Valutazione dell'impatto sulla privacy ("DPIA")

Introduzione

Regolamento Ue 2016/679

Il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (d'ora innanzi GDPR), come noto, ha profondamente innovato la materia della privacy.

Partendo dalla sintesi dell'esperienza applicativa nei singoli stati membri della c.d. direttiva madre - il riferimento è qui alla direttiva 95/46/CE -, infatti, la novella ha rimodulato l'intera disciplina in materia a partire da due principi cardine: da un lato, la tutela dei diritti e delle libertà degli interessati e, dall'altro lato, la responsabilizzazione degli operatori pubblici e privati che trattano i dati personali.

Per raggiungere il predetto, duplice, obiettivo, il legislatore europeo si è mosso secondo alcune direttrici fondamentali che, per sommi capi, comprendono:

- ✓ coerenza delle norme;
- ✓ semplificazione delle procedure;
- ✓ coordinazione delle azioni di prevenzione e di tutela;
- ✓ coinvolgimento degli utenti;
- ✓ maggiore e migliore trasparenza;
- ✓ rafforzamento dei poteri sanzionatori;

- ✓ partecipazione attiva delle imprese all'attuazione concreta del GDPR.

Partendo dalla prospettiva propria dell'interessato, in altre parole, il GDPR si è posto l'obiettivo di trovare il punto d'equilibrio tra le esigenze del singolo trattamento dei dati personali e i diritti inviolabili delle persone fisiche.

È proprio in quest'ottica, d'altro canto, che devono essere riempiti di concreti contenuti i principi cardine della privacy by design e della privacy by default, i quali impongono al titolare del trattamento di progettare la compliance aziendale al GDPR fin dalla fase di progettazione imprenditoriale - privacy by design - e, comunque, come impostazione predefinita rispetto al trattamento stesso - privacy by default -.

Da quanto precede discende un quadro d'insieme che, se per un verso, è volto alla de-burocratizzazione del settore-privacy, per l'altro verso, appare incentrato sulla responsabilizzazione dei titolari del trattamento, che, proprio nell'ottica di tutelare i diritti e le libertà degli interessati, vengono chiamati in prima persona a riempire di concreti contenuti i precetti normativi passati in rassegna dal GDPR.

Di primaria importanza, nella predetta prospettiva, risultano essere peraltro i profili sanzionatori propri del GDPR.

Contenuti principalmente nell'art. 83 GDPR, infatti, i predetti profili, sono chiamati a chiudere il cerchio della prevenzione - generale e particolare - posta a base del GDPR, contribuendo con ciò ad assicurare la piena attuazione dello stesso.

Modello di valutazione dei rischi

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

A mente dell'art. 35 par. 7 lett c] GDPR, la valutazione di impatto sulla protezione dei dati - che il GDPR impone di realizzare «[q]uando 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» - deve contenere anche «una valutazione dei rischi per i diritti e le libertà degli interessati».

Lo scopo del presente documento è quello di compiere una valutazione di impatto sulla protezione dei dati trattati per il tramite della Piattaforma SCS WHISTLEBLOWING

Criteri per la stima dei livelli di impatto, delle probabilità e vulnerabilità, metodologia per la valutazione dei rischi e criteri per l'accettazione dei rischi

Per la ***determinazione delle possibili conseguenze*** per gli interessati e per ***valutare i rischi*** per le libertà e i diretti degli interessati sono state considerate le seguenti pubblicazioni:

Le Linee guida WP248 Rev.01;

I pareri dell'EPDB (2018) rispetto agli Elenchi delle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto proposti dalle Autorità di Controllo;

Le pubblicazioni e il Tool PIA del CNIL;

Le pubblicazioni ENISA "Guidelines for SMEs on the security of personal data processing" e "Handbook on Security of Personal Data Processing";

Le Linee Guida per la Data Protection Impact Assessment dell'Osservatorio Information Security e Privacy del Politecnico di Milano School of Management;

La norma standard ISO/IEC 29134:2017;

La norma standard ISO 31000:2018;

Per gli ***obiettivi di controllo***, sono state considerate le seguenti pubblicazioni:

ISO/IEC 27001:2013;

ISO/IEC 29151:2017;

La framework NIST-800-SP53-Rev4;

