GDRP: IL NUOVO REGOLAMENTO UE NR.679/2016 IN MATERIA DI PRIVACY

ANCE VENETO

PADOVA

SCUOLE EDILI

21.03.2018

GIOVANNI TRETTI - SUSANNA GREGGIO
STUDIO LEGALE GTA

REGOLAMENTO UE 2016/679

- REGOLAMENTO UE 2016/679
- Attualmente in vigore
- Applicabile a decorrere dal 25 maggio 2018 in tutti gli Stati membri
- Protezione delle persone fisiche con riguardo al trattamento dei dati personali e libera circolazione di tali dati
- abroga la Direttiva 95/46/CE
- è direttamente applicabile in ciascuno degli stati membri
- Italia: Codice Privacy (D. Lgs. 196/2003)

Legge 25 ottobre 2017 n. 163

Legge delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione Europea;

Art. 13: Delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679:

- Abrogare disposizioni del codice privacy incompatibili con il Regolamento
- Modificare il codice per quanto necessario a dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento
- Emanare specifici provvedimenti attuativi ed integrativi

I PROVVEDIMENTI ITALIANI

- adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento(UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse.

- Tempi: sei mesi dal 25 ottobre 2017

I PROVVEDIMENTI ITALIANI

Legge 20 novembre 2017 n. 167 - Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea

- Modifica art. 29 Codice Privacy sul Responsabile del trattamento

- Il Garante è intervenuto negli anni con Linee Guida, Provvedimenti e decisioni che sono tuttora punto di riferimento per gli addetti ai lavori
- Es: Provvedimento in materia di videosorveglianza - 8 aprile 2010

Diritto alla Riservatezza

- diritto di nuova formazione: art. 13 Cost.: libertà personale; art. 14: inviolabilità del domicilio; art. 15: segretezza della corrispondenza; art. 2: diritti inviolabili dell'uomo

- descritto dalla dottrina come il diritto a tenere segreti aspetti, comportamenti, atti, relativi alla sfera intima della persona, impedendo che tali informazioni vengano divulgate senza l'autorizzazione del soggetto interessato

AMBITO DI APPLICAZIONE TERRITORIALE

Il Regolamento riguarda il Trattamento di dati personali di **residenti nell'unione Europea** effettuato:
- nell'ambito delle attività di uno stabilimento da parte del Titolare / Responsabile del trattamento nell'Unione, **indipendentemente dal fatto che il trattamento sia effettuato nell'Unione**

STABILIMENTO: implica effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tal riguardo, non è determinante la forma giuridica assunta, sia essa succursale o filiale dotata di personalità giuridica.

AMBITO DI APPLICAZIONE TERRITORIALE

ECCEZIONI:

a) Offerta di beni o prestazione di servizi agli interessati;
b) Monitoraggio del loro comportamento:

Anche se titolare o Responsabile non stabiliti nell'UE

RAPPRESENTANTE

Persona fisica o giuridica stabilita in uno degli Stati membri in cui si trovano gli interessati e i cui dati personali sono trattati nell'ambito dell'offerta di beni o servizi o il cui comportamento è monitorato.

Designata dal titolare o dal Responsabile

Sono salve le azioni legali che potrebbero essere promosse contro il Titolare od il Responsabile

I SOGGETTI – L'ORGANIGRAMMA

- Titolare (contitolari) e titolare autonomo
- Rappresentante stabilito
- Responsabili interni
- Responsabili esterni
- Incaricati (autorizzati) del trattamento
- (Amministratore di sistema)
- Data protection officer
- Interessati al trattamento

Privacy by Design

Il Titolare mette in campo misure tecniche e organizzative adeguate

Necessarie garanzie per soddisfare il Regolamento e tutelare i diritti dell'Interessato

Pseudonimizzazione (minimizzazione) (individuazione solo tramite informazioni aggiuntive) === Principio di Necessità Codice Privacy

Quando?

Fin dalla Progettazione e di default

Come?

tenendo conto dello stato dell'arte e dei costi di attuazione, della natura, ambito, contesto e finalità del trattamento

PROCESSO COMPLESSIVO DI MISURE

1) Giuridiche (es: Regolamento UE; Redazione modello Protezione dei Dati)
2) Organizzative (procedure interne, regolamenti aziendali)
3) Tecniche (misure di sicurezza adeguate)

anche attraverso l'elaborazione di specifici modelli organizzativi



La gestione del Sistema Protezione dei dati: SGPD

✔**CONFORMITA'**: prerequisito fondamentale di un SGPD è la conformità alle leggi e alla normativa nazionale ed europea. Eventuali conformità a NORME ISO potranno essere un ulteriore obiettivo da perseguire.

