WHISTLEBLOWING

Applicazione pratica in azienda

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Assolombarda Servizi

Soluzioni Concrete per lo sviluppo delle imprese

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

ASPETTI PRIVACY DELLA DISCIPLINA WHISTLEBLOWING

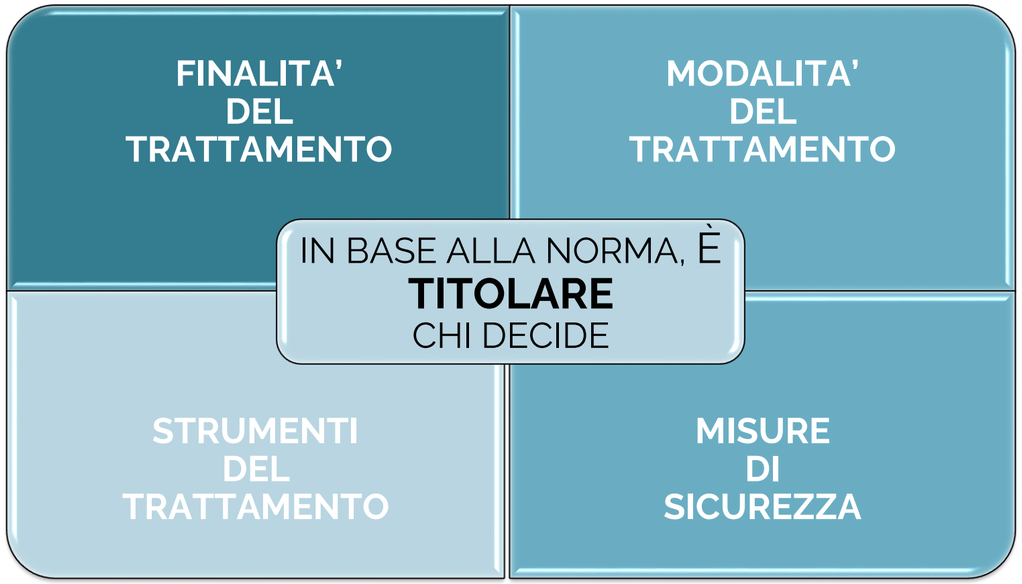
14.11.2023

IL D.LGS 24/2023

- IL **RICEVIMENTO E LA GESTIONE** DELLE SEGNALAZIONI DETERMINANO IN CAPO ALL'AZIENDA IL **TRATTAMENTO DI DATI PERSONALI** DEI SOGGETTI A VARIO TITOLO COINVOLTI NELLA SEGNALAZIONE

- **IL D.LGS 24/2023 CONTIENE DIVERSE DISPOSIZIONI** IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, VOLTE A:
  - ✓ DEFINIRE I VARI **RUOLI PRIVACY** AD ESEMPIO, DEGLI ENTI CHE ATTIVANO IL CANALE DI SEGNALAZIONE (ART. 13 COMMA 4 CHE INDIVIDUA IL TITOLARE DEL TRATTAMENTO) E DEI SOGGETTI CHE RICEVONO E GESTISCONO LA SEGNALAZIONE (ART. 12, COMMA 2)
  - ✓ **INDIRIZZARE L'IMPOSTAZIONE** DEL PROCESSO DI RICEVIMENTO E GESTIONE DELLE SEGNALAZIONI (AD. ES. ART. 12 COMMA 1, ART. 13 COMMI 1, 2, 6)

IL TITOLARE DEL TRATTAMENTO



- SONO **TITOLARI DEL TRATTAMENTO** I SOGGETTI DEL SETTORE PUBBLICO E PRIVATO CHE **ISTITUISCONO CANALI DI SEGNALAZIONE** INTERNI (**art. 13, comma 4 del D.lgs 24/2023**) E L'ANAC NELL'AMBITO DEL CANALE DI SEGNALAZIONE ESTERNO
- RICADE SUI **TITOLARI** LA RESPONSABILITÀ PRINCIPALE DI CONFORMARE IL CANALE DI SEGNALAZIONE ALLA NORMATIVA SULLA PROTEZIONE DEI DATI PERSONALI
- SONO I PRINCIPALI DESTINATARI DEL SISTEMA SANZIONATORIO DELLA NORMATIVA SULLA PROTEZIONE DEI DATI PERSONALI