Le UNI/PdR 43.1:2018 – Prassi di riferimento per la gestione dei dati personali in ambito ICT

Viene utilizzata la metodologia di valutazione: CNIL

Criteri utilizzati:

Per la ***determinazione dei livelli di impatto*** per gli interessati vengono considerati i seguenti:

Livello	**IMPATTO PRIVACY**
Trascurabile (Basso)	Gli interessati possono incontrare alcuni piccoli inconvenienti, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
Limitato (Medio)	Gli interessati possono incontrare inconvenienti significativi, che riusciranno a superare a dispetto di alcuni problemi (costi aggiuntivi, impossibilità di accesso a servizi, timore o mancanza di comprensione, stress, disagi o disturbi fisici minori, ecc.).
Importante (Alto)	Gli interessati possono incontrare 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 del posto di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
Massimo (Critico)	Gli interessati possono avere conseguenze significative, o addirittura irreversibili, che potrebbero non superare (incapacità di lavorare, gravissima perdita economica, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Per la scala dei ***livelli di probabilità*** che si verifichino le minacce sui dati:

Livello	**MINACCE PRIVACY**
Bassissimo	è molto raro che la minaccia si materializzi
Basso	è improbabile che la minaccia avvenga in condizioni normali
Moderato	la minaccia potrebbe materializzarsi, è un avvenimento già accaduto
Probabile	la minaccia potrebbe materialmente verificarsi, si è già verificata ed è
Quasi certo	è altamente probabile che la minaccia possa materializzarsi

Per la scala dei ***livelli di rischio*** valutati rispetto all'attività di trattamento

Livello	**RISCHIO PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI**
Trascurabile (Basso)	Il rischio è accettabile dall'organizzazione mediante misure organizzative e tecniche idonee, ma deve continuare ad essere monitorato per controllare che cambiamenti non incrementino il livello di rischio
Limitato (Medio)	Il rischio medio potrebbe essere accettabile ma l'adozione delle misure tecnico-organizzative deve essere monitorata su basi regolari, e il trattamento può essere sottoposto a ulteriori considerazioni
Importante (Alto)	Il rischio è ad un livello non accettabile e necessita un rafforzamento delle misure di mitigazione.
Massimo (Critico)	Il rischio si presenta elevato nella sua forma residuale, mantenendo un livello non accettabile per l'organizzazione e necessitando l'aggiunta di ulteriori controlli a prevenzione/mitigazione dello stesso.

*

"La protezione delle persone che segnalano violazioni del diritto dell'unione" (cd. disciplina whistleblowing)

Premessa

Con il decreto legislativo 10 marzo 2023, n. 24 (di seguito anche "Decreto"), pubblicato nella Gazzetta Ufficiale del 15 marzo 2023, è stata recepita nell'ordinamento italiano la direttiva UE 2019/1937 riguardante "la protezione delle persone che segnalano violazioni del diritto dell'Unione" (cd. disciplina whistleblowing).

L'obiettivo della direttiva europea è stabilire norme minime comuni per garantire un elevato livello di protezione delle persone che segnalano violazioni del diritto dell'Unione, creando canali di comunicazione sicuri, sia all'interno di un'organizzazione, sia all'esterno. In casi specifici, è prevista la possibilità di effettuare la segnalazione mediante la divulgazione pubblica attraverso i media.

Si tratta di una disciplina che persegue, come fine ultimo, il contrasto e la prevenzione dei fenomeni illeciti nelle organizzazioni pubbliche e private, incentivando l'emersione di condotte pregiudizievoli - di cui il segnalante sia venuto a conoscenza nell'ambito del suo contesto lavorativo - in danno dell'ente di appartenenza e, di riflesso, per l'interesse pubblico collettivo.

Il Decreto abroga e modifica la disciplina nazionale previgente, racchiudendo in un unico testo normativo - per il settore pubblico e per il settore privato - il regime di protezione dei soggetti che segnalano condotte illecite poste in essere in violazione non solo di disposizioni europee, ma anche nazionali, purché basate su fondati motivi e lesive dell'interesse pubblico o dell'integrità dell'ente, al fine di garantire il recepimento della direttiva senza arretrare nelle tutele già riconosciute nel nostro ordinamento.

