Sistema di segnalazione whistleblowing

riflessi della nuova disciplina sul trattamento dei dati personali

Confindustria Macerata, 28 settembre 2023

Daniele Santucci
DPO, Consulente privacy e protezione dei dati personali

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

SISTEMA DI SEGNALAZIONE

Il sistema di segnalazione presuppone un **trattamento di dati personali** riferito ai soggetti segnalanti, ai segnalati ed alle persone (eventualmente) menzionate nella segnalazione.

Affinché sia uno strumento efficace è necessario che sia in grado di assicurare una protezione adeguata ed equilibrata ai segnalanti

garanzie di protezione da ritorsioni e conseguenze negative

un sistema sicuro e riservato incoraggia l'utilizzo dello strumento stesso

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

CANALI DI SEGNALAZIONE

- **CANALE INTERNO**
  - canale progettato, realizzato e gestito dall'organizzazione
  - affidato ad un soggetto esterno autonomo, specificamente formato
- **CANALE ESTERNO** istituito presso l'Autorità Nazionale Anticorruzione (ANAC)
- **DIVULGAZIONE PUBBLICA**
  tramite la stampa, mezzi elettronici o mezzi di diffusione in grado di raggiungere un numero elevato di persone
- **DENUNCIA** all'Autorità giudiziaria o contabile

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

CANALI DI SEGNALAZIONE

- **CANALE INTERNO**
  - canale progettato, realizzato e gestito dall'organizzazione
  - affidato ad un soggetto esterno autonomo, specificamente formato

Oggetto dell'analisi odierna

- **CANALE ESTERNO** istituito presso l'Autorità Nazionale Anticorruzione (ANAC)
- **DIVULGAZIONE PUBBLICA**
  tramite la stampa, mezzi elettronici o mezzi di diffusione in grado di raggiungere un numero elevato di persone
- **DENUNCIA** all'Autorità giudiziaria o contabile

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

CANALE DI SEGNALAZIONE

La segnalazione può essere effettuata:

- **in forma scritta**, anche attraverso **posta** o modalità **informatiche** (es piattaforme di whistleblowing conformi)
- **in forma orale**, a mezzo di linee telefoniche, sistemi di messaggistica vocale, trascrivendo un verbale che il segnalante può verificare rettificare e confermare mediante sottoscrizione.
- su richiesta del segnalante, mediante un **incontro diretto** fissato entro un termine ragionevole

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

CANALE DI SEGNALAZIONE

Il canale interno per ricevere le segnalazioni deve essere **progettato**, **realizzato** e **gestito** in modo tale da garantire la **RISERVATEZZA**

dell'identità del segnalante

degli eventuali terzi
la persona coinvolta (segnalato),
il facilitatore,
le altre persone eventualmente menzionate nella segnalazione

del contenuto della segnalazione e della relativa documentazione

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

GARANZIE DI RISERVATEZZA

- l'identità del segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni
- la protezione riguarda il nominativo del segnalante e tutti gli elementi della segnalazione dai quali si possa ricavare, anche indirettamente, l'identificazione del segnalante
- la segnalazione è sottratta all'accesso agli atti amministrativi e al diritto di accesso civico generalizzato
- l'esercizio dei diritti previsti dal GDPR è limitato qualora possa derivarne un pregiudizio effettivo e concreto alla riservatezza dell'identità del segnalante
- la protezione della riservatezza è estesa all'identità delle persone coinvolte e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

RISERVATEZZA E PROTEZIONE DEI DATI PERSONALI

Nel Regolamento UE 2016/679 la tutela della riservatezza è uno dei principi di trattamento dei dati (art 5.1.f)

Il titolare del trattamento è obbligato alla **responsabilizzazione** , **comprovando** il rispetto dei principi (accountability)

adotta **misure tecniche e organizzative adeguate** per garantire, ed essere in grado di **dimostrare**, che il trattamento è effettuato conformemente al regolamento ed alle norme applicabili.