✔**GOVERNANCE**: la definizione di politiche, di processi e di momenti di controllo supporta la creazione di una cultura condivisa e favorisce la sensibilizzazione del personale e la responsabilizzazione del management in materia di protezione dei dati personali.

✔**BUSINESS**: l'esistenza di un SGPD consolida la fiducia dei clienti, fornitori e partner e aumenta il loro grado di soddisfazione nei confronti dell'azienda.

STUDIO LEGALE GTA

Compliance

➔D. LGS. nr. 231/2001: Responsabilità amministrativa degli enti

➔QUALITA': ISO 9001/2015

➔AMBIENTE - SALUTE E SICUREZZA: ISO 14001; OHSAS 18001

➔PROTEZIONE DEI DATI: (ISO 27001 Sicurezza delle informazioni)

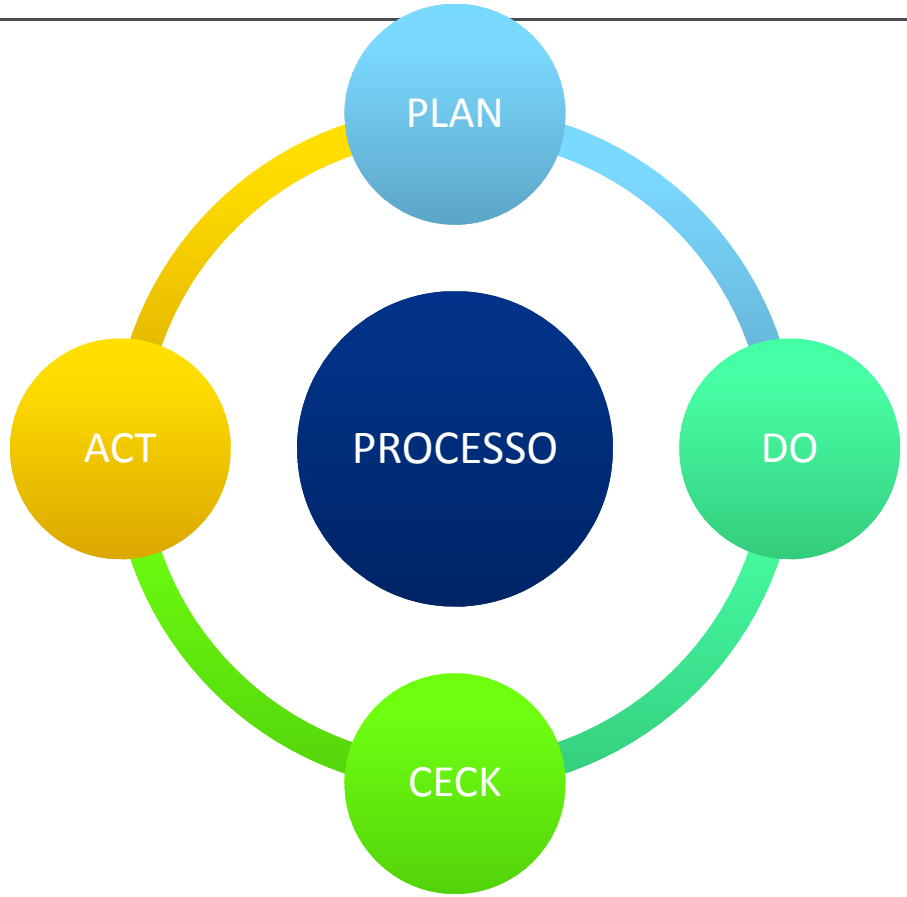
VERSO UN SISTEMA DI GESTIONE INTEGRATO

STUDIO LEGALE GTA

ACCOUNTABILITY

attraverso la costituzione di un sistema privacy, in particolare per mezzo del monitoraggio e del miglioramento continuo, il Titolare del trattamento è in grado di dimostrare di avere adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi.

Processo



PDCA

Pianificazione e progettazione con particolare attenzione alla valutazione del rischio; implementazione, monitoraggio, mantenimento e miglioramento

VIOLAZIONE DEI DATI PERSONALI

la 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

RUOLI AZIENDALI PROTEZIONE DEI DATI

RESPONSABILE (RESPONSABILE ESTERNO)

TITOLARE (CONTITOLARE)

