla segnalazione. Deve essere evitato il tracciamento di qualunque informazione che possa ricondurre all'identità o all'attività del segnalante. **Spetta comunque al titolare del trattamento alla luce del principio di responsabilizzazione, individuare le misure di sicurezza idonee alla luce del rischio in concreto.**

L'Informativa privacy nell'ambito delle Procedure di Whistleblowing

Cosa stabilisce l'ANAC?

Rendere *ex ante* ai possibili interessati un'**informativa sul trattamento dei dati personali** mediante la pubblicazione di documenti informativi (ad es. sul sito web, sulla piattaforma, oppure informative brevi in occasione dell'uso di altre modalità scritte o orali)

Laddove all'esito dell'istruttoria sulla segnalazione si avvii un **procedimento** nei confronti di uno specifico soggetto segnalato, a quest'ultimo va naturalmente resa un'informativa ad hoc.

Quali contenuti?

- **QUALI DATI PERSONALI RACCOGLIAMO? DA CHI ACQUISIAMO TALI DATI?**
- **QUALI SONO LE FINALITÀ CHE RENDONO NECESSARIO IL TRATTAMENTO DEI DATI?**
- **QUALI SONO I PRESUPPOSTI GIURIDICI CHE RENDONO LECITO IL TRATTAMENTO DEI DATI?**

Quali contenuti?

- **È OBBLIGATORIO CONFERIRE I DATI RICHIESTI e PRESTARE IL CONSENSO ALLA PROPRIA IDENTIFICAZIONE?**
- **PER QUANTO TEMPO L'ORGANIZZAZIONE CONSERVERÀ I DATI?**
- **QUALI DIRITTI IN MATERIA DI PRIVACY POSSIEDE L'INTERESSATO?**

Per esercitare i propri diritti l'interessato può straordinariamente rivolgersi direttamente al RPCT (Responsabile della Prevenzione della Corruzione e della Trasparenza) o all'OdV.

All'occorrenza, restano in ogni caso attivi i contatti del DPO (Data Protection Officer) pubblicati sull'informativa istituzionale.

Quali sono i presupposti giuridici?

- Il trattamento dei dati è effettuato, **senza consenso espresso dell'interessato**, sulla base dei seguenti presupposti giuridici:
  - Il trattamento è necessario ad adempiere a quanto previsto dal D.lgs. 10 marzo 2023, n. 24 (art. 6 c. I lett. c) e art. 10 del Reg. UE 2016/679);
  - Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui sono investiti i titolari del trattamento (art. 6 c. I lett. e) del Reg. UE 2016/679).
- Qualora la contestazione disciplinare che ricade sul segnalato sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante e risulti indispensabile per la difesa dell'incolpato, si stabilisce che la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del **consenso espresso** della persona segnalante alla **rivelazione della propria identità** (art. 6 c. I lett. a) del Reg. 2016/679 e art. 1 c. III della L. 179/2017).

Criteri per ammissibilità della segnalazione

COMPORTAMENTI, ATTI O OMISSIONI DI CUI IL SEGNALANTE O IL DENUNCIANTE SIA VENUTO A CONOSCENZA NEL CONTESTO LAVORATIVO PUBBLICO O PRIVATO

CIRCOSTANZE DI TEMPO E DI LUOGO IN CUI SI È VERIFICATO IL FATTO OGGETTO DELLA SEGNALAZIONE

ACCURATA **DESCRIZIONE DEL FATTO**

GENERALITÀ O ALTRI ELEMENTI CHE CONSENTONO DI **IDENTIFICARE** IL SOGGETTO CUI ATTRIBUIRE I FATTI SEGNALATI

DOCUMENTI CHE POSSONO FORNIRE ELEMENTI DI FONDATEZZA DEI FATTI OGGETTO DI SEGNALAZIONE, NONCHÉ L'**INDICAZIONE DI ALTRI SOGGETTI** POTENZIALMENTE A CONOSCENZA DEI FATTI. OVE QUANTO SEGNALATO NON SIA ADEGUATAMENTE CIRCOSTANZIATO, CHI GESTISCE LE SEGNALAZIONI PUÒ CHIEDERE ELEMENTI INTEGRATIVI AL SEGNALANTE TRAMITE IL CANALE A CIÒ DEDICATO O ANCHE DI PERSONA, OVE IL SEGNALANTE ABBIA RICHIESTO UN INCONTRO DIRETTO

Raccogliere i dati al solo fine di gestire e dare seguito alle segnalazioni, divulgazioni pubbliche o denunce

- È essenziale avere un modello di riferimento per le **domande**
- Agevolare il **dialogo** con il segnalatore, la rettifica e l'aggiornamento