La violazione della riservatezza costituisce una **violazione dei dati personali** (data breach)

La violazione dei principi è soggetta alla massima **sanzione amministrativa** pecuniaria (fino a 20 mln euro o 4 % del fatturato)

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

PRINCIPI DI TRATTAMENTO DEI DATI PERSONALI

LICEITÀ	Idonea base giuridica: Obbligo legale Consenso (nei casi previsti) Motivi di interesse pubblico
CORRETTEZZA	riconoscimento e rispetto dei diritti degli interessati
TRASPARENZA	Informativa sul trattamento dei dati personali
LIMITAZIONE DELLE FINALITÀ	segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse
ESATTEZZA	verificare che I dati siano esatti, aggiornati.
MINIMIZZAZIONE	I dati che non sono utili al trattamento della segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente
LIMITAZIONE DELLA CONSERVAZIONE	Durata gestione segnalazione e estro 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione
INTEGRITÀ RISERVATEZZA DISPONIBILITÀ	PROTEZIONE DA RISCHIO DI trattamento illecito trattamento non consentito distruzione, perdita modifica, accesso, divulgazione non consentiti

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

PRIVACY BY DESIGN E DEFAULT DEL CANALE DI SEGNALAZIONE

Tenuto conto:

- della natura,
- dell'ambito di applicazione
- del contesto
- delle finalità del trattamento
- dei rischi

Il titolare fornisce

garanzie fin dalla progettazione
(artt. 24, 25 e 32 del GDPR)

- al momento di determinare i mezzi del trattamento
- all'atto del trattamento stesso

misure tecniche e organizzative **adeguate** volte ad:

- attuare in modo efficace i principi di protezione dei dati
- integrare nel trattamento le necessarie garanzie
- trattare solo i dati personali necessari
- non rendere accessibili dati a un numero indefinito di persone

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

PRIVACY BY DEFAULT DEL CANALE DI SEGNALAZIONE

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

PROTEZIONE DEI DATI PERSONALI

Indicazioni di conformità:

- Il legislatore ha ritenuto di fornire nel D.lgs 24/2023 diverse indicazioni per conformare il trattamento alla disciplina in materia di protezione dei dati personali (artt. 12 e 13).
- Le linee guida ANAC sul forniscono importanti indicazioni sulle modalità operative di gestione dei canali di segnalazione
- Il Garante Privacy ha pubblicato alcuni pareri (Provvedimento n. 1 dell'11 gennaio 2023 su uno schema di decreto legislativo recante attuazione della direttiva (UE) 2019/1937, Provvedimento n. 304 del 6 luglio 2023 sulle linee guida ANAC)

L'avvio di un nuovo trattamento presuppone **in ogni caso** una valutazione «privacy by design» dei principi del trattamento, del rischio e delle specifiche misure tecniche ed organizzative connesse alle modalità di segnalazione che si intendono adottare

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

PRIVACY BY DESIGN – CONTENUTI DI UNA «POLICY WHISTLEBLOWING»

- aggiornamento delle **responsabilità** e identificazione delle titolarità del trattamento del canale di segnalazione
- **informativa** agli interessati (art 13,14)
- predisposizione di una **procedura organizzativa** (art 5.2 e 25)
- valutazione del rischio e adozione e documentazione specifiche **misure di sicurezza** (specie a tutela dell'anonimato del segnalante) (art 24 e 32)
- aggiornamento **registro dei trattamenti** (art 30)
- definizione dei termini **conservazione dei dati** (data retenction) (art 5.1.e)
- predisposizione delle **autorizzazioni** da rendere ai preposti al trattamento con le relative **istruzioni** (art 29 e 32.4)
- **formazione** (art 29)
- inquadramento del fornitore della piattaforma di segnalazione come r**esponsabile del trattamento** (art 28)
- conduzione di una **valutazione d'impatto sulla protezione dei dati** (art 35)
- Gestire le violazioni dei dati personali (data breach) (art 33)

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

NEL QUADRO DEL PIANO DI INNOVAZIONE DEL FRAMEWORK NORMATIVO EUROPEO

RUOLI E RESPONSABILITÀ

Interessati	• Segnalante • Persona coinvolta (segnalato) • Persone (eventualmente) menzionate nella segnalazione • Facilitatori	• art 4.1.1) del GDPR • art. 2 D.lgs. 24/2023

RUOLO	AZIONE	RIF NORMATIVO
titolarità	I soggetti pubblici e privati tenuti all'attivazione dei canali di segnalazione interna ed esterna sono i **titolari del trattamento**	• art 4.1.7) del GDPR • art. 13 co. 4 D.lgs 24/2023
contitolarità	L'eventuale utilizzo di un canale condiviso (per imprese con meno di 249 dipendenti) presuppone un **rapporto di contitolarità**. Occorre determinare in modo trasparente, **mediante un accordo di contitolarità interno**, le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali.	• art 26 del GDPR • art. 13 co. 5 D.lgs 24/2023

