saev group

Corso di formazione privacy e sicurezza sul lavoro

ORDINE DEI DOTTORI AGRONOMI E DOTTORI FORESTALI DELLE MARCHE

PRIVACY
PROTEZIONE DEI DATI PERSONALI

IL NUOVO REGOLAMENTO EUROPEO N. 679/2016

4 MAGGIO 2016
Pubblicazione nella Gazzetta Ufficiale dell'Unione Europea

25 MAGGIO 2016
Entrata in vigore

I 28 Paesi Membri iniziano il processo di adeguamento

25 MAGGIO 2018

IL REG. (U.E.) N. 679/2016 DIVENTA *ESECUTIVO!*

Consulente Privacy e Privacy Officer
Certificato Dott. Stefano Vecchi CDP N° 80

ATTENZIONE!!!

Il nuovo Regolamento europeo n. 679/2016 abroga SOLTANTO la Dir. (C.E.) n. 46/1995, c.d. *Direttiva madre*:

IL D.LGS. N. 196/2003, RUBRICATO *CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI,*

RESTA *IN VIGORE!*

Il Legislatore non impone più il rispetto di misure minime di sicurezza

[CIVIL LAW]

MA

Richiede una partecipazione proattiva del Titolare del Trattamento che, conoscitore effettivo della propria realtà è chiamato a valutare l'ADEGUATEZZA e l'EFFICACIA delle misure

[COMMON LAW]

Dato Personale

Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Categorie particolari di dati personali (art. 9)

Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Dato Genetico:
I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Dato Biometrico:
I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati relativi alla salute:
I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

MI INTERESSA??

RIGUARDA CHIUNQUE FACCIA

TRATTAMENTO DEI DATI

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzatiati e applicate a dati personali o insiemi di dati personali, come la RACCOLTA, la REGISTRAZIONE, l'ORGANIZZAZIONE, la STRUTTURAZIONE, la CONSERVAZIONE, l'ADATTAMENTO o la MODIFICA, l'ESTRAZIONE, la CONSULTAZIONE, l'USO, la COMUNICAZIONE MEDIANTE TRASMISSIONE, DIFFUSIONE o qualsiasi altra forma messa a disposizione, il RAFFRONTO o l'INTERCONNESSIONE, la LIMITAZIONE, la CANCELLAZIONE o la DISTRUZIONE.

Esame dei soggetti interessati:

TITOLARE DEL TRATTAMENTO

Persona fisica o giuridica, pubblica o privata che determina le finalità e i mezzi del trattamento dei dati personali

INTERESSATO

Persona fisica a cui si riferiscono i dati personali trattati

RESPONSABILE DEL TRATTAMENTO

Persona fisica/giuridica che può essere interno od esterno, designato tramite atto formale dal Titolare del trattamento che tratta dati personali per conto del Titolare

RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI:

È la nuova figura di garanzia per l'Autorità Garante e per il Titolare del Trattamento.

Conoscenza specialistica in materia di protezione dei dati personali e capacità di assolvere i compiti di cui all'art. 39 Reg.UE 679/2016

Incaricati del trattamento:

Il D.Lgs 196/03 prevedeva: ⟺ **Il Regolamento:**

(Art. 30) INCARICATI

La **designazione** è effettuata per i**scritto**;
Individua l'ambito del **trattamento consentito**;
Deve **attenersi alle istruzioni** impartite dal **Titolare** o dal responsabile

Non vi è una definizione specifica di tale figura, ma ne prevede comunque l'esistenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del responsabile (art. 4, n. 10 – art. 32, paragrafo 4)

Almeno **annualmente** deve essere **aggiornata la lista degli incaricati,** con individuazione dell'ambito del trattamento consentito agli stessi

DIRITTI PIU' AMPI RICONOSCIUTI ALL'INTERESSATO :

ACCESSO

Art. 15 GDPR

CANCELLAZIONE
LIMITAZIONE

Art. 16-17-18 GDPR

PORTABILITA' DEI DATI

Art. 20 GDPR

TRASPARENZA

Con riferimento al Trattamento dei dati il Legislatore UE richiede che l'INFORMATIVA all'interessato siano:

LINGUAGGIO
SEMPLICE E CHIARO

ELEMENTI
. FINALITA' DEL TRATTAMENTO
. PERIODO DI CONSERVAZIONE
. DIRITTO DI RECLAMO ALL'AUTORITA' DI CONTROLLO
. EVENTUALE TRASFERIMENTO DEI DATI IN PAESI TERZI