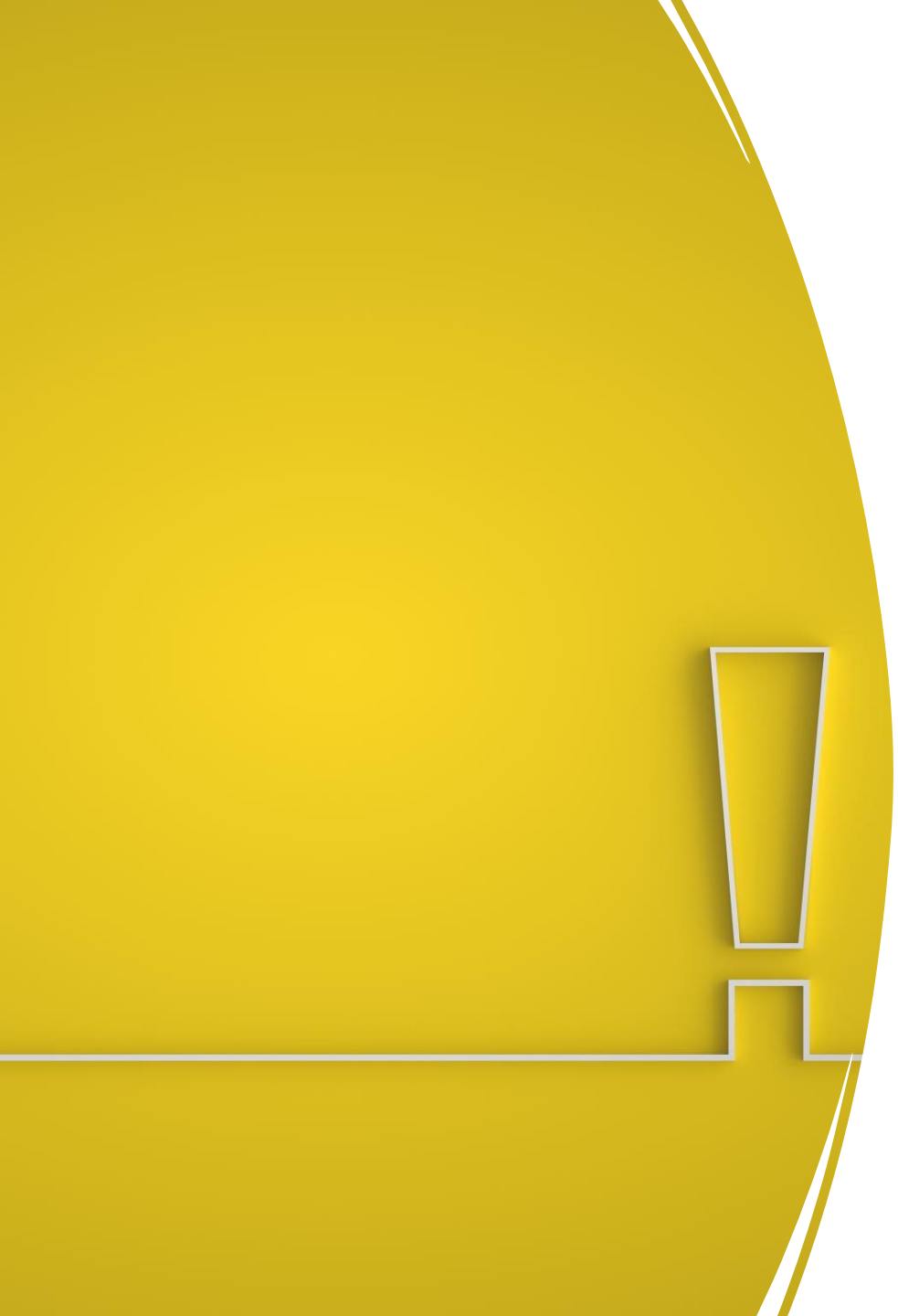
Minimizzazione del trattamento ed esattezza

Garantire che i **dati siano adeguati, pertinenti e limitati a quanto necessario** rispetto alle finalità per le quali sono trattati *(«minimizzazione dei dati»).* A tal riguardo, il decreto precisa, infatti, che i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati senza indugio.

Assicurare che i **dati siano esatti e**, se necessario, **aggiornati**; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti relativi alla specifica segnalazione, divulgazione pubblica o denuncia che viene gestita («esattezza»).

Conservare i dati in una forma che consenta l'**identificazione degli interessati** per il tempo necessario al trattamento della specifica segnalazione e comunque non oltre **cinque anni** a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione *(«limitazione della conservazione»).* Per ANAC, tale termine decorre dalla chiusura del fascicolo sulla segnalazione da parte dell'ufficio UWHIB.