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

NEL QUADRO DEL PIANO DI INNOVAZIONE DEL FRAMEWORK NORMATIVO EUROPEO

RUOLI E RESPONSABILITÀ

RUOLO	ATTIVITÀ	RIF NORMATIVO

soggetti autorizzati alla gestione del canale	• persona fisica **autorizzata a compiere le operazioni di trattamento** dei dati attenendosi alle istruzioni impartite
	• soggetti coinvolti nella gestione delle segnalazioni
	• soggetti **competenti** e **formati** a ricevere e a dare seguito alle segnalazioni
	• autorizzati al trattamento mediante **atto di designazione** nel quale sia disciplinato:
	  • l'ambito di trattamento
	  • le istruzioni relative al trattamento e relative misure di sicurezza
	  • riferimenti a procedure whistleblowing e utilizzo dei canali
	  • informazioni sui vincoli di riservatezza, anche successivamente al termine del rapporto di collaborazione
	  • rischi connessi al trattamento
		• art. 4 co. 2 D.lgs. 24/2023
		• art. 2-quaterdecies D.lgs 196/2003

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

NEL QUADRO DEL PIANO DI INNOVAZIONE DEL FRAMEWORK NORMATIVO EUROPEO

RUOLI E RESPONSABILITÀ

RUOLO	ATTIVITÀ	RIF NORMATIVO
Responsabili del trattamento	• Il soggetto che **tratta dati personali per conto del titolare del trattamento** (es fornitore della piattaforma whistleblowing, gestore esterno del canale, consulente esterno ecc.) • deve presentare **garanzie sufficienti**, valutate preliminarmente, mantenute e verificate nel tempo • deve essere in grado di mettere in atto misure tecniche e organizzative che garantiscano la protezione dei dati • fornisce elementi **utili alla conduzione della valutazione di impatto** • fornisce supporto al titolare nella gestione di incidenti di sicurezza e violazioni di dati personali • i rapporto va disciplinato da un contratto o da altro atto giuridico vincolante (**Data Processing Agreement**) • In caso di danno causato dal trattamento Il responsabile e il titolare sono responsabili in solido per l'intero ammontare del danno	• art 28 del GDPR • art. 13 co. 4 D.lgs 24/2023

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

NEL QUADRO DEL PIANO DI INNOVAZIONE DEL FRAMEWORK NORMATIVO EUROPEO

RUOLI E RESPONSABILITÀ – RPD/DPO

RUOLO	ATTIVITÀ	RIF NORMATIVO
RPD / DPO	• fornire pareri **sull'utilizzabilità dei dati** trattati nel corso dell'istruttoria, evitando che possano aver luogo trattamenti di dati personali non riconducibili all'ambito di trattamento consentito • sorvegliare il rispetto dei **principi di liceità e proporzionalità** • fornire suggerimenti e pareri sulle **procedure ed i sistemi di segnalazione** • fornire supporto nella **prevenzione e gestione delle violazioni** • attuare **controlli** ed **audit** sullo stato di adozione delle procedure e sulle misure di sicurezza • partecipare alla **formazione** del personale • se richiesto fornire un **parere in merito alla valutazione d'impatto** • gestire le **richieste di informazioni** che possano pervenire al RPD/DPO • fornire supporto nelle istanze di esercizio dei diritti	• Artt. 37-39 del GDPR • Art 2 co.1 lett. a 3) D.lgs 24/2023

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

TRASPARENZA

devono essere comunicati chiaramente

(art 12, 13 e 14 GDPR e artt. 13 co. 4 e 5 D.lgs 24/2023)

- i canali di segnalazione
- le procedure ed i presupposti per effettuare le segnalazioni
- le informative sul trattamento dei dati personali

Le informazioni sulle modalità di una segnalazione sono rese disponibili in modo **chiaro** e **facilmente accessibile**

- eventuale sezione whistleblowing dedicata nel **sito web**
- esposte e rese facilmente visibili nei **luoghi di lavoro**,
- in luoghi **accessibili ai terzi** che intrattengono rapporti giuridici con il titolare del canale di segnalazione
- **invitano** i segnalanti a utilizzare esclusivamente i canali appositamente istituiti che offrono maggiori garanzie di sicurezza e riservatezza

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

INFORMATIVA SUL TRATTAMENTO

Informativa al segnalante

Rendere ex ante agli interessati segnalanti e facilitatori l'informativa sul trattamento dei dati personali
(art 13 del GDPR – dati personali siano raccolti presso l'interessato)

Informativa al segnalato

Nella fase di acquisizione della segnalazione e della eventuale successiva istruttoria **non devono essere fornite informative ai soggetti interessati diversi dal segnalante** (rischio di pregiudicare la finalità del trattamento)

Laddove all'esito dell'istruttoria sulla segnalazione si avvii un procedimento nei confronti di uno specifico soggetto segnalato, a quest'ultimo andrà resa un'informativa specifica.
(art 14 del GDPR – dati non ottenuti presso l'interessato)

L'informativa deve essere

concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (es con indici, icone, versioni sintetiche ecc.)