FORMA
SCRITTA
(la forma orale è ammessa solo quando possa essere in ogni caso comprovata con altri mezzi l'identità dell'interessato)

CONDIZIONI PER IL CONSENSO

INEQUIVOCABILE

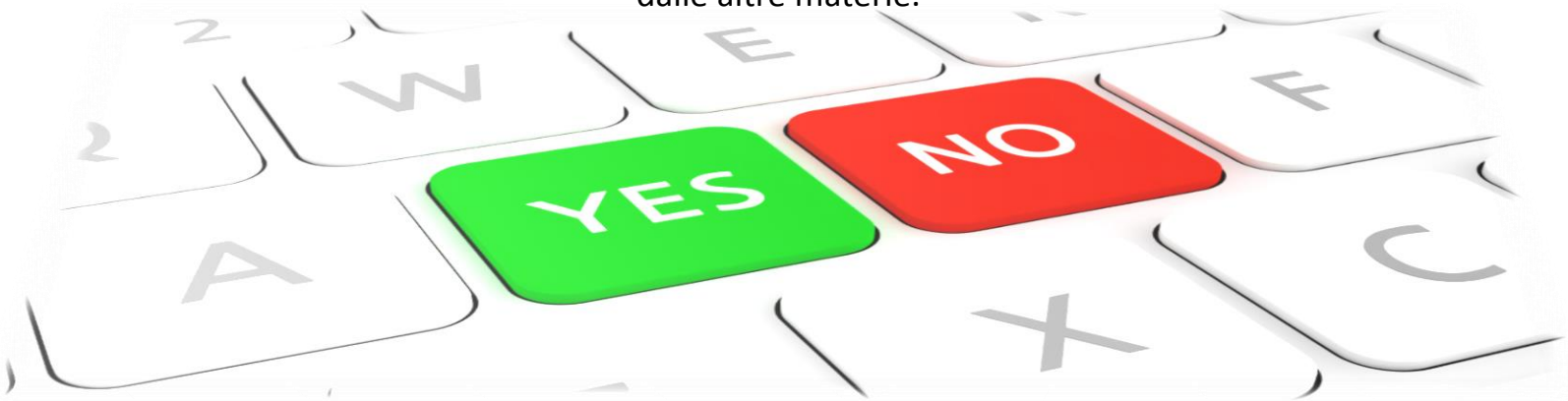
Qualsiasi manifestazione di volontà libera, specifica, informata con il quale l'interessato manifesta il proprio assenso

GRANULARE

Quando il consenso sia fornito in una dichiarazione scritta che riguardi anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie.

REVOCABILE

Il diritto di revoca è previsto in ogni momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.



DOVERI PIU' STRINGENTI RICONOSCIUTI AI SOGGETTI OBBLIGATI :

PRIVACY by **DESIGN** / PRIVACY by **DEFAULT**

ANALISI DEI RISCHI

REGISTRO DEI **TRATTAMENTI**

MISURE DI SICUREZZA

ACCOUNTABILITY

Art. 25 GDPR
Nuovo concetto **PRIVACY BY DESIGN E PRIVACY BY DEFAULT**

<<Responsabilizzazione>> delle figure principali del trattamento

adottare e rendere evidenza di comportamenti proattivi

tali da dimostrare la concreta adozione di misure adeguate finalizzate ad assicurare l'applicazione del regolamento.

Implementare procedure ufficiali che prevedano anche:

- L'attuazione di VALUTAZIONE D'IMPATTO (se ed in che termini si rendano necessarie) ;
- Elaborazione di POLICY DI STUDIO, piani di formazione delle risorse interne che trattano dati, piani di audit;
- Redazione di STANDARD DI RISPOSTA ad eventuali richieste degli interessati;
- Previsione di un PIANO DI COMUNICAZIONE di violazioni dei dati personali;
- Definizione delle MISURE DI SICUREZZA(**ADEGUATE**).

Art. 30 GDPR

IL REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Ogni Titolare del Trattamento e, ove applicabile il suo Rappresentante, tengono un Registro delle attività svolte sotto la propria responsabilità.

OBBLIGATORIO PER :

- aziende > 250 dipendenti
- trattamento dati sensibili
- trattamento dati giudiziari

Il Registro delle attività prevede la mappatura dei trattamenti precisando per ciascuno di essi l'origine e la natura dei dati, le modalità e le finalità di trattamento, i tempi di conservazione, la loro eventuale comunicazione a soggetti terzi, le categorie di interessati, e una descrizione generale delle misure di sicurezza per ciascuna macro area.