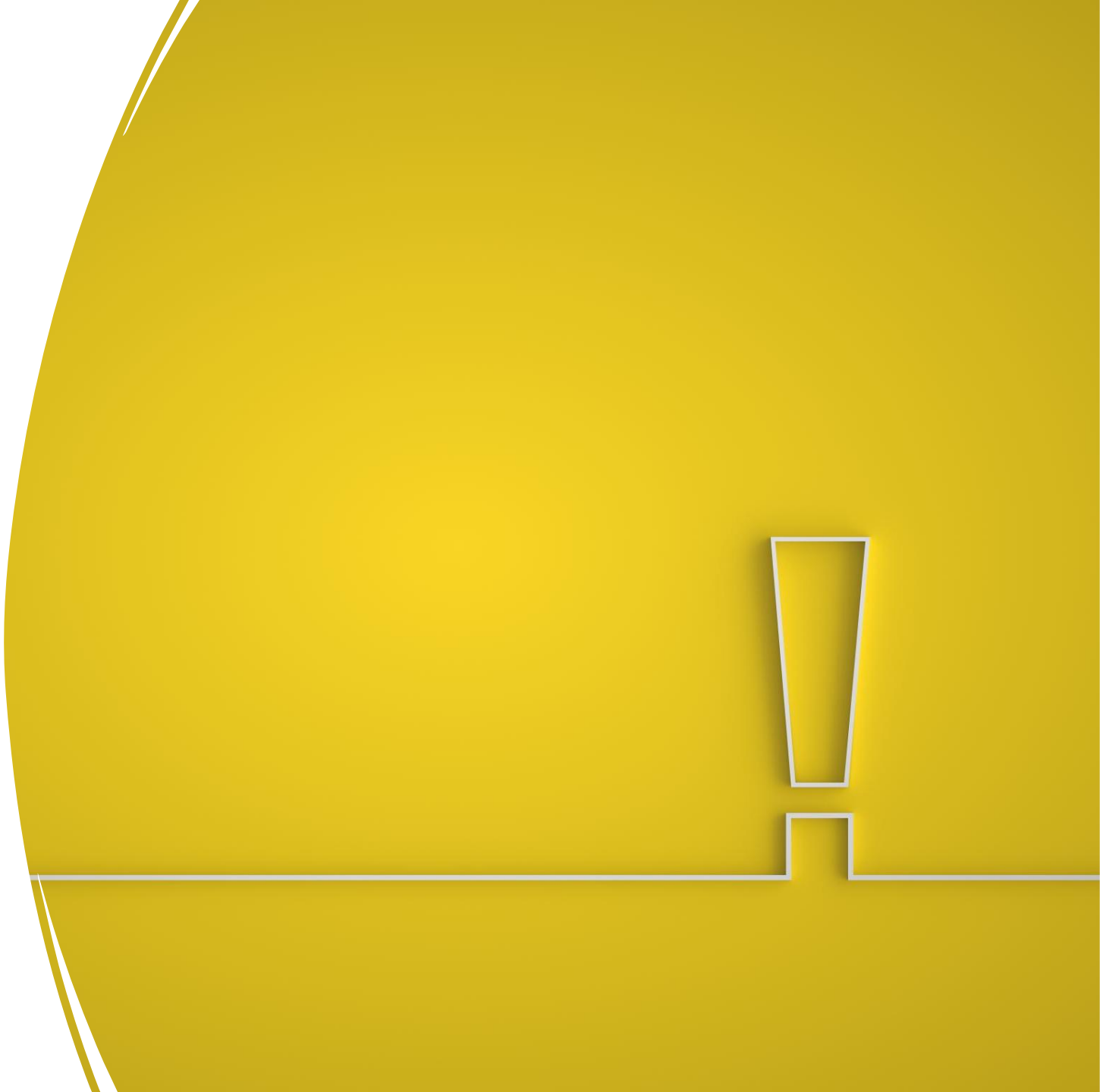
Gestione segnalazioni anonime



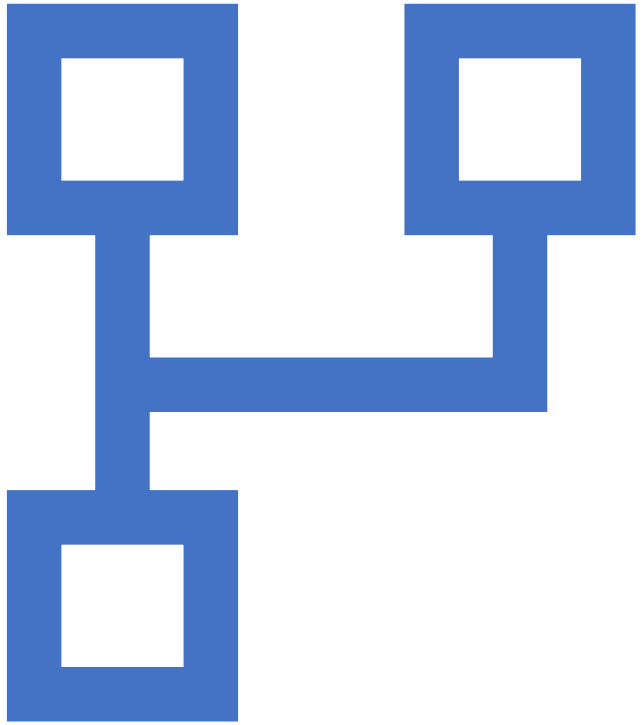
- In ogni caso, il segnalante o il denunciante anonimo, successivamente identificato, che ha comunicato ad ANAC di aver subito ritorsioni può beneficiare della **tutela** che il decreto garantisce a fronte di misure ritorsive.
- Gli enti del settore pubblico o privato che ricevono le segnalazioni attraverso canali interni e la stessa Autorità sono, quindi, tenuti a registrare le **segnalazioni anonime** ricevute e conservare la relativa documentazione secondo i criteri generali di conservazione degli atti applicabili nei rispettivi ordinamenti rendendo così possibile rintracciarle, nel caso in cui il segnalante, o chi abbia sporto denuncia, comunichi ad ANAC di aver subito **misure ritorsive** a causa di quella segnalazione o denuncia anonima.