INCARICATO

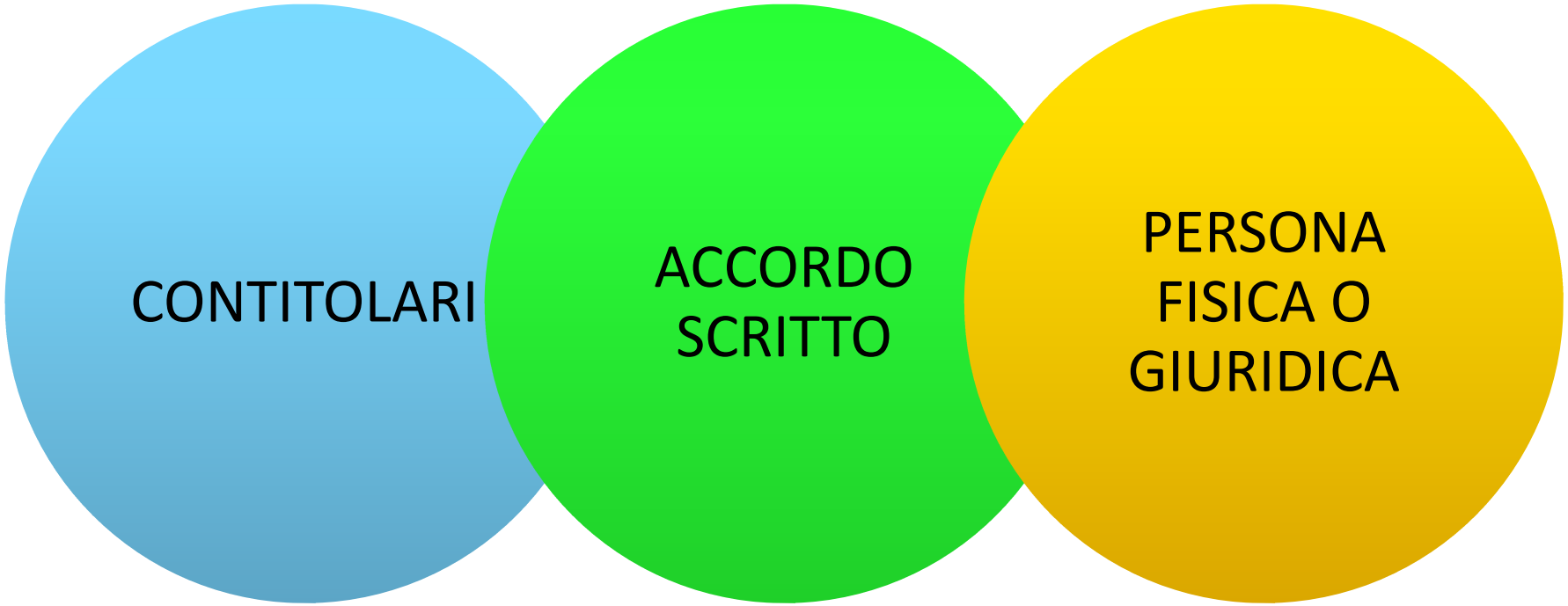
RUOLI AZIENDALI PROTEZIONE DEI DATI

AMMINISTRATORE DI SISTEMA

RESPONSABILE PROTEZIONE DATI

SECURITY MANAGER

Data Controller (Titolare del trattamento)



(Data Processor) Responsabile del trattamento

Incaricato

Informazione e accesso ai dati personali

INFORMATIVA EX ART. 13

Responsabile della protezione dei dati (DPO)

QUANDO E' OBBLIGATORIO?

a) il trattamento è effettuato nel settore pubblico

b) le attività principali consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10

Compiti del DPO

Riferisce ai vertici aziendali

Informa e fornisce consulenza al titolare del trattamento o al responsabile ed ai dipendenti

Sorveglia l'osservanza del Regolamento, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti

Fornisce un parere, se richiesto, in merito alla VALUTAZIONE D'IMPATTO sulla protezione dei dati

coinvolto in tutte le questioni riguardanti la protezione dei dati personali

Quali caratteristiche deve avere il DPO?

Conoscenza approfondita della normativa sulla protezione dei dati

Può svolgere altri compiti purchè in assenza di conflitto di interessi

Capacità di effettuare ispezioni

Obbligo di segreto o riservatezza

Quali sono i compiti del Titolare verso il DPO?

Fornirgli le risorse necessarie per assolvere ai propri compiti ed accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica

Assicurarsi che il DPO non riceva istruzioni per assolvere ai propri compiti

Data Breach

In caso di violazione dei dati personali, il titolare notifica la violazione all'Autorità di controllo, senza ingiustificato ritardo, e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza (se oltre deve essere corredata dai motivi del ritardo)

A meno che:

Sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche

Cosa deve documentare il titolare?

Qualsiasi violazione di dati personali, le circostanze relative, le conseguenze ed i provvedimenti adottati per porvi rimedio

Il Titolare informa altresì l'Interessato, se vi è rischio elevato per i diritti e le libertà delle persone fisiche

Registri delle attività di trattamento

Contengono il quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio

devono avere forma scritta, anche elettronica, e devono essere esibiti su richiesta al Garante

sono parte integrante di un sistema di corretta gestione dei dati personali.