Art. 33-34 GDPR

OBBLIGO DI DATA BREACH

Lo scopo è quello, in caso di violazione , di permettere all'Autorità di controllo di attivarsi senza ritardo in modo da valutare la gravità della violazione e la tipologia di misure da imporre al Titolare.

RESPONSABILE → **TITOLARE** → **AUTORITA' DI CONTROLLO**

- Natura della violazione
- Natura dei dati
- Numero di interessati
- Nome e contatto del Resp. o di altro referente
- Descrizione delle probabili conseguenze

Max. 72 h

CONSEGUENZA DELLA VIOLAZIONE

Rischio elevato per i diritti e le libertà delle persone fisiche

COMUNICAZIONE ALL'INTERESSATO
termini chiari/ fruibili

- il titolare del trattamento ha messo in atto le misure tecniche ed organizzative necessarie alla protezione dei dati violati (es. la cifratura)
- adozione di misure atte a scongiurare il sopraggiungere di un rischio elevato per diritti e libertà dell'interessato
- la comunicazione al singolo interessato risulterebbe troppo gravosa = **COMUNICAZIONE PUBBLICA**

NON SI PROCEDE ALLA COMUNICAZIONE ALL'INTERESSATO

Art. 35 GDPR

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Procedura volta alla descrizione di un trattamento per valutarne la necessità e la proporzionalità nonché i relativi rischi

SCELTA CONSEPEVOLE ED INFORMATA DELLE MISURE IDONEE AD AFFRONTARLI

Responsabile della DPIA è il Titolare che dovrebbe condurla PRIMA di procedere al trattamento.

E' UNO STRUMENTO DI ACCOUNTABILITY IN QUANTO E' PROVA DI IMPEGNO E GARANZIA DA PARTE DEL TITOLARE

D.P.I.A. OBBLIGATORIA
Art. 35 GDPR

- Valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basato su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- Trattamento su larga scala di dati sensibili/ giudiziari;
- Sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

LINEE GUIDA WP 29 [4 ottobre 2017] :

LA D.P.I.A. NON E' NECESSARIA PER I TRATTAMENTI CHE

- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- -fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui la definizione è stata condotta una DPIA

LE MISURE DI SICUREZZA

Non più misure MINIME → MISURE ADEGUATE AL RISCHIO DEL TRATTAMENTO

Dopo il 25 maggio cioè non potranno sussistere OBBLIGHI GENERALIZZATI DI ADOZIONE DI MISURE MINIME di sicurezza poiché le misure dovranno "GARANTIRE UN LIVELLO DI SICUREZZA ADEGUATO AL RISCHIO" DEL TRATTAMENTO (art. 32, paragrafo 1);
La valutazione di ADEGUATEZZA sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento.

BUONE PRASSI

LINEE GUIDA

SCHEMI DI CERTIFICAZIONE

CODICI DI CONDOTTA

…UNA NUOVA INFRASTRUTTURA DEL SISTEMA PRIVACY
CON NUOVI STRUMENTI E NUOVE FIGURE…

IL DATA PROTECTION OFFICER

è il RESPONSABILE DELLA PROTEZIONE DATI

Artt. 37 ss. Reg. UE 679/2016

NOMINA OBBLIGATORIA

- Il trattamento è effettuato da un Soggetto Pubblico
- le **attività principali** di trattamento consistono in trattamenti che - per natura, ambito di applicazione e/o finalità - richiedono **il monitoraggio regolare e sistematico degli interessati su LARGA SCALA**
- Le attività principali consistono nel trattamento, su larga scala di particolari categorie di dati

Da non confondere con il Responsabile del Trattamento!!!

IL RUOLO (art. 38)

Non riceve istruzioni per l'espletamento dei suoi compiti

Riferisce direttamente al vertice gerarchico dell'organizzazione

Deve essere coinvolto in ogni questione inerente la protezione dei dati

Per l'espletamento dei suoi compiti non può essere penalizzato né rimosso

Ha accesso alle risorse umane e finanziarie necessarie all'espletamento del ruolo