Gestione segnalazioni anonime

- Le segnalazioni dalle quali non è possibile ricavare l'identità del segnalante sono considerate **anonime**. Le segnalazioni anonime, ove circostanziate, sono equiparate da ANAC a **segnalazioni ordinarie** e trattate consequenzialmente in conformità a quanto previsto nei Regolamenti di vigilanza.
- I soggetti del settore pubblico e del settore privato considerano le **segnalazioni anonime** ricevute attraverso i **canali interni** alla stregua di **segnalazioni ordinarie**, laddove ne sia prevista la trattazione. In tali casi quindi le segnalazioni anonime saranno gestite secondo i criteri stabiliti, nei rispettivi ordinamenti, per le segnalazioni ordinarie.



Fornitori e figure incaricate: come definirne gli accordi



Definire ruoli e responsabilità

RUOLO IN AZIENDA	FUNZIONE PRIVACY	EVIDENZE
AZIENDA/ENTE/ANAC	TITOLARE DEL TRATTAMENTO	
GLI ENTI CHE CONDIVIDONO IL CANALE INTERNO PER LA RICEZIONE E LA GESTIONE DELLE SEGNALAZIONI	CONTITOLARI DEL TRATTAMENTO	Accordo giuridico ex art. 26 del Reg. UE 2016/679
TUTTE LE PERSONE CHE SONO COINVOLTE NELLA GESTIONE DELLE SEGNALAZIONI (SI PENSI AL CASO IN CUI ERRONEAMENTE LA SEGNALAZIONE INVECE DI PERVENIRE ATTRAVERSO IL CANALE INTERNO PERVENGA TRAMITE PROTOCOLLO).	AUTORIZZATI AL TRATTAMENTO	Lettera di autorizzazione al trattamento Formazione + istruzioni privacy
SOGGETTO ESTERNO AUTONOMO CHE GESTISCE LE SEGNALAZIONI	RESPONSABILE DEL TRATTAMENTO	Accordo giuridico ex art. 28 del Reg. UE 2016/679
SOGGETTO ESTERNO CHE GESTISCE CANALE DI SEGNALAZIONE	RESPONSABILE DEL TRATATMENTO	Accordo giuridico ex art. 28 del Reg. UE 2016/679

Nel caso la segnalazione arrivi a persona diversa

Se la segnalazione è considerata **“segnalazione whistleblowing”** va trasmessa, entro sette giorni dal suo ricevimento, al **soggetto interno competente**, dandone contestuale notizia della trasmissione alla **persona segnalante**.

Responsabile della gestione delle segnalazioni

- È **affidata**, alternativamente:
  - a una persona interna all'amministrazione/ente;
  - a un ufficio dell'amministrazione/ente con personale dedicato, anche se non in via esclusiva;
  - a un soggetto esterno.
- Si deve trattare di **soggetti autonomi**, requisito che per ANAC va declinato come **imparzialità** e **indipendenza**.
- Negli **enti del settore pubblico** la gestione è affidata al RPCT, ove tenuti a nominarlo.
- Negli **enti del settore privato** la scelta è rimessa all'autonomia organizzativa di ciascun ente.

Tale figura dovrà essere a**utorizzata al trattamento dei dati personali** e dovranno esserle fornite **specifiche istruzioni** per assicurare la tutela dei dati stessi ex art. 29 del Reg. UE 2016/679

Funzioni principali

rilascia alla persona segnalante un **avviso di ricevimento** della segnalazione entro **sette giorni** dalla data di ricezione

mantiene le **interlocuzioni** con la persona segnalante

dà un corretto **seguito** alle segnalazioni ricevute

fornisce un **riscontro** alla persona segnalante

DPIA: rischi e misure di sicurezza da valutare per un’efficace redazione

Dalle misure minime alle misure idonee

Il Regolamento Europeo chiede alle organizzazioni di stabilire **misure IDONEE** a tutela e sicurezza delle banche dati.

Il regolamento non stabilisce un elenco di misure minime di sicurezza, ma affida alle organizzazioni la responsabilità di identificare **opportune cautele in funzione dei propri rischi**.