250 dipendenti o a prescindere dalle dimensioni dell'organizzazione?

Registri delle attività di trattamento

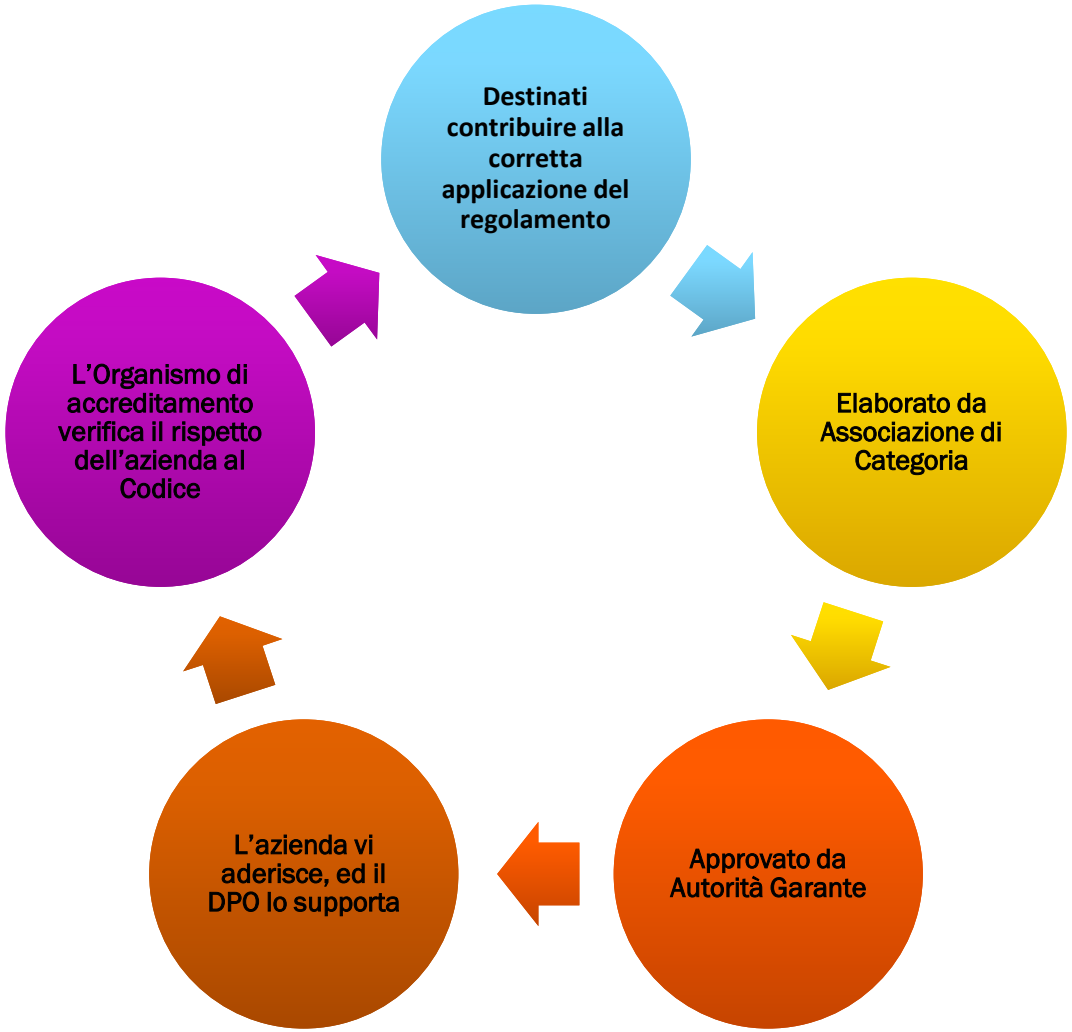
a) Il Registro del Titolare deve contenere

- Le finalità del trattamento
- Categorie di interessati e dei dati personali
- Categorie di destinatari dei dati
- Trasferimenti verso paesi terzi
- Ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative

b) Il Registro del Responsabile deve contenere

Le categorie di trattamenti effettuati per conto di ogni titolare del trattamento

Codice di condotta: sistema di autoregolamentazione



Sistemi di autoregolamentazione volontaria

meccanismi di certificazione dei propri trattamenti (norma ISO / IEC 17065:2012 prodotto, processo e servizio?) – sigilli e marchi di protezione dei dati

attraverso il controllo della conformità ad un codice di condotta effettuato da un organismo accreditato

allo scopo di dimostrare la conformità al Regolamento dei trattamenti effettuati

sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese

l'Autorità ne tiene conto, per esempio, nell'applicare eventuali sanzioni o nell'analizzare la correttezza di una valutazione di impatto effettuata dal Titolare

MISURE DI SICUREZZA

- Cosa sono le Misure di Sicurezza?