- **INDIPENDENTE**
- **COMPETENTE**
- **VINCOLATO ALLA RISERVATEZZA**

COOPERA CON L'AUTORITA' E PER QUESTA FUNGE DA PUNTO DI CONTATTO PER LE VARIE QUESTIONI/ DATI

INFORMA E FORNISCE SUPPORTO E CONSULENZA ALL'ORGANIZZAZIONE IN RIF. AGLI OBBLIGHI RELATIVI ALLA PROTEZIONE DEI DATI

SORVEGLIA L'OSSERVANZA DELLE DISPOSIZIONI ALL'INTERNO DELL'ORGANIZZAZIONE

FORNISCE UN PARERE IN MERITO ALLA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

E' una **figura di garanzia** ed è designato in funzione delle **qualità professionali**, in particolare della **conoscenza specialistica** della normativa e delle prassi in materia di protezione dei dati, e delle capacità di assolvere i compiti di cui all'art. 39 del Reg. UE 679/16.

Con il Regolamento Europeo cambia veramente tutto??

NO, perché oltre al Codice della Privacy che come già detto rimane in vigore, applicabili in toto rimangono anche specifici provvedimenti del Garante riferiti a particolari settori.

PROVVEDIMENTI DEL GARANTE

- AMMINISTRATORE DI SISTEMA

- VIDEOSORVEGLIANZA

- DISCIPLINARE POSTA ELETTRONICA ED INTERNET

-ADEGUAMENTO DEL SITO

- RAEE

QUALI LE SANZIONI?

ART. 83 Reg.UE

Nella definizione/ applicazione della sanzione l'Autorità è chiamata a tener conto di taluni elementi es:

- NATURA DELLA VIOLAZIONE
- GRAVITA' DELLA VIOLAZIONE
- L'OGGETTO O A FINALITÀ DEL TRATTAMENTO IN QUESTIONE
- IL NUMERO DI INTERESSATI LESI DAL DANNO E IL LIVELLO DEL DANNO DA ESSI SUBITO
- CARATTERE DOLOSO/COLPOSO DELLA VIOLAZIONE

QUANTO E COSA SOPRATTUTTUTOIL RESPONSABILE HA FATTO PER EVIATRE L'AGGRAVAMENTO DELLA VIOLAZIONE E LE MISURE DI SICUREZZA APPLICATE

Tra le sanzioni pecuniarie più specificatamente definite:

SANZIONI COMUNQUE
. EFFETTIVE
.PROPORZIONATE
.DISSAUSIVE

Co.4) Sanzioni amministrative pecuniarie fino a 10.000.000 EUR o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente in caso di violazioni di

- art.8 (MINORI)
- art. 11 (SULLA IDENTIFICAZIONE DELL'INTERESSATO)
- Art. da 25 a 39 (OBBLIGHI PROPRI DEL RESP. DEL TRATTAMENTO E DEL D.P.O.)
- Art. 42 e 43 (CERTIFICAZIONE ED ORGANISMI DI CERTIFICAZIONE)

Co.5) Sanzioni amministrative pecuniarie fino a 20.000.000 EUR o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente in caso di violazioni di:

-PRINCIPI BASE DEL TRATTAMENTO
-DIRITTI DELL'INTERESSATO
-TRASFERIMENTI DI DATI PERSONALI ALL'ESTERO
-VIOLAZIONE DI OBBLIGHI DI DIVIETO O INTERRUZIONE DI FLUSSI DI DATI

…COSA FARE QUINDI A PARTIRE DA DOMANI ???

1 **ASSESSMENT**

Il primo passo per l'adeguamento è l' Assessment, cioè l'individuazione di tutti i trattamenti di dati personali effettuati e i processi attuati dall'azienda al fine di verificare quale è ad oggi lo stato di conformità con la nuova normativa che introduce concetti e criteri differenti dal D.Lgs 196/03 e analizzare puntualmente quelle che sono le azioni correttive da pianificare.

2 ANALISI DEI RISCHI

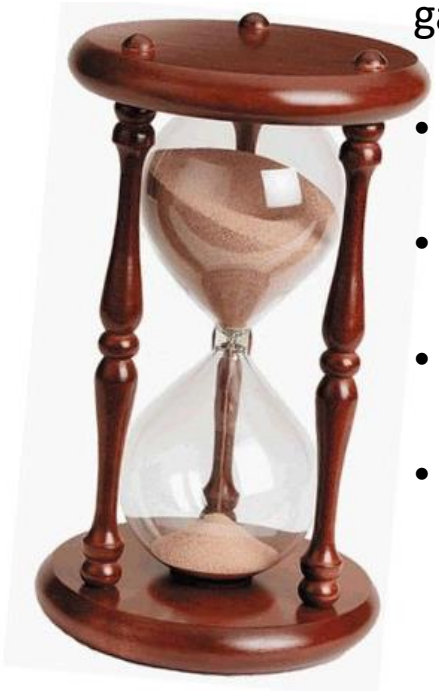
Il Titolare in virtù delle posizioni di garanzia che rivestono sono chiamati ad elaborare una attenta analisi dei rischi in riferimento alle vulnerabilità aziendali nello svolgimento delle attività di trattamento dei dati personali.