IL RESPONSABILE DEL TRATTAMENTO

SIGNIFICATO

- «RESPONSABILE» NON SIGNIFICA «COLUI CHE RISPONDE», BENSI' «RESPONSALIZZATO», ALLA GESTIONE DI UNO O PIU' TRATTAMENTI

CHI PUO' ESSERLO

- UNA SOCIETA' ESTERNA O UN CONSULENTE CUI IL TITOLARE CHIEDE DI SVOLGERE, PER CONTO DEL TITOLARE STESSO, UNO O PIU' TRATTAMENTO

COME LO SI DIVENTA

- MEDIANTE CONTRATTO O ATTO SCRITTO DI NOMINA A RESPONSABILE («DPA»), FIRMATO DA ENTRAMBE LE PARTI (TITOLARE E RESPONSABILE)

QUANDO L'ENTE AFFIDA ATTIVITÀ CONNESSE AL CANALE DI SEGNALAZIONE INTERNO A UNO O PIÙ SOGGETTI ESTERNI ALLA SUA ORGANIZZAZIONE (ES. **FORNITORE DELLA PIATTAFORMA – GESTORE ESTERNO)**, QUESTI TRATTANO I DATI IN QUALITÀ DI RESPONSABILI DEL TRATTAMENTO (**ART. 13 COMMA 6, D.LGS 24/2023 E 28 GDPR**) E, IN QUANTO TALI, DEVONO PRESENTARE **GARANZIE SUFFICIENTI**, IN PARTICOLARE IN TERMINI DI CONOSCENZA SPECIALISTICA, AFFIDABILITÀ E RISORSE, **PER METTERE IN ATTO MISURE TECNICHE E ORGANIZZATIVE CHE GARANTISCANO LA PROTEZIONE DEI DATI**

AUTORIZZAZIONI ED ISTRUZIONI

LA NORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI PRESCRIVE CHE IL TITOLARE E IL RESPONSABILE, NELL'AMBITO DEL PROPRIO ASSETTO ORGANIZZATIVO, **FORMALIZZINO COMPITI E FUNZIONI CONNESSI AL TRATTAMENTO** DEI DATI PERSONALI AUTORIZZANDO ED ISTRUENDO LE PERSONE FISICHE CHE OPERANO SOTTO LA LORO DIRETTA AUTORITÀ

LE AUTORIZZAZIONI AL TRATTAMENTO CON RELATIVE ISTRUZIONI OPERATIVE (**art. 12 comma 2 D.lgs 24/2023)** DEVONO **RICOMPRENDERE TUTTE LE PERSONE** CHE SONO **COINVOLTE NELLA GESTIONE DELLE SEGNALAZIONI**. TALI SOGGETTI DEVONO INOLTRE RICEVERE UN'ADEGUATA E **SPECIFICA FORMAZIONE** SIA SULLA **PROTEZIONE DEI DATI** PERSONALI, SICUREZZA DEI DATI E DELLE INFORMAZIONI, **NONCHÉ SULLA POLICY WHISTLEBLOWING**

PRINCIPI DA RISPETTARE NEL TRATTAMENTO

LICEITA' E CORRETTEZZA

- BISOGNA INDIVIDUARE, QUALI SONO LE REGOLE IN VIGORE, E RISPETTARLE

FINALITA'

- BISOGNA PERSEGUIRE **FINALITA' LECITE, ESPLICITE E SPECIFICHE**, E DICHIARARLE AGLI INTERESSATI

MINIMIZZAZIONE

- **DATI ADEGUATI, PERTINENTI E LIMITATI**. I DATI CHE MANIFESTATAMENTE NON SONO UTILI AL TRATTAMENTO DI UNA SEGNALAZIONE NON SONO RACCOLTI E, SE RACCOLTI ACCIDENTALMENTE VANNO CANCELLATI SENZA RITARDO (ART. 13, COMMA 2 , D.LGS 24/2023)