  Misure tecniche (protezione patrimonio informatico)

organizzative (adozione modelli e procedure organizzative)

preventive utili per ridurre al minimo il pericolo di perdita, distruzione o comunque qualsiasi trattamento illecito dei dati

GDPR: MISURE DI SICUREZZA ADEGUATE – ART. 32

- Tenendo conto dello stato dell'arte e dei costi di attuazione, nonchè della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche
- nessun rilievo sui soggetti preposti ad attività strategiche come quelle che si consumano in campo informatico

Provvedimento del Garante Privacy del 27.11.2008 sull'Amministratore di Sistema

- Figura professionale in ambito informatico finalizzata alla gestione e manutenzione di un impianto di elaborazione o di sue componenti (ora All. B Codice Privacy: - misure minime di sicurezza - operazioni di backup, recovery dei dati, custodia delle credenziali, gestione dei sistemi di autenticazione ed autorizzazione)
- Concreta capacità, per atto intenzionale ma anche per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati personali cui non si è legittimati ad accedere rispetto ai profili di autorizzazione attribuiti

Provvedimento del Garante Privacy del 27.11.2008 sull'Amministratore di Sistema

- Valutazione delle caratteristiche soggettive: esperienza, capacità ed affidabilità – soggetto qualificato e rapporto fiduciario
- Designazione individuale che comprenda l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato
- Operato oggetto di verifica una volta l'anno da parte del Titolare del Responsabile

AMMINISTRATORE DI SISTEMA

- laddove l'attività degli AdS, anche solo indirettamente, può riguardare servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati, nella qualità di datori di lavoro, devono rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. La cautela si spiega per l'osservanza degli obblighi che incombono sui Titolari in ragione dell'art. 4 dello Statuto dei lavoratori (Legge n. 300/1970), oggi modificato dal D.lgs. n. 151/2015, in merito al controllo a distanza dei lavoratori (e, in particolare, al divieto di controllo occulto).

Dati sensibili: definizione

Sono dati personali idonei a rivelare (art. 4 co. 1 lett. d) D.lgs. 196/2003):

- origine razziale ed etnica
- convinzioni e adesioni religiose, politiche e filosofiche
- stato di salute e vita sessuale

Il Regolamento Europeo non parla di dati sensibili ma di **categorie particolari di dati personali** (art. 9), tra i quali comprende anche:

- dati genetici
- dati biometrici intesi a identificare in modo univoco una persona fisica
- orientamento sessuale

Divieto generale di trattamento

Il trattamento di dati sensibili potrebbe creare **rischi significativi** per i diritti e le libertà fondamentali, in particolare: discriminazioni, furto o usurpazione di identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, altri danni economici o sociali significativi (***Considerando 75***)

È, in via generale, **vietato**, salvo quando vi sia il consenso espresso dell'interessato o ricorra una delle altre esigenze specifiche previste dall'art. 9 par. 2 Reg. UE 679/16

In ogni caso si applicano i principi generali e le altre norme del Regolamento, in particolare per quanto riguarda le condizioni per il trattamento lecito (art. 6)

Eccezioni

Il trattamento è consentito qualora si verifichi uno dei seguenti casi:

- **consenso esplicito** dell'interessato per una o più finalità specifiche
- **necessità** di assolvere obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale
- interesse vitale dell'interessato o di un'altra persona
- trattamento effettuato da un organismo non lucrativo con finalità politiche, religiose, filosofiche, sindacali, riguardante i membri o gli ex membri
- dati resi manifestamente pubblici dall'interessato
- necessità di accertare, esercitare, difendere un diritto in sede giudiziaria
- interesse pubblico sulla base dell'ordinamento europeo o interno
- trattamenti sanitari: medicina preventiva o medicina del lavoro, valutazione capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale se trattai da un professionista soggetto al segreto professionale
- ricerca scientifica, storica e statistica

Coordinamento con il diritto nazionale

Sono destinate a rimanere in vigore tutte le norme nazionali non espressamente in contraddizione con il GDPR

Il diritto degli Stati membri può stabilire disposizioni specifiche sulla protezione dei dati per adeguare l'applicazione delle norme del Regolamento, determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili») (***Considerando 10***)

Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, biometrici o dati relativi alla salute (art. 9 par. 4)

Autorizzazioni generali

Il Garante ha emesso varie autorizzazioni di carattere generale, relative a determinate categorie di titolari o di trattamenti:

- **autorizzazione n. 1/2014**: autorizzazione al trattamento dei dati sensibili nel rapporto di lavoro

Efficacia: dal 1° gennaio 2017 al 24 maggio 2018 «*tenuto conto che a decorrere dal 25 maggio 2018 sarà applicabile il Regolamento (UE) 2016/679 […] salve le modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia e ferme restando le determinazioni eventualmente adottate dall'Autorità in applicazione del citato Regolamento*».