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

DIRITTI DEGLI INTERESSATI

Esercizio dei diritti

Se dall'esercizio dei diritti cui agli articoli da 15 a 22 del GDPR possa **derivare un pregiudizio alla tutela della riservatezza** dell'identità del segnalante, alla persona coinvolta o la persona menzionata nella segnalazione è **preclusa la possibilità di rivolgersi al Titolare del trattamento**.

In tal caso i diritti potranno essere esercitati per tramite del Autorità Garante per la protezione dei dati personali (con le modalità di cui all'articolo 160 del Codice Privacy).

In tale ipotesi, l'Autorità Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché' del diritto dell'interessato di proporre ricorso giurisdizionale

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

CONSENSO AL TRATTAMENTO

Consenso del segnalante
(art 6 par 1 lett a) del GDPR).

La segnalazione potrà essere utilizzata per un eventuale il procedimento disciplinare solo in caso di un **espresso consenso del segnalante a rivelare la sua identità** ove la stessa sia necessaria per lo svolgimento del procedimento.

La **registrazione** o la **trascrizione** della segnalazione in presenza, telefonica o tramite messaggistica vocale può avvenire solo con espresso consenso del segnalante (art 6 par 1 lett a) del GDPR).

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.

Condizioni del consenso
(art 7 par 1 lett a) del GDPR).

Manifestazione di volontà libera, specifica, informata e inequivocabile, verificabile. Si suggerisce la dichiarazione scritta, anche attraverso mezzi elettronici, ai fini della documentazione.

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

NEL QUADRO DEL PIANO DI INNOVAZIONE DEL FRAMEWORK NORMATIVO EUROPEO

REGISTRO DEI TRATTAMENTI – TITOLARE DEL TRATTAMENTO

- Predisporre una specifica scheda del registro dei trattamenti riferita al trattamento dei dati connesso all'istituzione del canale di segnalazione
- La norma fornisce elementi utili alla predisposizione del registro delle attività di trattamento in ordine alle:

Finalità e basi giuridiche del trattamento
Categorie di interessati
Categorie di dati personali
Categorie di destinatari
Termini di cancellazione

attenzione

i contenti del registro devono essere allineati ai contenuti dell'informativa sul trattamento dei dati

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

NEL QUADRO DEL PIANO DI INNOVAZIONE DEL FRAMEWORK NORMATIVO EUROPEO

REGISTRO DEI TRATTAMENTI – TITOLARE DEL TRATTAMENTO

Finalità e basi giuridiche del trattamento	acquisizione e gestione delle segnalazioni di fatti illeciti e per la gestione dell'eventuale istruttoria
Categorie di interessati	• **adempimento di un obbligo legale** al quale è soggetto il titolare del trattamento (dall'art. 6, par 1, lett. c) del GDPR) • Enti: **esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il titolare del trattamento (art 6 par 1 lett e) del GDPR).; • **Consenso** del segnalante (art 6 par 1 lett a) del GDPR) nel caso di procedimento disciplinare o trascrizione
Categorie di dati personali	• dati personali contenuti nella segnalazione (identificativi, di contatto, professionali ecc.) • eventuali categorie dati personali qualificabili come particolari
Categorie di destinatari	• soggetti pubblici o privati in presenza di violazioni delle normative applicabili • eventuali consulenti e professionisti • fornitori di servizi informatici (piattaforme di segnalazione) • Organismo di Vigilanza
Termini di cancellazione	• conservazione 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
Misure di sicurezza	• Riferimenti alle specifiche misure del canale di segnalazione (es crittografia piattaforma ecc.)