ESATTEZZA

- **ASSICURARE** CHE I DATI SIANO **ESATTI E, SE NECESSARIO, AGGIORNATI**. DEVONO ESSERE ADOTTATE TUTTE LE MISURE RAGIONEVOLI PER RETTIFICARE O CANCELLARE I DATI INESATTI RELATIVI ALLA SPECIFICA SEGNALAZIONE CHE VIENE GESTITA

CONSERVAZIONE

- **CONSERVARE I DATI/DOCUMENTI** 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 (ART. 14 , COMMA 1, D.LGS 24/2023)

LA NATURA DEI TRATTAMENTI

I TRATTAMENTI DI DATI PERSONALI CONNESSI A RICEVIMENTO E GESTIONE SEGNALAZIONI SONO:

- DI **NATURA COMUNE,** EVENTUALMENTE, DI **NATURA SENSIBILE** E RELATIVI A CONDANNE PENALI E REATI (CONTENUTI NELLA SEGNALAZIONE E NEGLI ATTI AD ESSA ALLEGATI) RIFERIBILI AD INTERESSATI IDENTIFICATI O IDENTIFICABILI (SEGNALANTE, SEGNALATO, ALTRI TERZI)
- NECESSARI A DARE **ATTUAZIONE AD OBBLIGHI DI LEGGE** PREVISTI DAL D.LGS. 24/2023 LA CUI OSSERVANZA DELLE RELATIVE PRESCRIZIONI È **CONDIZIONE DI LICEITÀ** DEL TRATTAMENTO (ARTT. 6 PAR. 1, LETT. C) - 9 PAR.2 LETT. B) – 10 E 88 GDPR)
- EFFETTUATI AL SOLO SCOPO DI **DARE SEGUITO** ALLE SEGNALAZIONI (ART. 12 COMMA 1, D.LGS 24/2023)