Autorizzazione n. 5/2016

Autorizza «*Società ed altri organismi che gestiscono fondi-pensione o di assistenza, ovvero fondi o casse di previdenza*» [art. 1 lett. a)] al trattamento di dati sensibili, fatta eccezione dei dati idonei a rivelare la vita sessuale

Limitatamente ai dati ed alle operazioni indispensabili per adempiere agli obblighi anche precontrattuali che i soggetti assumono, nel proprio settore di attività, al fine di fornire beni specifici, prestazioni o servizi richiesti dall'interessato

Fa salvo il rispetto del **principio di necessità**:

i sistemi informativi e i programmi informatici vanno configurati riducendo al minimo l'utilizzazione di dati personali e identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità (art. 3 Codice Privacy)

Conservazione

I dati personali possono essere conservati per un periodo non superiore a quello necessario per perseguire le finalità, ovvero per adempiere agli obblighi o agli incarichi previsti.

Deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso

I dati che risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene

Responsabilità Civile

- Art. 15 D.lgs 196/2003

  "Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile"

- Art. 2050 c.c.

  "Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno"

Responsabilità Civile

Il Trattamento dei dati è attività Pericolosa

- **Il pericolo è in RE IPSA** – Maggior Cautela per chi tratta dati rispetto alle attività non pericolose

- **Responsabilità Oggettiva:** Presunzione di colpa del danneggiante (prescinde dal DOLO o dalla COLPA)

- **Prova liberatoria:** Prova dell'adozione di tutte le "misure IDONEE" ad evitare il danno (prova liberatoria particolarmente rigorosa, parametro della **concretezza** dimostrazione dell'adozione di tutte le misure idonee necessarie per evitare l'illecito tenuto conto del progresso tecnico del momento)

- **Risarcimento del danno:** Patrimoniale e non patrimoniale (in caso di sofferenza fisica/morale, risarcito in via equitativa ma solo se violato art. 11, cioè se il trattamento costituisce reato ai sensi del 167 Codice Privacy)

Responsabilità Penale

Perché l'esigenza di una tutela di natura Penale?

- Il Diritto alla Riservatezza (informazioni personali) è di rango Costituzionale
- Funzione General –Preventiva propria del Diritto Penale
- Effettuo dissuasivo maggiore per Organizzazioni medio-grandi, rispetto alle sanzioni amministrative

Sanzioni Codice Privacy

Sistema sanzionatorio a "DOPPIO BINARIO" (Violazioni amministrative e illeciti penali)

Sanzioni Amministrative -specifiche per singola violazione o tratt. Illecito:
alcuni esempi:

1. Omessa o inidonea informativa all'interessato: **da 6.000,00 a 36.000,00 Euro**
2. Trattamento in violazione misure sicurezza: **da 10.000,00 a 120.000,00 Euro**
3. Inosservanza di prescrizioni di misure necessarie e/o divieti del Garante: **da 30.000,00 a 180.000,00 Euro**
4. Mancata tempestiva notifica (per chi è tenuto a farlo): **da 20.000,00 a 120.000,00 Euro**
5. Mancata esibizione documenti richiesti dal Garante o rifiuto di fornire informazioni: **da 10.000,00 a 60.000,00 Euro**
6. Pubblicazione dell'Ordinanza-Ingiunzione su quotidiani Nazionali e Locali

Sanzioni Codice Privacy

Sanzioni Amministrative:

In particolare:

- Violazione di minor gravità applicato **2/5 della sanzione**
- **Più violazioni** di una disposizione o più disposizioni (tranne art. 162 co. 2, 162 bis e164) : sanzione **da 50.000,00 a 300.000,00 Euro**
- Caso particolarmente **grave** o se il pregiudizio coinvolge **più interessati** le sanzioni sono **raddoppiate**
- Possibilità di aumento sanzione **sino al quadruplo in relazione al fatturato**

Sanzioni GDPR 679/16

DALLA FORMA ALLA SOSTANZA

Impianto sanzionatorio Completamente nuovo

(art. 83 Regolamento):