Come determinare misure idonee

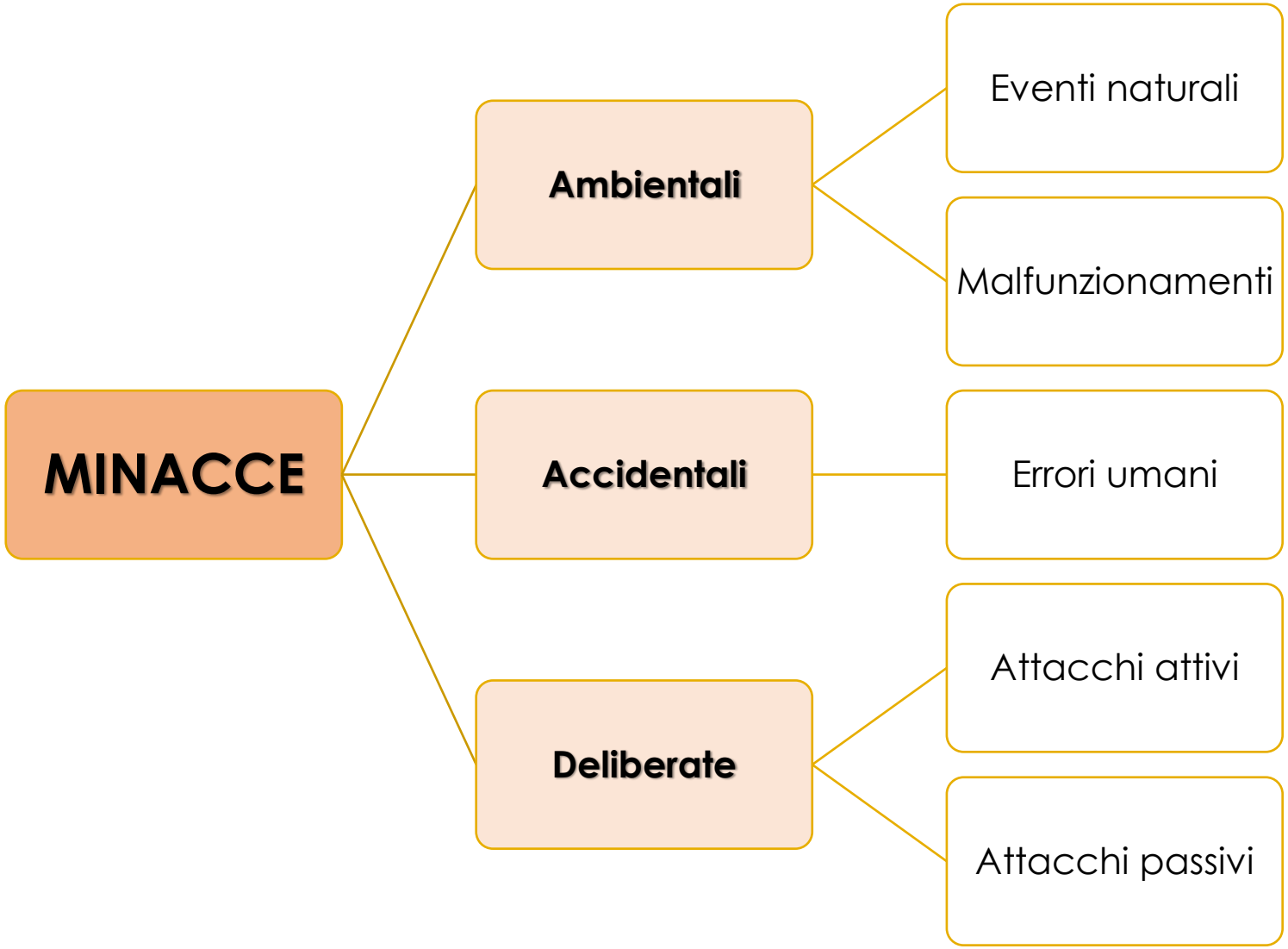
Le **misure** dunque devono tenere conto:

a) Dello stato dell'arte dell'organizzazione;
b) Dei costi di attuazione;
c) Della natura, oggetto, contesto e finalità di trattamento;
d) Probabilità e gravità del rischio per i diritti e le libertà delle persone fisiche

Le **misure** possono essere:

- Tecniche
- Organizzative

Minacce


MINACCE
Ambientali
Accidentali
Deliberate
Eventi naturali
Malfunzionamenti
Errori umani
Attacchi attivi
Attacchi passivi

Le misure tecniche e generali per la mitigazione dei rischi art. 32 REG. UE

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

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

Cosa è il rischio?

COSA SI INTENDE PER RISCHIO?

Per **rischio** si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di **gravità** e **probabilità**.

Quando esiste la probabilità di un rischio elevato, per l'art.35 del regolamento?

Nel momento in cui il trattamento «*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*»

La "**gestione del rischio**" è definibile come l'**insieme coordinato delle attività finalizzate** a guidare e monitorare un ente o organismo nei riguardi di tale rischio.

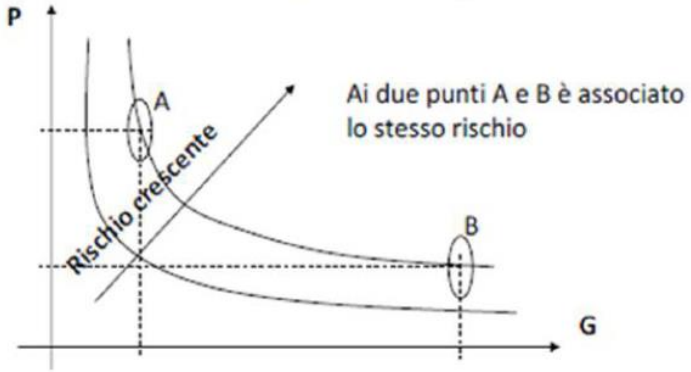
Analizzare i rischi

RISCHIO

Impatto sul business dell'evento indesiderabile X probabilità di accadimento

R = G x P

Le curve a pari Livello di Rischio sono quindi delle **iperboli equilatere**



Analizzare i rischi

In un modello più sofisticato i valori di occorrenza e impatto non sono valutati direttamente ma vengono a loro volta calcolati mediante un modello che tiene conto di ulteriori fattori

Occorrenza

la concretezza della minaccia e il grado di vulnerabilità del sistema (in altre parole probabilità o frequenza che tale minaccia possa fruttare la vulnerabilità)

Occorrenza = Minaccia × Vulnerabilità

Impatto

valore dei beni coinvolti e gravità delle conseguenze dell'incidente sul bene

Impatto = ValoreBeni × Conseguenze

Analizzare i rischi

Analizzare i rischi

In che modo quantificare il rischio?