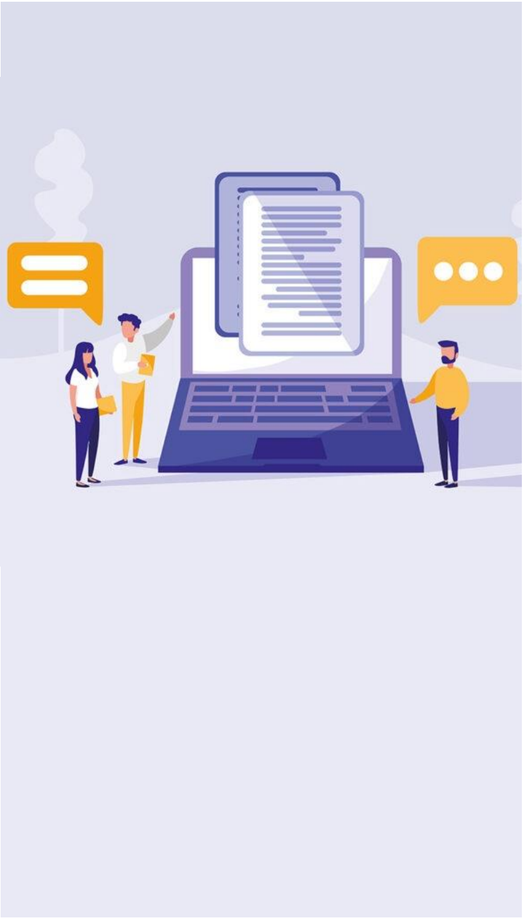
L'INFORMATIVA PRIVACY

- IL TITOLARE DEL TRATTAMENTO DEVE **RENDERE *EX ANTE*** AI POSSIBILI INTERESSATI UN'INFORMATIVA PRIVACY IN LINEA CON LE PRESCRIZIONI DEL GDPR
- I **DESTINATARI** SONO, AD ESEMPIO, I SEGNALANTI, I SEGNALATI, EVENTUALI PERSONE MENZIONATE NELLA SEGNALAZIONE
- L'INFORMATIVA PUÒ ESSERE RILASCIATA **IN ALLEGATO ALLA POLICY** WHISTLEBLOWING, **PUBBLICATA SUL SITO** WEB E/O IN APPOSITA AREA DELLA **PIATTAFORMA** DI SEGNALAZIONE, IN FORMA BREVE IN OCCASIONE DI SEGNALAZIONI ORALI O TRAMITE INCONTRO RICHIESTO DAL SEGNALANTE
- NELLA FASE DI ACQUISIZIONE DELLA SEGNALAZIONE E DELLA EVENTUALE ISTRUTTORIA NON DEVONO ESSERE FORNITE INFORMATIVE SPECIFICHE AI SOGGETTI DIVERSI DAL SEGNALANTE
- LADDOVE ALL'ESITO DELL'ISTRUTTORIA SULLA SEGNALAZIONE SI AVVII UN PROCEDIMENTO NEI CONFRONTI DI UNO SPECIFICO SOGGETTO SEGNALATO, A QUEST'ULTIMO VA RESA UN'INFORMATIVA AD HOC

L'INFORMATIVA PRIVACY

I CONTENUTI PRINCIPALI PRESCRITTI DAL GDPR

- INDICAZIONE DEL TITOLARE DEI RELATIVI DATI DI CONTATTO
- TIPOLOGIA DI DATI RACCOLTI
- FINALITÀ E MODALITÀ DEL TRATTAMENTO
- BASE GIURIDICA CHE RENDE LEGITTIMO IL TRATTAMENTO
- AMBITO DEL TRATTAMENTO E SOGGETTI CUI I DATI POSSONO ESSERE COMUNICATI (A.E. RESPONSABILI O SOGGETTI AUTORIZZATI AL TRATTAMENTO)
- TERMINI DI CONSERVAZIONE DEI DATI
- TRASFERIMENTI DI DATI ALL'ESTERO E RELATIVA BASE DI LEGITTIMITÀ
- LE MODALITÀ ED I LIMITI ALL'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI



LA LIMITAZIONE DELL'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

IL D.LGS 24/2023 HA MODIFICATO **L'ART. 2 UNDECIES COMMA 1, LETT. F**) DEL CODICE PRIVACY:

QUALORA POSSA DERIVARE UN **PREGIUDIZIO** EFFETTIVO E CONCRETO **ALLA TUTELA DELLA RISERVATEZZA DELL'IDENTITÀ DEL SEGNALANTE**, LA PERSONA COINVOLTA O IL SEGNALATO - CON RIFERIMENTO AI PROPRI DATI PERSONALI TRATTATI NELL'AMBITO DELLA SEGNALAZIONE, DIVULGAZIONE PUBBLICA O DENUNCIA - **NON POSSONO ESERCITARE** – PER IL TEMPO E NEI LIMITI IN CUI CIÒ COSTITUISCA UNA MISURA NECESSARIA E PROPORZIONATA - **I DIRITTI** CHE NORMALMENTE IL GDPR RICONOSCE AGLI INTERESSATI.

LA SICUREZZA DELLE INFORMAZIONI

- OCCORRE 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 CONFIDENZIALITÀ») (**ART. 32 GDPR**)
- I TRATTAMENTI IN ESAME SONO CARATTERIZZATI DA **ELEVATI RISCHI** PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI PERTANTO IL RICORSO A STRUMENTI DI **CRITTOGRAFIA** NELL'AMBITO DEI CANALI DI SEGNALAZIONE, SI RITIENE UNA **MISURA ADEGUATA DA ATTUARE FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA (SICUREZZA BY DESIGN E BY DEFAULT)**
- OCCORRE GARANTIRE IL DIVIETO DI TRACCIAMENTO DEI CANALI INTERNO ED ESTERNO DI SEGNALAZIONE NEL CASO IN CUI L'ACCESSO AVVENGA DALLA RETE AZIENDALE
- LE MISURE DI SICUREZZA DEVONO ESSERE PERIODICAMENTE RIESAMINATE E SE NECESSARIO AGGIORNATE