Il quadro regolatorio di riferimento è stato infine completato con le Linee Guida ANAC adottate con delibera del 12 luglio 2023, recanti procedure per la presentazione e gestione delle segnalazioni esterne, nonché indicazioni e principi di cui enti pubblici e privati possono tener conto per i canali interni.

Il Decreto prevede che la nuova disciplina si applichi, in via generale, a decorrere dallo scorso 15 luglio 2023 (art. 24). Invece, per i soggetti del settore privato che, nell'ultimo anno, hanno impiegato una media di lavoratori subordinati fino a 249 unità, l'obbligo di istituire un canale interno

di segnalazione ha effetto a decorrere dal 17 dicembre 2023; fino a quel giorno, continua ad applicarsi la disciplina previgente (art. 6, co. 2-bis del Decreto legislativo 8 giugno 2001, n. 231, di seguito anche "Decreto 231").

A mente della normativa, il ricevimento e la gestione delle segnalazioni determinano in capo al Cliente un trattamento dei dati personali:

• di natura comune, di natura particolare (ex "dati sensibili") e giudiziari (quali condanne penali e reati), eventualmente contenuti nella segnalazione e negli atti e nei documenti a essa allegati (v. Parere del Garante privacy sullo "Schema di 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", provv. 6 luglio 2023, n. 304, di seguito, "Parere del Garante privacy");

• relativi a tutte le persone fisiche - identificate o identificabili - a vario titolo coinvolte nelle vicende segnalate (segnalante, segnalato, facilitatore, eventuali altri terzi), c.d. interessati;

• necessario per dare attuazione agli obblighi di legge previsti dalla disciplina whistleblowing la cui osservanza è condizione di liceità del trattamento ex art. 6, par. 1, lett. c) e parr. 2 e 3, art. 9, par. 2, lett. b) e artt. 10 e. 88 del GDPR (v. Parere del Garante privacy);

• realizzato al solo fine di gestire e dare seguito alle segnalazioni (art. 12, co. 1 del Decreto);

• che, in ragione della particolare delicatezza delle informazioni potenzialmente trattate, della vulnerabilità degli interessati nel contesto lavorativo, nonché dello specifico regime di riservatezza dell'identità del segnalante previsto dal Decreto, presenta rischi specifici per i diritti e le libertà degli interessati (v. Parere del Garante privacy) e, pertanto, deve essere preceduto da una valutazione d'impatto sulla protezione dei dati, c.d. DPIA (art. 13, co. 6 del Decreto e artt. 35 e 36 del GDPR);

• rispetto al quale, l'esercizio dei diritti degli interessati (es. accesso, rettifica, aggiornamento, cancellazione, limitazione del trattamento, portabilità, opposizione) può essere limitato qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del segnalante (art. 13, co. 3 del Decreto e art. 2-undecies del Codice privacy).

DPIA SCS WHISTLEBLOWING

Contesto

La piattaforma SCS WHISTLEBLOWING consente l'identificazione di ogni segnalazione ricevuta mediante l'attribuzione di un codice univoco progressivo.

La piattaforma SCS WHISTLEBLOWING consente, in modo informatizzato, la compilazione, l'invio e la ricezione del modulo di segnalazione, la gestione dell'istruttoria e l'eventuale inoltro agli organi / funzioni interne competenti per i relativi seguiti.

SCS WHISTLEBLOWING conformemente alla disposizione di cui all' art. 7, co. 1, del d.lgs. n. 24/2023, utilizza strumenti di crittografia ed accesso con autenticazione informatica a più fattori. Ciò garantisce la riservatezza dei dati personali trattati nel processo di segnalazione, ovverosia, sia dei dati trasmessi e ricevuti che di quelli conservati dalla piattaforma.

Il segnalante può liberamente accedere alla apposita area della piattaforma per l'inserimento della segnalazione senza preventiva necessità di autenticazione. In questa area visualizza il modulo di segnalazione da compilare e inviare. Il modulo prevede una apposita sezione che il segnalante deve compilare per sottoscrivere la segnalazione. I dati inseriti in questa sezione, utili alla sua identificazione univoca, sono oggetto di oscuramento e quindi non accessibili ai gestori della segnalazione che si occuperanno dell'istruttoria.