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

NEL QUADRO DEL PIANO DI INNOVAZIONE DEL FRAMEWORK NORMATIVO EUROPEO

REGISTRO DEI TRATTAMENTI – TITOLARE DEL TRATTAMENTO

Il registro può essere integrato con altre informazioni che il titolare o il responsabile ritengano utile indicare:

Referenti interni, responsabili di processo	(es. ufficio segnalazioni, RPCT, OdV …)
Riferimenti a processi operativi e procedure di gestione del whistleblowing	
Dettagli sulla provenienza dei dati in relazione al canale di segnalazione adottato	
Riferimenti a procedure di trasparenza ed informative	(es. riferimenti informativa su web)
Riferimenti a strumenti	(es. piattaforma whistleblowing)
Riferimenti alla valutazione di impatto	
Elementi di valutazione del rischio	(es matrici di rischio, valori di rischio residuo, valutazioni in caso di perdita riservatezza, integrità, disponibilità ecc.)

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

TERMINI DI CANCELLAZIONE

Durata del trattamento

Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e, se del caso, all'adozione dei provvedimenti disciplinari conseguenti e/o all'esaurirsi di eventuali contenziosi avviati a seguito della segnalazione.

Termini di cancellazione

Il trattamento non si protrarrà oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

Conservazione anonima

i dati potranno essere successivamente anonimizzati per finalità statistiche o di storicizzazione.

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

PROCEDURA ORGANIZZATIVA

funzione generale

- definisce i criteri generali, le responsabilità e le modalità operative, regolando le modalità di segnalazione, la gestione dell'istruttoria,
- strumento organizzativo e di «accountability»
- fornisce prescrizioni chiare e univoche per tutte le risorse e le funzioni coinvolte
- descrive quanto deve essere fatto per assicurare che i requisiti normativi siano chiaramente definiti
- evita errori, dimenticanze, ambiguità e incompatibilità nelle prescrizioni
- può essere integrata nei Sistemi di Gestione, nei MOG, Codice Etico ecc

funzione specifica

- consentire all'interessato di effettuare le segnalazioni assicurandone la riservatezza
- negli enti la procedura diviene parte dell'attività di trasparenza (D.Lgs 33/2013)
- elemento verificabile, disponibile agli auditor, garanzia di conformità e trasparenza

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

*Quando un tipo di trattamento, allorché prevede in particolare l'uso di **nuove tecnologie**, considerati la **natura**, **l'oggetto**, il **contesto** e le **finalità del trattamento**, può presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.*

(art 35 del GDPR)

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

il trattamento dei dati personali mediante i sistemi di acquisizione e gestione delle segnalazioni **presenta rischi specifici per i diritti e le libertà degli interessati**

OGGETTO	CONTESTO	FINALITÀ
particolare delicatezza delle informazioni potenzialmente trattate	vulnerabilità degli interessati nel contesto lavorativo	perseguita in regime di riservatezza dell'identità del segnalante

è necessario definire il modello di ricevimento e gestione delle segnalazioni sulla base di una valutazione d'impatto sulla protezione dei dati

espressamente previsto dal D.lgs 24/2023 (art. 13, co. 6) e in relazione alla valutazione del doppio criterio delle linee guida WP 248 sulla valutazione di impatto.

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La **valutazione di impatto contiene almeno**:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento

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

c) una valutazione dei rischi per i diritti e le libertà degli interessati

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

(art 35 par 7 del GDPR)

Il legislatore ha fornito elementi relativi alle **finalità, necessità e proporzionalità del trattamento** e (pre)definito **elevato l'impatto** sugli interessati

la valutazione si concentrerà sulla valutazione dei rischi e sulla implementazione delle misure di sicurezza

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

VALUTAZIONE DEL RISCHIO

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

(alcune significative) conseguenze al concretizzarsi di rischi privacy nel whistleblowing