Esposizione = probabilità x danno

- **probabilità di accadimento della minaccia rilevata** (la probabilità è legata anche all'esistenza o meno di strumenti di controllo/regole atti a prevenire il verificarsi della minaccia rilevata)

- danno inteso come danno materiali o immateriale all'interessato derivante dal verificarsi dell'evento considerato a rischio.

probabilità	**alta (3)**	**3**	**6**	**9**
	media (2)	2	4	6
	bassa (1)	1	2	3
		minimo (1)	medio (2)	significativo(3)
		danno		

- **Significativo -> Azione urgente**
- **Medio -> Azione richiesta**
- **Minimo -> Monitoraggio**

La valutazione d'impatto secondo le Linee Guida ENISA

LIVELLO DI IMPATTO	DESCRIZIONE
Basso	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
Medio	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
Alto	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
Molto alto	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

I 5 possibili rischi

Le cautele da adottare variano in funzione delle Modalità

in **forma scritta**, anche con modalità informatiche (piattaforma online)

in **forma orale**, alternativamente attraverso linee telefoniche, con sistemi di messaggistica vocale o incontro diretto (su richiesta)

Istituzione del canale interno

Soggetti del settore pubblico: Definizione con atto organizzativo sentite le rappresentanze o le organizzazioni sindacali di cui all'art. 51 del D.lgs. n. 81/2015

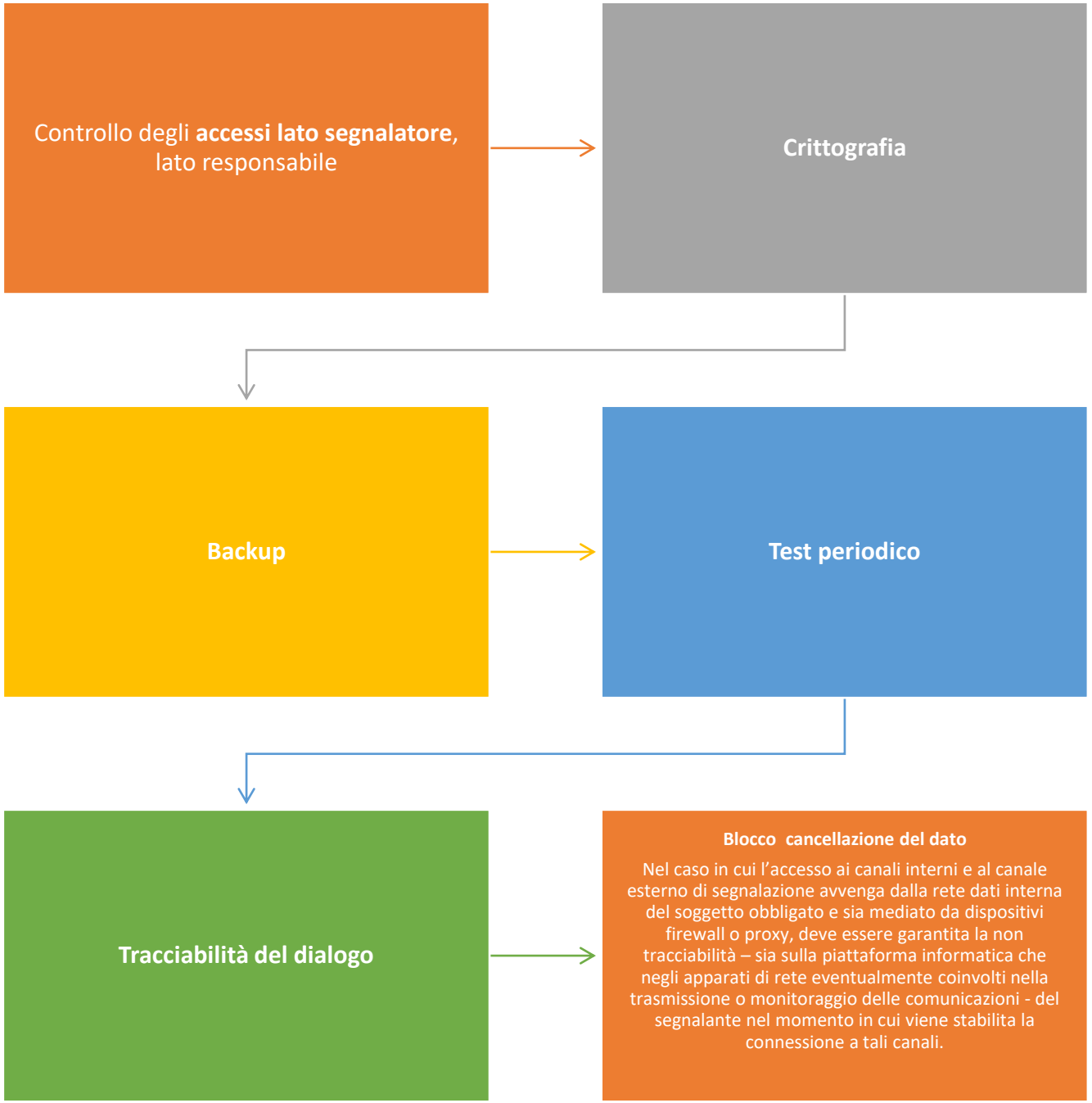
Soggetti del settore privato: Definizione all'interno del MOG 231 o con atto organizzativo cui il MOG 231 rinvia sentite le rappresentanze o le organizzazioni di cui all'art. 51 del D.lgs. n. 81/2015