Un'analisi dei rischi efficace ed efficiente DEVE:

- Definire puntualmente il livello di rischio
- Essere specifica per ogni processo aziendale e ambito di applicazione;
- Individuare tutti i rischi correlati alle attività di trattamento dei dati da voi svolti;
- **Monitorare periodicamente lo stato di adeguamento alla normativa il relazione ai rischi**

Risultato dell'analisi dei rischi è la presa di coscienza dello stato attuale di rischio per l'azienda, la conseguente scelta consapevole delle misure adeguate da applicare e l'elaborazione di un piano di adeguamento costante.

3 REVISIONE DI INFORMATIVE E NOMINE



Revisionare la documentazione in modo da garantire:

- Aggiornamento delle informative agli interessati;
- Gestione conforme del consenso sia nei moduli cartacei che informatici;
- Revisione delle nomine formali (ex. D.lgs. 196/03) eventualmente già presenti;
- Revisione delle clausole sulla protezione dei dati nei contratti con fornitori, partners, dipendenti, collaboratori e clienti.

4 FORMAZIONE

Definire un piano di formazione continuo e specifico per le varie mansioni che accresca e mantenga le competenze del personale deputato alle attività di trattamento.

SICUREZZA NEI LUOGHI DI LAVORO

CHI SI DEVE ADEGUARE E QUALI SONO GLI OBBLIGHI DI LEGGE

- **La normativa si applica a tutti i settori di attività, privati e pubblici e a tutte le tipologie di rischio**
- **A tutti i lavoratori e le lavoratrici subordinati ed autonomi nonché verso quei soggetti ad essi equiparati**

LAVORATORE: Art. 2 comma 1 lettera a) "persona che, indipendentemente dalla tipologia contrattuale, svolge una attività lavorativa nell'ambito dell'organizzazione di un datore di lavoro pubblico o privato, con o senza retribuzione, anche al solo fine di apprendere un mestiere, un'arte o una professione…."

EQUIPARATI: Il socio lavoratore di cooperative o di società, anche di fatto; il soggetto beneficiario delle iniziative di tirocini formativi e di orientamento di cui all'art. 18 della legge 24/06/1997 n. 196; l'allievo degli istituti di istruzione ed universitari e il partecipante ai corsi di formazione professionale nei quali si faccia uso di laboratori, attrezzature di lavoro in genere, agenti chimici, fisici e biologici, ivi comprese le apparecchiature fornite di videoterminali

CHI SI DEVE ADEGUARE E QUALI SONO GLI OBBLIGHI DI LEGGE

Gli adempimenti previsti dalla normativa sono:

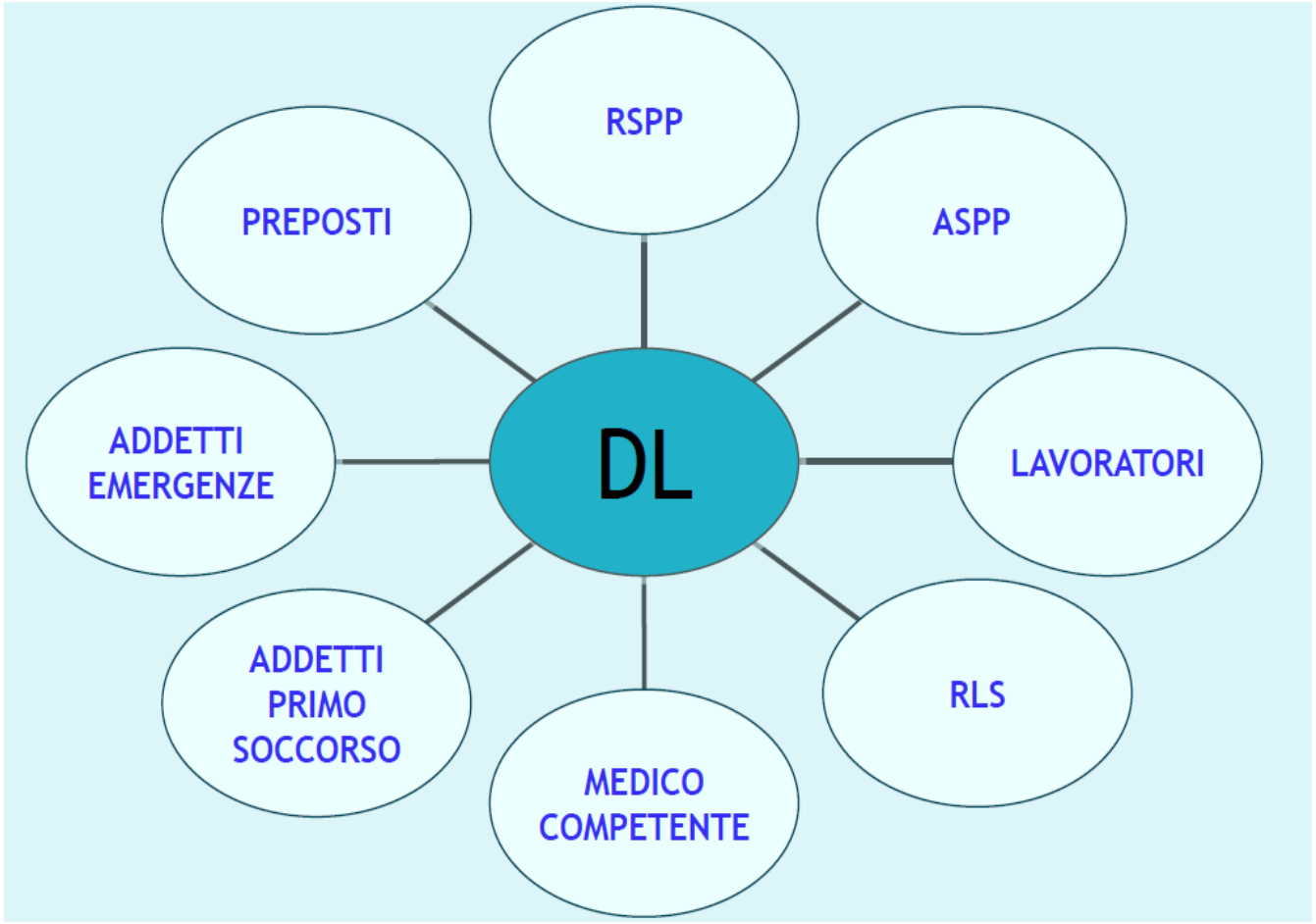
- **La valutazione di tutti i rischi e l'elaborazione del relativo documento;**
- **La designazione e la formazione dell' R.S.P.P.;**
- **La nomina del medico competente, ove previsto;**
- **Designazione preventiva dei lavoratori incaricati all'attuazione delle misure di sicurezza (Responsabile delle Emergenze, Addetto Antincendio, Addetto Primo Soccorso);**
- **Fornire ai lavoratori i necessari ed idonei dispositivi di protezione individuale;**
- **Assicurare a ciascun lavoratore una formazione sufficiente ed adeguata in materia di salute e sicurezza negli ambienti di lavoro;**
- **Consegnare tempestivamente al rappresentante dei lavoratori per la sicurezza, copia del documento relativo alla valutazione dei rischi**

CHI SI DEVE ADEGUARE E QUALI SONO GLI OBBLIGHI DI LEGGE

Gli adempimenti previsti dalla normativa sono:

- **Adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei luoghi di lavoro**
- **Nelle aziende con più di 15 lavoratori, convocare la riunione periodica prevista dalla normativa;**
- **Comunicare all'INAIL i nominativi dei rappresentanti dei lavoratori per la sicurezza;**
- **Vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità;**
- **……..**

LE PRINCIPALI FIGURE DELLA SICUREZZA



COME RIDURRE IL TASSO INAIL CON IL MODELLO OT24

L'INAIL offre l'opportunità di ottenere una riduzione del premio annuale alle imprese che hanno effettuato nell'anno solare precedente investimenti volti a migliorare la salubrità degli ambienti lavorativi e la sicurezza delle condizioni di lavoro, attraverso la presentazione di una domanda su apposito modello.

ESEMPIO RIDUZIONE 2017

Lavoratori-Anno	Riduzione
Fino a 10	28%
Da 11 a 50	18%
Da 51 a 200	10%
Oltre 200	5%

…GRAZIE PER L'ATTENZIONE !!