- Il GDPR prevede **solo** sanzioni amministrative
- Sanzioni Penali – competenza dei singoli stati
- Eliminato sistema sanzionatorio per singola tipologia di illecito trattamento
- Nuovo sistema basato sulla **gravità** della condotta

Sanzioni GDPR 679/16

Il Garante della Privacy dovrà garantire in ogni singolo caso che la sanzione sia:

A) **Effettiva**
B) **Proporzionata**
C) **Dissuasiva**

<u>Tenuto conto dei seguenti parametri:</u>

- Natura, Gravità e durata violazione
- Il dolo o la colpa nella violazione
- Azioni intraprese dal Titolare per mitigare i danni subiti dall'interessato
- Misure organizzative attuate, anche tecniche per prevenire le violazioni
- Recidiva
- Livello di cooperazione con il Garante per porre rimedio
- Categoria di dati oggetto di violazione
- Adesione a codici di condotta o presenza di Certificazioni
- Circostanze attenuanti / aggravanti
- Benefici economici ottenuti o perdite evitate come conseguenza della violazione

Sanzioni GDPR 679/16

Previsti due livelli di sanzioni:

A. Sanzioni amministrativa fino a 10 milioni di euro, o in caso di un'impresa, fino al 2% del fatturato totale annuo mondiale dell'esercizio precedente, se superiore, le violazioni delle disposizioni relative agli obblighi del Titolare o del Responsabile

Sanzioni GDPR 679/16

B. Sanzioni amministrative fino a 20 milioni di euro, o in caso di un'impresa, fino al 4% del fatturato totale annuo mondiale dell'esercizio precedente, se superiore, nel caso in cui le violazioni interessano ad esempio:

- Principi base del regolamento
- Condizioni per il consenso
- Diritti degli interessati
- Trasferimento dati all'estero
- Mancata ottemperanza ad un ordine del Garante

LA PRIVACY NEL RAPPORTO DI LAVORO

BILANCIAMENTO DEGLI INTERESSI LEGITTIMI

- Riservatezza
- Libertà e dignità

***

- Tutela patrimonio aziendale
- Controlli difensivi

PRINCIPI CARDINE

Applicabili al trattamento dati dei lavoratori

- Liceità
- Correttezza trasparenza
- Limitazione finalità
- Esattezza
- Integrità riservatezza
- Limitazione conservazione

CONSENSO DEL LAVORATORE

E' vietato trattare dati personali che:
- rivelino l'origine razziale o etnica
- opinioni politiche
- convinzioni religiose o filosofiche
- appartenenza sindacale
- nonché trattare dati genetici
- dati biometrici intesi a identificare in modo univoco la persona
- dati relativi alla salute o alla vita sessuale o all'orientamento sessuale

Tale divieto si supera se:
1. si ha il consenso esplicito del lavoratore al trattamento per una o più finalità specifiche;
2. il trattamento è necessario per assolvere gli obblighi ed esercitare diritti specifici del titolare o dell'interessato in materia di diritto del lavoro, sicurezza sociale perché esiste una legge o un contratto collettivo.

FORMAZIONE ED INFORMAZIONE

- Adempimento fondamentale alla base del bilanciamento degli interessi e dei principi di cui allo Statuto dei Lavoratori (art. 4)
- Policy aziendali (ex sull'uso degli strumenti di lavoro-videosorveglianza e geo localizzazione)
- L'assenza di una esplicita policy può determinare una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione
- Indispensabile per ogni valutazione e analisi del rischio

ESEMPIO: USO POSTA ELETTRONICA (Linee guida Garante 2007)

1. rendere disponibili indirizzi di posta elettronica condivisi tra più lavoratori eventualmente affiancandoli a quelli individuali

2. Valutare la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore

3. assenze programmate: il datore di lavoro metta a disposizione apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura

4. assenze non programmate: attivare la procedura descritta avvalendosi di servizi webmail ovvero possibilità di delegare altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

CONTROLLI A DISTANZA VIETATI

In particolare non può ritenersi consentito:

• la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori

• la riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;

• la lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;

• dell'analisi occulta di computer portatili affidati in uso.

CONSERVAZIONE DATI INTERNET

Necessità di dotarsi di sistemi software configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

NUOVO ART. 4 STATUTO LAVORATORI

Dal superamento del divieto a priori dei controlli a distanza al bilanciamento degli interessi datoriali e i diritti dei lavoratori:

- sicurezza patrimonio, esigenze organizzative produttive e sicurezza sul lavoro

- diritti alla riservatezza e dignità della sfera personale del lavoratore

ACCORDO SINDACALE

- Previo accordo sindacale stipulato dalle rappresentanze sindacali: è sufficiente avere la maggioranza delle RSA purché ad esprimersi siano tutte le diverse unità produttive ove può essere attivato il controllo

- Misura alternativa e sussidiaria del provvedimento amministrativo autorizzatorio dell'Ispettorato Nazionale del Lavoro locale o centrale

FORMAZIONE ED INFORMAZIONE - III co. art. 4

- Le informazioni raccolte ai sensi del comma I e II sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti (policy) e di effettuazione dei controlli nel rispetto della normativa privacy vigente.