Canale cartaceo

- Autorizzare **chi riceve**
- Individuare i **punti di ricezione** e verificare le **misure di controllo degli accessi**
- Individuare i **punti di conservazione** e verificare le **misure di limitazione degli accessi e impatto ambientale**
- Individuare **modalità sicure per l'imbustamento**:

Ad esempio, a tal fine ed in vista della protocollazione riservata della segnalazione a cura del gestore, è necessario che la segnalazione venga inserita in due buste chiuse: la prima con i dati identificativi del segnalante unitamente alla fotocopia del documento di riconoscimento; la seconda con la segnalazione, in modo da separare i dati identificativi del segnalante dalla segnalazione. Entrambe dovranno poi essere inserite in una terza busta chiusa che rechi all'esterno la dicitura "riservata" al gestore della segnalazione (ad es. "riservata al RPCT"). La segnalazione è poi oggetto di protocollazione riservata, anche mediante autonomo registro, da parte del gestore.

Canale digitale



Altre misure

- L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale **identità** non possono essere rivelate senza il **consenso espresso** della stessa persona segnalante a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni

Come è garantita la riservatezza del segnalante nell'ambito giurisdizionale?

- Nell'ambito del procedimento penale, l'identità del segnalante è coperta dal **segreto** nei modi e nei limiti previsti dall'articolo 329 c.p.p.
- Nell'ambito del procedimento dinanzi alla Corte dei conti, l'identità della persona segnalante non può essere rivelata fino alla **chiusura della fase istruttoria**

Altre misure

- Nell'ambito del procedimento disciplinare, l'**identità della persona segnalante non può essere rivelata**, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia **indispensabile** per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del **consenso espresso** della persona segnalante alla rivelazione della propria identità.

Altre misure

- Definire un modello di gestione delle segnalazioni in conformità ai **principi di protezione dei dati personali**.
- In particolare, tali misure devono fare in modo che **non siano resi accessibili**, in via automatica senza il tramite del titolare del trattamento o soggetto autorizzato, dati personali a un numero indefinito di soggetti.

Aggiornamento registro dei trattamenti

È necessario aggiornare descrivendo:

- *finalità*
- *tempi di conservazione*
- *attori coinvolti*
- *punti di archiviazione*
- *trasferimento verso paesi terzi*

Data retantion

- Le segnalazioni interne e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui alla normativa europea e nazionale in materia di protezione di dati personali.

I principali diritti dell'interessato

- ACCESSO
- OPPOSIZIONE
- CANCELLAZIONE
- LIMITAZIONE
- RETTIFICA
- PORTABILITA'

Aspetti sanzionatori

Aspetti sanzionatori

•da 10.000 a 50.000 euro quando accerta che sono state commesse ritorsioni o quando accerta che la segnalazione è stata ostacolata o che si è tentato di ostacolarla o che è stato violato l'obbligo di riservatezza;

•da 10.000 a 50.000 euro quando accerta che non sono stati istituiti canali di segnalazione, che non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni ovvero che l'adozione di tali procedure non è conforme a quella richiesta dalla legge, nonché quando accerta che non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute;

•da 500 a 2.500 euro, nel caso di perdita delle tutele, salvo che la persona segnalante sia stata condannata, anche in primo grado, per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile.

CASE STUDY

La piattaforma Globaleaks

Il whistleblowing può sicuro e semplice

Tutti possono facilmente avviare una iniziativa di whistleblowing sicuro e anonimo. Progettato per essere semplice da utilizzarsi il software è personalizzabile per ogni necessità a protegge la privacy dei segnalanti e delle loro segnalazioni di default.

Molti casi d'uso, un solo framework

GlobaLeaks vuole soddisfare una ampia varietà di casi d'uso ed è quindi stato progettato come un framework. Con alla base la flessibilità, GlobaLeaks è oggi usato nel mondo da più di 10000 progetti. Questo alto numero di adozioni include testate indipendenti, attivisti, pubbliche amministrazioni, aziende e altro ancora. La piattaforma è conforme allo Standard ISO 37002, alla Direttiva EU 2019/1937 e al Regolamento Generale sulla Protezione dei Dati (GDPR).

La piattaforma Globaleaks

Open source, documentazione libera

GlobaLeaks (https://www.globaleaks.org/it/) è un software di whistleblowing libero ed open-source e utilizza la Licenza AGPL. E' supportato da una comunità aperta di utenti, volontari e contributori che lavorano costantemente insieme per migliorare il software e la sua documentazione. Se noti un problema, crea un ticket sul nostro Ticketing System e aiutaci a supportare la trasparenza in tutto il mondo!