DATA PROTECTION IMPACT ASSESSMENT

COSA È? È UNA PROCEDURA PREVISTA DALL'ARTICOLO 35 DEL REGOLAMENTO UE/2016/679 (RGPD) CHE MIRA A **DESCRIVERE UN TRATTAMENTO DI DATI PER VALUTARNE LA NECESSITÀ E LA PROPORZIONALITÀ NONCHÉ I RELATIVI RISCHI,** ALLO SCOPO DI **APPRONTARE MISURE IDONEE AD AFFRONTARLI**. UNA DPIA PUÒ RIGUARDARE UN SINGOLO TRATTAMENTO OPPURE PIÙ TRATTAMENTI CHE PRESENTANO ANALOGIE IN TERMINI DI NATURA, AMBITO, CONTESTO, FINALITÀ E RISCHI.

PERCHÉ? LA DPIA È UNO STRUMENTO IMPORTANTE IN TERMINI DI **RESPONSABILIZZAZIONE (ACCOUNTABILITY)** IN QUANTO AIUTA IL TITOLARE NON SOLTANTO A **RISPETTARE LE PRESCRIZIONI DEL RGPD**, MA ANCHE AD **ATTESTARE DI AVER ADOTTATO MISURE IDONEE A GARANTIRE IL RISPETTO** DI TALI PRESCRIZIONI. IN ALTRI TERMINI, LA DPIA È UNA PROCEDURA CHE PERMETTE DI VALUTARE E DIMOSTRARE LA CONFORMITÀ CON LE NORME IN MATERIA DI PROTEZIONE DEI DATI PERSONALI.

IN CHE MOMENTO? LA DPIA DEVE ESSERE CONDOTTA **PRIMA** DI PROCEDERE AL TRATTAMENTO. DOVREBBE COMUNQUE ESSERE PREVISTO UN RIESAME CONTINUO DELLA DPIA, RIPETENDO LA VALUTAZIONE A INTERVALLI REGOLARI.

CHI? LA RESPONSABILITÀ DELLA DPIA **SPETTA AL TITOLARE**, ANCHE SE LA CONDUZIONE MATERIALE DELLA VALUTAZIONE DI IMPATTO PUÒ ESSERE AFFIDATA A UN ALTRO SOGGETTO, INTERNO O ESTERNO ALL'ORGANIZZAZIONE. IL TITOLARE NE MONITORA LO SVOLGIMENTO CONSULTANDOSI CON IL RESPONSABILE DELLA PROTEZIONE DEI DATI E ACQUISENDO - SE I TRATTAMENTI LO RICHIEDONO - IL PARERE DI ESPERTI DI SETTORE, DEL RESPONSABILE DELLA SICUREZZA DEI SISTEMI INFORMATIVI (CHIEF INFORMATION SECURITY OFFICER, CISO) E DEL RESPONSABILE IT.

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 24/2023, IL TRATTAMENTO DI GESTIONE DELLE SEGNALAZIONI **PRESENTA RISCHI SPECIFICI PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI** (CFR. 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 ART. 35 DEL GDPR)

LA CO-TITOLARITÀ

IN CASO DI CONDIVISIONE DI RISORSE PER IL RICEVIMENTO E LA GESTIONE DELLE SEGNALAZIONI, GLI ENTI INTERESSATI DALLA CONDIVISIONE TRATTANO I DATI IN QUALITÀ DI CO-TITOLARI DEL TRATTAMENTO (art. 4, comma 4 e art. 13 comma 5 del D.lgs 24/2023)

QUANDO DUE O PIÙ TITOLARI DETERMINANO CONGIUNTAMENTE LE FINALITÀ E I MEZZI DEL TRATTAMENTO (art. 26 GDPR)