- Policy aziendali (ex sull'uso degli strumenti di lavoro-videosorveglianza e geo localizzazione)

- Controlli difensivi

STRUMENTI DI LAVORO - II co. Art. 4

- Per gli strumenti necessari al lavoratore per rendere la sua prestazione come pure per quelli di rilevazione delle presenze non si esigono né le causali né il preventivo accordo sindacale/l'autorizzazione governativa.
- I dati legittimamente raccolti potranno essere utilizzati ai fini di aumentare la produttività dei lavoratori, la sicurezza, ai fini disciplinari e giudiziari ma a condizione che l'azienda rispetti i principi della pertinenza correttezza e non eccedenza del trattamento dei dati raccolti nonché il divieto della profilazione e del controllo massivo e generalizzato.

QUADRO SANZIONATORIO

SANZIONI PENALI

ART. 4 E 38 L. 300/70

Reato colposo di installazione di una apparecchiatura audiovisiva atta potenzialmente al controllo a distanza dei lavoratori in assenza di accordo o autorizzazione anche con telecamere non attivate : pena fino a 1549 o arresto sino ad un anno salvo che il fatto non costituisca più grave reato.

SANZIONI VIOLAZIONE NORMATIVA PRIVACY IN MANCANZA DI IDONEA INFORMAZIONE E FORMAZIONE DEI LAVORATORI SCORRETTA CONSERVAZIONE E MISURE DI SICUREZZA

Sanzioni amministrative fino 180.000,00 Euro e arresto sino a 2 anni

CREAZIONE ED ADOZIONE DI UN MODELLO DI ORGANIZZAZIONE E DI GESTIONE IDONEO ALLA PREVENZIONE DEI REATI

CREAZIONE ED ADOZIONE DI UN MODELLO DI ORGANIZZAZIONE E DI GESTIONE PRIVACY AL FINE DI RISPETTARE LE PRESCRIZIONI DEL REGOLAMENTO

PRIVACY E WHISTLEBLOWING L. 197/2017

- Parere 1/2006 del WP art. 29 direttiva 95/46 CE relativo all'applicazione della normative UE sulla protezione dei dati alle procedure interne per la denuncia delle irregolarità riguardanti la tenuta della contabilità, i controlli contabili interni, la revisione contabile, la lotta contro la corruzione, la criminalità bancaria e finanziaria

- Segnalazione al Parlamento ed al Governo sull'individuazione, mediante sistemi di segnalazione, degli illeciti commessi da soggetti operanti a vario titolo nell'organizzazione aziendale (10 dicembre 2009)

NOMINA ADS

Tra i compiti deve essere previsto quello di

"garantire che la gestione e l'archiviazione dei dati relativi all'apposita casella di posta elettronica dedicata alle comunicazioni all'organismo di vigilanza, avvenga nel rispetto integrale della Legge nr. 179/2017 sulla tutela della riservatezza dell'identità del segnalante, in caso di eventuali segnalazioni di condotte illecite e/o violazioni del Modello 231, rispettando l'AdS stesso rigorosamente l'obbligo di riservatezza circa l'identità del segnalante (c.d. whistleblower), nonché circa qualsiasi informazione contenuta nella predetta casella di posta elettronica".

I passi verso il Regolamento UE nr. 2016/679

1. Verifica compliance alla normativa (attraverso interviste alle funzioni aziendali coinvolte ed esame della documentazione e dei processi in uso in azienda)
2. Nelle realtà più strutturate, individuazione di uno staff preparato
3. Creazione ed adozione del Modello aziendale Protezione dei dati
4. Formazione del personale coinvolto nel progetto
5. Designare un DPO
6. Effettuare una analisi dei rischi (organizzativi, informatici)
7. Predisporre un piano di sicurezza anche al fine della comunicazione di data breach
8. Revisione dei contratti fornitori informatici e di dati
9. Altri adempimenti: sito internet, videosorveglianza, geolocalizzazione, etc..

Domande ?

……. grazie per l’attenzione.

Contatti

STUDIO LEGALE GTA

Avv. Giovanni Tretti

Giovanni.tretti@gtastudio.eu

Avv. Susanna Greggio (Data Protection Officer)

susanna.greggio@gtastudio.eu

info@gtastudio.eu