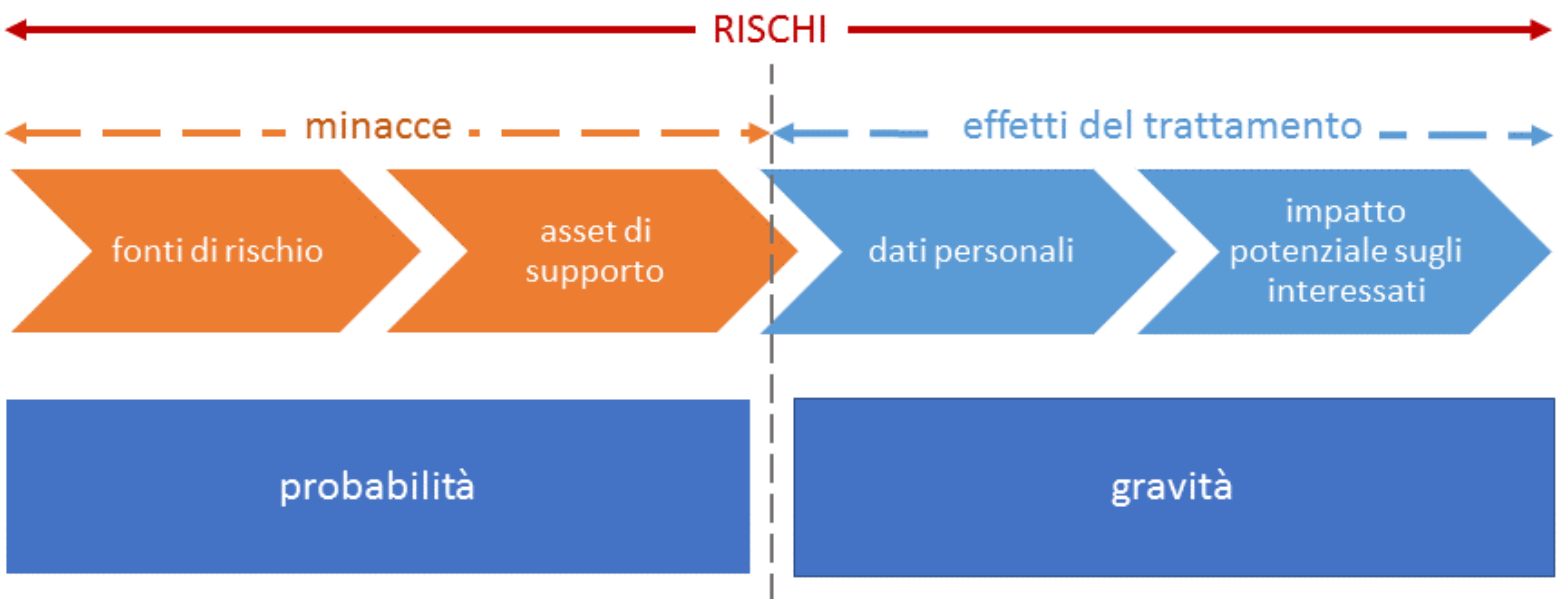
comportamenti ritorsivi

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

VALUTAZIONE DEL RISCHIO

rapporto scalare tra
le CONSEGUENZE (e loro gravità) di un
EVENTO (minaccia) e la
PROBABILITÀ di accadimento di tale evento



SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

VALUTAZIONE DEL RISCHIO

Perdita dei dati	Violazione DISPONIBILITA'
Distruzione non autorizzata	
Modifica indesiderata o non autorizzata	Violazione INTEGRITA' E ESATTEZZA
Divulgazione non autorizzata	Violazione RISERVATEZZA
Accesso ai dati non autorizzato o illegittimo	
Eccessiva raccolta di dati personali;	Violazione NECESSITA' E PROPORZIONALITA'
Collegamenti o raffronti inappropriati o non autorizzati di dati personali	
Perdita di controllo da parte degli interessati (mancanza di trasparenza, chiarezza, non considerazione dei diritti)	Violazione LICEITA'. TRASPARENZA E CORRETTEZZA
Divulgazione o riuso per finalità diverse dei dati personali senza la consapevolezza e/o il consenso degli interessati	
Conservazione immotivamente prolungata dei dati personali	Violazione LIMITAZIONE DELLA CONSERVAZIONE

(ISO/IEC 29134 -paragrafo 6.4.4.1 identificazione dei rischi privacy)

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

MITIGAZIONE DEL RISCHIO

ADOZIONE DI MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

indicate dalla norma e linee guida:

- crittografia
- oscuramento
- protocollazione riservata
- formazione
- …….

Misure adottate dall'organizzazione in relazione ai canali di segnalazione utilizzati