SONO CO-TITOLARI DEL TRATTAMENTO

I CO-TITOLARI DEVONO DEFINIRE IN MODO TRASPARENTE MEDIANTE UN ACCORDO INTERNO, LE RISPETTIVE RESPONSABILITÀ CIRCA L'OSSERVANZA DEL GDPR

GESTIONE DEI DIRITTI DELL'INTERESSATO

RISPETTIVE FUNZIONI NELL'ATTUAZIONE GDPR

IL CONTENUTO ESSENZIALE DELL'ACCORDO È MESSO A DISPOSIZIONE DELL'INTERESSATO

L'INTERESSATO PUÒ **ESERCITARE I PROPRI DIRITTI NEI CONFRONTI DI CIASCUN TITOLARE**

LA CO-TITOLARITÀ

ALCUNI CONTENUTI DI MASSIMA DELL'ACCORDO DI CO-TITOLARITÀ

- DEFINIZIONE DELL'**AMBITO** DI CO-TITOLARITÀ (A.E. MEZZI DI TRATTAMENTO E MODALITÀ)
- CHI ESEGUE **LA DPIA**
- CHI SI OCCUPA DELLA VERIFICA/IMPLEMENTAZIONE DELLE MISURE TECNICHE ED ORGANIZZATIVE ADEGUATE A GARANTIRE LA SICUREZZA DEL TRATTAMENTO
- **CHI SI OCCUPA DI FORMALIZZARE LE NOMINE A RESPONSABILE** DEI TERZI CUI SI AFFIDANO ATTIVITÀ DI TRATTAMENTO DATI PER CONTO DEI CO-TITOLARI CON PARTICOLARE ATTENZIONE MISURE TECNICHE/ORGANIZZATIVE E **SEGREGAZIONE DELLE SEGNALAZIONI** RIFERITE A CIASCUN CO-TITOLARE
- CHI **FORMALIZZA LE AUTORIZZAZIONI/ISTRUZIONI** PER IL TRATTAMENTO DA INDIRIZZARE AI GESTORI DELLE SEGNALAZIONI
- CHI SI OCCUPA DI **DEFINIRE LE INFORMATIVE PRIVACY**
- CHI FUNGE DA **PUNTO DI CONTATTO** PER LA GESTIONE DELLE RICHIESTE DI ESERCIZIO DEI DIRITTI DEGLI INTERESSATI
- MODALITÀ DI GESTIONE DI **EVENTUALI DATA BREACH**

IL REGISTRO DEI TRATTAMENTI

- IL TITOLARE, IL RESPONSABILE ED I CO-TITOLARI **DOVRANNO AGGIORNARE** I RISPETTIVI REGISTRI DEI TRATTAMENTI
- IL REGISTRO È UNO STRUMENTO UTILE PER DISPORRE DI UN **QUADRO AGGIORNATO DEI TRATTAMENTI** DI DATI EFFETTUATI DA UN ENTE IN QUALITA' DI TITOLARE O RESPONSABILE
- **CONTENUTI DEL REGISTRO** RIFERITE AI TRATTAMENTI DI RACCOLTA E GESTIONE DELLE SEGNALAZIONI
  - ✓ DATI DI CONTATTO
  - ✓ FINALITÀ
  - ✓ CATEGORIE DI DATI E CATEGORIE DI INTERESSATI
  - ✓ AUTORITÀ COMPETENTI CUI LE SEGNALAZIONI, DIVULGAZIONI PUBBLICHE O DENUNCE VENGONO INOLTRATE
  - ✓ EVENTUALI TRASFERIMENTI ESTERI
  - ✓ RESPONSABILI DEL TRATTAMENTO COINVOLTI
  - ✓ TERMINI DI DATA RETENTION
  - ✓ DESCRIZIONE SINTETICA DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE APPLICATE
- IL REGISTRO DEI TRATTAMENTI DEVE ESSERE ESIBITO SU RICHIESTA DEL GARANTE