L'interessato è tenuto, altresì, a compilare, in modo chiaro, preciso e circostanziato le rimanenti sezioni del modulo fornendo le informazioni richieste come obbligatorie e il maggior numero possibile di quelle facoltative. La piattaforma informatica funge, di fatto da registro particolare e, pertanto, deve garantire l'integrità e l'immodificabilità della segnalazione.

La piattaforma informatica consente al segnalante di accedere alla propria segnalazione fino a cinque anni successivi alla data di chiusura del fascicolo da parte del gestore della segnalazione. Tale accesso avviene tramite l'utilizzo di un codice identificativo univoco (key code), generato in modo casuale e automatico dalla piattaforma informatica e fornito al segnalante all'esito dell'inoltro della segnalazione. Tale codice consente al segnalante di monitorare lo svolgimento del procedimento eventualmente avviato a seguito della segnalazione, integrare la stessa e dialogare (in modo anonimo e sicuro) con il gestore della segnalazione.

SCS WHISTLEBLOWING, consente, altresì, l'acquisizione delle segnalazioni orali mediante click sull'apposito tasto presente. La piattaforma, dunque, acquisisce la segnalazione e viene attribuito il codice identificativo univoco (*key code*) di primo accesso, generato in modo casuale e automatico. Il canale della segnalazione orale è criptato.

Misure di sicurezza adottate

- Firewall di sicurezza per mitigazione attacchi DDOS;
- I dati risiedono in Cloud Italiano (REEVO) certificato 270001 ISO9001, ISO27001, ISO27017, ISO27018, LEEDS, ISAE 3402, SSAE18, AGID, PCI DSS;
- Disaster Recovery su Farm italiana (Recovery Point Object 1 ora);
- Crittografia E2E 256 bit per mantenere la riservatezza del canale di segnalazione;
- Penetration Test ricorrenti per monitorare le vulnerabilità della piattaforma;
- Database cifrato per garantire la riservatezza dei dati;
- Le connessioni del segnalatore dal firewall alla piattaforma non sono tracciate (Ip non tracciato);