AGID — MISURE AGID

ISO 27000 — CONTRLLI DERIVATI DA STANDARD

enisa — MISURE ENISA

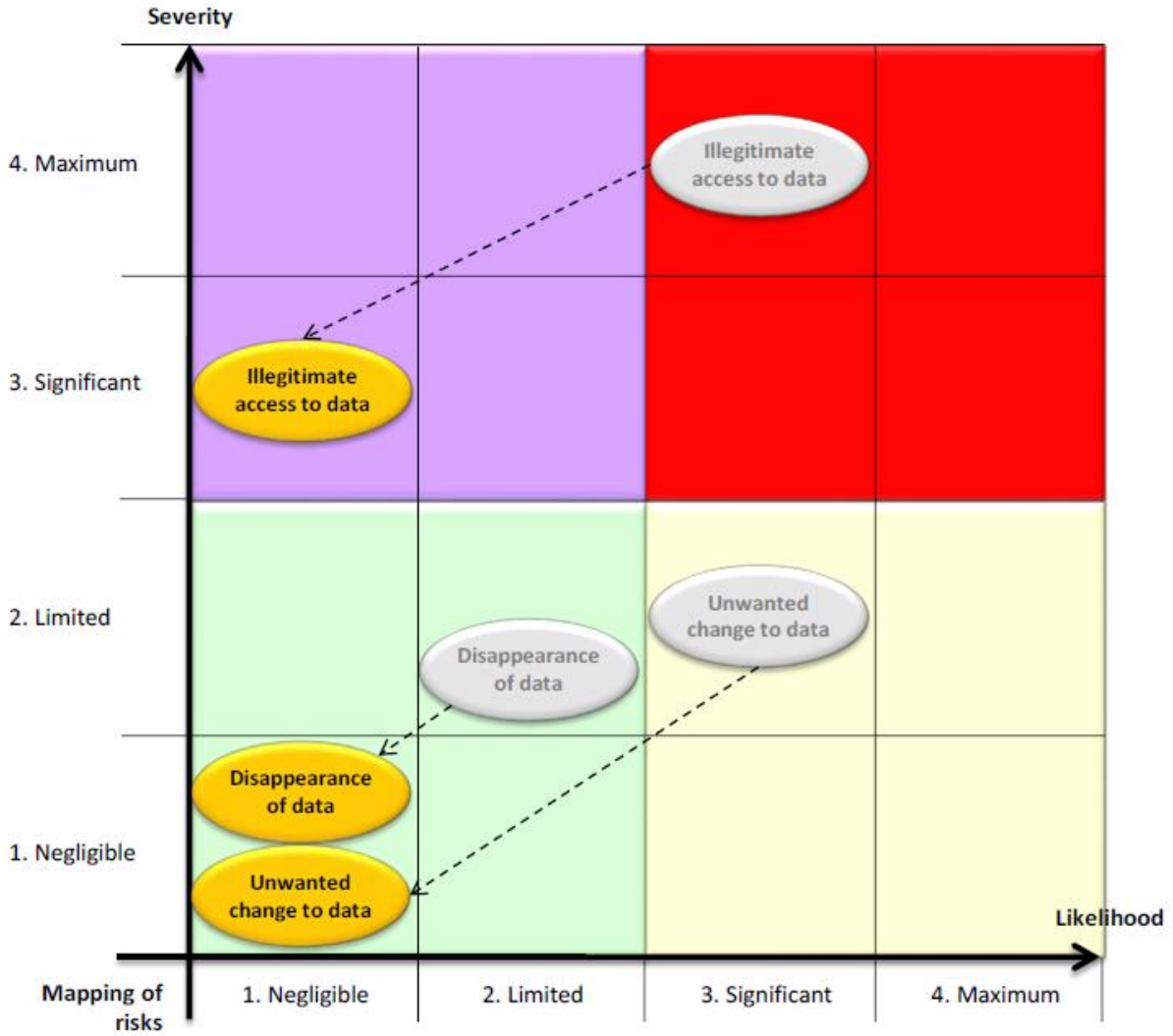
NIST National Institute of Standards and Technology U.S. Department of Commerce — MISURE NIST

ECC….

RIDUZIONE DEL RISCHIO AD UN LIVELLO ACCETTABILE

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali



SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

MISURE DI SICUREZZA

(alcune) misure atte a mitigare il rischio, intervenendo sulle minacce e sulle vulnerabilità

Misure di sicurezza

Crittografia del canale di segnalazione

procedura di oscuramento dei dati personali riservati qualora, per ragioni istruttorie, anche altri soggetti debbano essere messi a conoscenza del contenuto della segnalazione e/o della documentazione ad essa allegata.

protocollazione riservata (ad esempio mediante il meccanismo delle doppia (o tripla) busta chiusa)

Misure organizzative

Procedure organizzative ed istruzioni Operative

Formazione del personale

Valutazione iniziale e monitoraggio dei fornitori responsabili del trattamento

procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

MISURE DI SICUREZZA

Accorgimenti e indicazioni dell'Autorità Garante Privacy e dell'ANAC (Linee Guida whistleblowing, delibera n. 311 del 12 luglio 2023)

posta elettronica e PEC

il ricorso alla posta elettronica ordinaria e certificata **non è di per sé adeguato** a garantire la riservatezza

tracciamento

è **vietato il tracciamento dei canali di segnalazione** e di qualunque informazione che possa ricondurre all'identità o all'attività del segnalante

ove possibile **garantire 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.