Disponibile in ogni lingua

Fin dai primi sviluppi di GlobaLeaks avevamo idea che lo strumento di whistleblowing debba essere più vicino possibile ai cittadini e al loro contesto. Per questa ragione abbiamo concentrato la nostra ricerca sulle problematiche di internazionalizzazione e traduzione ed il software è ora piamente tradotto in oltre 60 lingue che includono il Chinese, lo Spagnolo, l'Arabo, il Francese, il Tedesco e altre grazie al supporto del Localization Lab e della sua community.

La piattaforma demo

https://wb.pwd-whistleblowing.it/#/

Le segnalazioni sulla piattaforma possono avvenire sia in **forma anonima**, sia con **identificazione del soggetto denunciante**, attuando tutte le tutele previste dalla norma (sia specifica in tema di whistleblowing, sia a tutela della privacy – GDPR).

La piattaforma demo

Italiano

Kato Whistleblowing

Con il decreto legislativo 10 marzo 2023, n. 24 il nostro Paese recepisce la Direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea di cui siano venuti a conoscenza in un contesto lavorativo pubblico o privato, illeciti che vadano a ledere l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato.

Kato ha aderito al progetto Whistleblowing per la Trasparenza e i Diritti Umani e Digitali e ha adottato la piattaforma informatica prevista per adempiere agli obblighi normativi e in quanto ritiene importante dotarsi di uno strumento sicuro per le segnalazioni.

Invia una segnalazione

Hai già effettuato una segnalazione? Inserisci la tua ricevuta.

Accedi

LA PIATTAFORMA PERMETTE DI:

Inviare una **nuova segnalazione** di illecito

Verificare lo **stato** di una **segnalazione già inviata**

La piattaforma demo

La piattaforma guida il whistleblower nell'esecuzione della segnalazione, richiedendo la compilazione di **sezioni** con **campi obbligatori e facoltativi.**

SEGNALAZIONE
Informazioni generiche sul segnalante e descrizione della segnalazione

ALTRI SOGGETTI INFORMATI
Informazioni su eventuali altri soggetti a cui è stata già effettuata la segnalazione di illecito

ALLEGATI
Possibilità di caricare file documentali o multimediali a sostegno della segnalazione

ULTERIORI INFORMAZIONI
Ulteriori informazioni riguardanti l'illecito

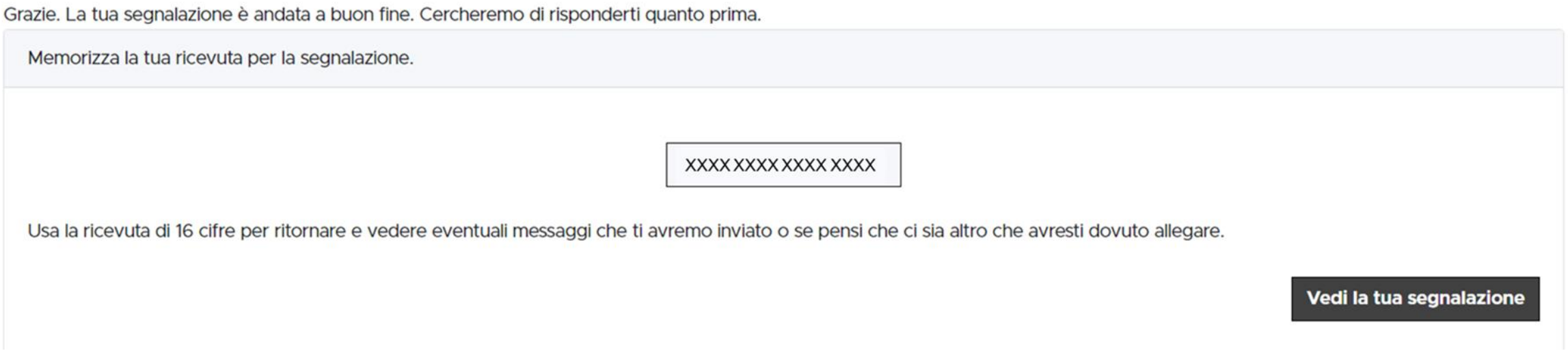
Possibile specificare Identità
Indicazione facoltativa dei dati identificativi e delle modalità di contatto

INVIA
Accettazione dei termini di servizio e invio della segnalazione

La piattaforma demo

Una volta inviata la segnalazione verrà generato un **codice identificativo** (Key Code) che può essere utilizzato dall'utente per monitorare lo stato della stessa.

Nel caso in cui l'utente abbia accettato di identificarsi, verrà contattato nella modalità da lui scelta.



La piattaforma demo

La sola piattaforma è sufficiente ?

- Autorizzazioni Interne
- Accordo Responsabile del Trattamento
- Accordo di Contitolarità (solo per i Gruppi di aziende)
- Informativa
- **Disciplinare Tecnico DPIA**
- Istruzioni operative per l'utilizzo della piattaforma da parte degli utenti.

SCAN ME


Questions
?
?
Answers
?

KATO
ORGANIZZA PER RISOLVERE

GRAZIE PER L'ATTENZIONE

KATO srls
Sede legale ed operativa: 24121 BERGAMO (BG) – Via Pignolo n. 51
Tel. : 328-1378104 – 0350401897
Email: info@katoservizi.it PEC: katosrls@pec.it
Web: http://www.katoservizi.it