Architettura

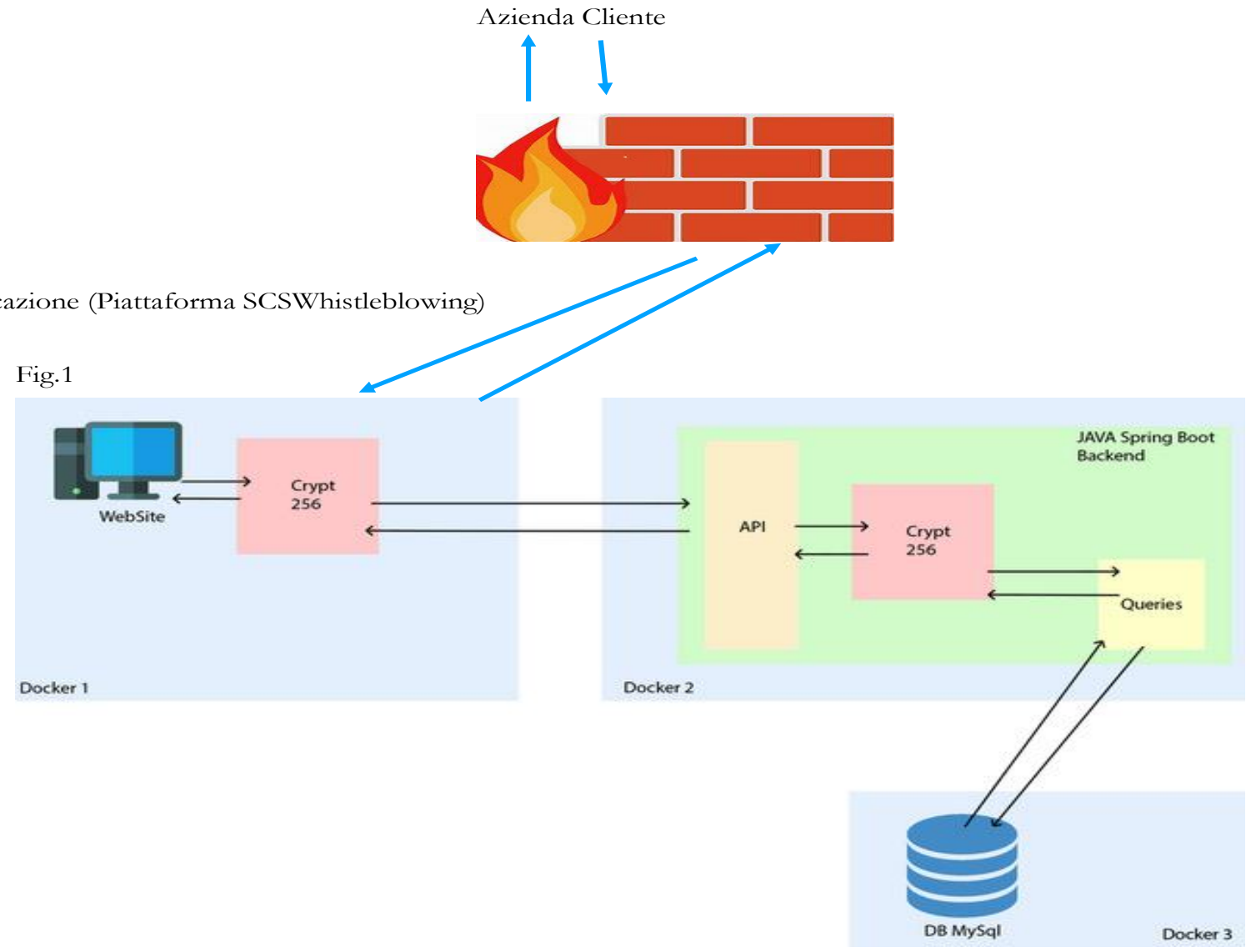

Fig.1

responsabilità connesse al trattamento svolto per il tramite della piattaforma SCS WHISTLEBLOWING

Responsabile del trattamento è SCS4U S.r.l.

Mappatura rischio

No.	1. Il trattamento del dato	2. Necessità e proporzionalità	3. Rischio	4. Vulnerabilità	5. Misura(e)	6. Sono state consultate le altre parti?	7. Rischio dopo la/e misura/e	8. È necessaria la consultazione con l'autorità di vigilanza?
1.	Ricezione di informazioni sulle segnalazioni in SCS Whistleblowing	Obbligatorio ai sensi della normativa sul whistleblowing	Rischio che nel sistema vengano segnalate informazioni intenzionalmente false o comunque errate, il che significa che vengono	Alto	Si raccomanda sempre che lo screening iniziale delle segnalazioni ricevute sia condotto da una persona opportunamente nominata che conosca il	Consulenti legali esperti in protezione dei dati	Accettato	No

			trattati dati personali errati.		sistema e i processi stabiliti in materia di whistleblowing			

No.	1. Il trattamento del dato	2. Necessità e proporzionalità	3. Rischio	4. Vulnerabilità	5. Misura(e)	6. Sono state consultate altre parti?	7. Rischio dopo la/e misura/e	8. È necessaria la consultazione con l'autorità di vigilanza?
2.	Invio del rapporto della segnalazione	Obbligatorio ai sensi della normativa sul whistleblowing	Rischio che l'azienda e/o il personale di SCS Whistleblowing identifichino il segnalante anonimo in violazione delle regole e delle	Alto	Misure tecniche volte a rendere estremamente difficile l'accesso a tali informazioni, tra cui: non vi è alcun collegamento con l'indirizzo e-mail, il	Consulenti legali esperti in protezione dei dati	Accettato	No

			procedure interne		numero di telefono o altri dati di contatto dei segnalanti. Non è obbligatorio inserire i dati di contatto del segnalante.			
No.	1. Il trattamento del dato	2. Necessità e proporzionalità	3. Rischio	4. Vulnerabilità	5. Misura(e)	6. Sono state consultate altre parti?	7. Rischio dopo la/e misura/e	8. È necessaria la consultazione con l'autorità di vigilanza?
3.	Invio di un messaggio al segnalante	Obbligatorio ai sensi della normativa sul whistleblowing	rischio che qualcuno diverso dal segnalante ottenga l'accesso al messaggio.	Alto	Quando il segnalante invia la segnalazione, ottiene un numero di caso univoco e un codice password,	Consulenti legali esperti in protezione dei dati	Accettato	No

					necessari per accedere ai messaggi dell'azienda.			
4.	Assegnazione del caso a un soggetto destinatario della segnalazione	È necessario nominare uno o più soggetti destinatari della segnalazione.	Rischio che qualcun altro, oltre al soggetto destinatario della segnalazione, ottenga l'accesso alla segnalazione.	Alto	Funzionalità di accesso utente, in cui il proprietario o l'amministratore dell'account deve inserire utente e password (Requisiti password: almeno una lettera minuscola. Almeno una lettera maiuscola. Almeno un numero.	Consulenti legali esperti in protezione dei dati	Accettato	No