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

MISURE DI SICUREZZA

REQUISITO	AZIONE OPERATIVA E RACCOMANDAZIONE
RISERVATEZZA	**PIATTAFORMA DI SEGNALAZIONE** **Crittografia** • in transito: es protocolli https (certificati SSL) nelle piattaforme web based • in memorizzazione su database / server • policy di gestione chiavi crittografiche (conservazione e backup) **Anonimizzazione** policy di cancellazione, automatica o manuale, dei riferimenti identificativi (inclusi i record dei database o presenti nei documenti) una volta raggiunti i termini di conservazione **Protezione da accesso non autorizzato / trattamento non consentito**: • autenticazione nominale autorizzati e controllo accessi logici (2FA / SSO e LOG degli accessi) • aggiornamento password periodico • profili di autorizzazione alla piattaforma

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

MISURE DI SICUREZZA

REQUISITO	AZIONE OPERATIVA E RACCOMANDAZIONE
INTEGRITÀ	• canali trasmissione sicuri (es https) • tracciabilità (LOG accessi soggetti autorizzati) • analisi integrità dei backup
DISPONIBILITÀ	• procedura di backup e misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico • eventuale integrazione con piani di disaster recovery • test integrità dei dati
RESILIENZA	• verifica e gestione delle vulnerabilità e aggiornamento • eventuale integrazione con piani di business continuity • gestione eventi imprevisti, incidenti • misure proattive, policy di hardening dei sistemi • meccanismi di blocco automatico dell'utenza, in caso di ripetuti tentativi di autenticazione falliti

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

MISURE DI SICUREZZA

REQUISITO	AZIONE OPERATIVA E RACCOMANDAZIONE
ALTRE MISURE E CYBERSECURITY	• sistemi protetti da antimalware e firewall • sistemi di alert vulnerabilità • policy aggiornamenti sistemi e patch • policy di gestione manutenzioni esterne • policy di gestione accessi fisici (tutela documentazione cartacea) • policy di gestione documenti cartacei • rilevazione e gestione incidenti e violazioni
CONFIGURAZIONI / PERSONALIZZAZIONI RESE POSSIBILI DAL SISTEMA	• modifica complessità credenziali • modifica profili autorizzazione / tipologia accessibilità dati • modifica tempi conservazione dati • accesso ai LOG (amministratori di sistema / soggetti autorizzati) • estrazione di report (individuali / statistici con dati aggregati)

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

VIOLAZIONI DEI DATI PERSONALI (DATA BREACH)

una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

(art33 GDPR)

concretizzazione del rischio

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

PROVVEDIMENTI SANZIONATORI DEL GARANTE PRIVACY

Provvedimento nei confronti di Aeroporto G.Marconi di Bologna Spa, 10 giugno 2021 [9685922]

violazione degli artt. 5, par. 1, lett. f), 25, 32 e 35 del Regolamento, sanzione € 40,000

Provvedimento nei confronti di aiComply Srl, 10 giugno 2021 [9685947]

violazione degli artt. 28 e 32 del Regolamento, sanzione € 20,000

Provvedimento nei confronti di Azienda ospedaliera di Perugia, 7 aprile 2022 [9768363]

violazione degli artt. 5, par. 1, lett. a) e f), 13, 14, 25, 30, 32 e 35 del Regolamento, sanzione € 40,000

Provvedimento nei confronti di ISWEB Spa, 7 aprile 2022 [9768387]

violazione degli art 28 del Regolamento, sanzione € 40,000

SISTEMA DI SEGNALAZIONE WHISTLEBLOWING

riflessi della nuova disciplina sul trattamento dei dati personali

PROVVEDIMENTI SANZIONATORI DEL GARANTE PRIVACY

Principali motivazioni:

- Mancata regolazione del rapporto con il fornitore del servizio
- Mancato aggiornamento del registro del trattamento
- Assenza dell'informativa agli interessati
- Assenza di una valutazione di impatto
- Inadeguatezza delle misure di sicurezza:
  - Mancato utilizzo di tecniche crittografiche per il trasporto e la conservazione dei dati
  - Inidoneità delle modalità di gestione delle credenziali di autenticazione
  - Tracciamento degli accessi all'applicativo per l'acquisizione e la gestione delle segnalazioni di condotte illecite

grazie per l’attenzione

Confindustria Macerata, 28 settembre 2023

Daniele Santucci
DPO, Consulente privacy e protezione dei dati personali