					Almeno un carattere speciale. Con una lunghezza minima di 10 caratteri.) di ogni gestore di casi aggiunto. Registrazione di ogni azione per ogni utente. Limiti di tempo per l'utilizzo del sistema e l'inattività.			
No.	1. Il trattamento del dato	2. Necessità e proporzionalità	3. Rischio	4. Vulnerabilità	5. Misura(e)	6. Sono state consultate le seguenti parti?	7. Rischio dopo la/e misura/e	8. È necessaria la consultazione con l'autorità di vigilanza?
5.	Assegnazione del caso a una	È necessario uno o più soggetti	Rischio che qualcun altro,	Alto	Funzionalità di accesso utente,	Consulenti legali esperti	Accettato	No

	terza parte, ad esempio l'ODV o altro soggetto destinatario esterno della segnalazione	destinatari della segnalazione.	oltre al soggetto destinatario della segnalazione, ottenga l'accesso alla segnalazione.		in cui il proprietario o l'amministratore dell'account deve inserire utente e password (Requisiti password: almeno una lettera minuscola. Almeno una lettera maiuscola. Almeno un numero. Almeno un carattere speciale. Con una lunghezza minima di 10 caratteri.) di	in protezione dei dati		

					ogni gestore di casi aggiunto. Registrazione di ogni azione per ogni utente. Limiti di tempo per l'utilizzo del sistema e l'inattività.			
No.	1. Il trattamento del dato	2. Necessità e proporzionalità	3. Rischio	4. Vulnerabilità	5. Misura(e)	6. Sono state consultate le seguenti parti?	7. Rischio dopo la/e misura/e	8. È necessaria la consultazione con l'autorità di vigilanza?
6.	Scrivere note nella piattaforma	Necessario per avere le informazioni collegate alla segnalazione nella piattaforma.	Rischio che qualcun altro, oltre al soggetto destinatario della segnalazione, ottenga	Alto	Funzionalità di accesso utente, in cui il proprietario o l'amministratore dell'account deve inserire utente e	Consulenti legali esperti in protezione dei dati	Accettato	No

			l'accesso alla segnalazione.		password (Requisiti password: almeno una lettera minuscola. Almeno una lettera maiuscola. Almeno un numero. Almeno un carattere speciale. Con una lunghezza minima di 10 caratteri.) di ogni gestore di casi aggiunto. Registrazione di ogni azione per ogni utente. Limiti di tempo per			

					l'utilizzo del sistema e per l'inattività. Limiti di tempo per l'utilizzo del sistema e l'inattività.			
No.	1. Il trattamento del dato	2. Necessità e proporzionalità	3. Rischio	4. Vulnerabilità	5. Misura(e)	6. Sono state consultate le seguenti parti?	7. Rischio dopo la/e misura/e	8. È necessaria la consultazione con l'autorità di vigilanza?
7.	L'amministratore o il soggetto destinatario della segnalazione è soggetto destinatario della segnalazione	Il segnalante ha il diritto e la possibilità di segnalare qualsiasi persona all'interno dell'azienda	Rischio che la persona segnalata abbia accesso alla segnalazione in qualità di amministratore o soggetto destinatario della	Alto	Nelle nostre istruzioni di onboarding, consigliamo al cliente di nominare sempre più soggetti destinatari che possano avere accesso a tutte	Consulenti legali esperti in protezione dei dati	Accettato	No

			segnalazione e potenzialmente possa distruggere le prove e/o chiudere il caso senza ulteriori indagini.		le segnalazioni di whistleblower o prevedere nell'atto organizzativo un recapito fisico ove spedire la segnalazione.			