Nuovo Regolamento sulla Protezione dei dati

- Il 24 Maggio 2016 e' entrato in vigore il Regolamento UE 2016/679 (General Data Protection Regulation – GDPR), che introduce nuove disposizioni e obblighi a carico dei Soggetti che trattano i dati , applicabili in ogni scenario di *business*, sia nel settore privato che in quello pubblico.
- Il Regolamento (GDPR) introduce importanti novità a forte impatto sotto il profilo giuridico, organizzativo e di sistemi informatici.
- In tale prospettiva tutte le aziende, società, organizzazioni hanno avviato processi di adeguamento, essedo il Regolamente (fonte primaria) direttamente applicabile in tutti gli stati Membri della Comunità Europea.
- Lo scorso 31 Marzo, il Consiglio dei Ministri ha approvato, in esame preliminare, lo schema di Decreto Legislativo per l'adeguamento nazionale alle disposizioni del Regolamento (GDPR); sostanzialmente il testo evidenzia "integrazioni" sul funzionamento della Autorità Garante e mezzi di tutela disponibili , disciplinando la transizione dal regime attuale (vigente codice privacy) a quello futuro.
- In particolare, viene espressamente previsto che sono fatti salvi (solo) i Provvedimenti del Garante per quanto compatibili con il GDPR. Al momento, tale valutazione di compatibilità è in corso, essendo previso il termine di 90 giorni (dalla pubblicazione del Decreto) per l'individuazione dei provvedimenti del Garante "compatibili" con il Gdpr; le previsioni contenute in altri provvedimenti (non compatibili) perderanno (automaticamente) efficacia decorso il suddetto termine.
- Entro il 21 Maggio p.v. il Governo dovrà licenziare il Decreto (in via definitive), previo parere delle Commissioni parlamentari e del Garante Privacy.
- In questi giorni , è in corso un importante lavoro di "riscrittura" del Testo di Decreto che dovrebbe recepire, in sostanziale continuità con il (precedente) Codice privacy, il regime della tutela penale connessa al trattamento dei dati.

Principi fondamentali GDPR

- Il Regolamento nasce dalla esigenza di unificare il sistema del trattamento dei dati a livello europeo in forza del principio
  - "ONE CONTINENT ONE LAW"

- Viene definito un quadro unificato di regole per tutta l'Unione Europea, che pone le Imprese in condizione di parità, consentendo di trarre il massimo vantaggio dal mercato unico digitale.
- Un maggiore livello di garanzia circa l'utilizzo dei dati personali ed il trasferimento degli stessi al di fuori dell'Unione Europea.
- Ri-definizione degli adempimenti in carico ai Titolari ed ai Responsabili (Imprese) del trattamento, secondo approccio basato sul rischio (Risk based) che collega gli obblighi al livello di rischio del trattamento
- **Principio di Accountability**: responsabilizzazione del Titolare del Trattamento (Azienda) al fine di controllare a valle "il trattamento dei "dati" e minimizzare il rischio, anche attraverso interventi mirati sugli strumenti informativi ed informatici (Infrastruttura/ processi di Information Communication Technology (ICT) a presidio.
- **Privacy by design e by default**: le tecnologie utilizzate per il trattamento dei dati devono essere progettate/configurate per garantire, al massimo livello, la protezione dei dati
- **Valutazione di impatto privacy (PIA):** il Titolare (Impresa) deve effettuare una valutazione preliminare di impatto quando il trattamento presenti un rischio elevato per i diritti degli interessati; in presenza di "rischi" obbligo di consultazione (preventiva) della Autorità di controllo.

Le novità del GDPR

Principio di Accountability

Termine anglo-sassone che non trova un diretto corrispondente nella lingua italiana in quanto sintetizza e racchiude due aspetti (C74; art. 24):

- La responsabilizzazione nell'adottare adeguate misure di sicurezza volte all'implementazione dei principi di protezione dei dati (i.e. *liceità, correttezza, trasparenza, necessità e minimizzazione dei dati, limitazione della conservazione, integrità e riservatezza*,..);
- La capacità di dimostrare che tali misure siano effettivamente applicate ed efficaci

Responsabilità verificabile →

L'accountability diviene il ***principio dei principi,*** in quanto si sostanzia nel rendere effettivi gli altri principi del trattamento e nella capacità del Titolare di *dimostrare* di averli osservati

Il **WP29** aveva già rilevato (op. 3/10) come il quadro giuridico allora vigente non fosse riuscito appieno a garantire che gli obblighi in tema di protezione dei dati si traducessero in meccanismi efficaci atti a fornire una protezione reale, proponendo alla Commissione Europea l'introduzione di meccanismi basati su un principio di responsabilità.

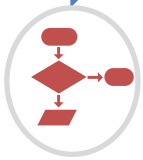
La *ratio*, dunque, sottesa all'introduzione dell'*accountability* è quella di **permettere il passaggio dalla teoria dei principi di trattamento alla loro messa in pratica** (da FORMA a SOSTANZA).

Le novità del GDPR

Principio di Accountability – Art. 37-38-39

In coerenza al principio di responsabilizzazione, spariscono le misure "minime" (ex Codice Privacy – All. B) per lasciare spazio alle misure "adeguate", lasciando al titolare libertà di autodeterminare quali misure, in ragione del trattamento effettuato (natura, campo di applicazione, contesto, finalità) e del rischio allo stesso associato, siano più idonee ed efficaci.

C79 – ripartizione delle responsabilità



La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari e dei responsabili del trattamento,.., esigono una chiara ripartizione delle responsabilità ai sensi del presente regolamento…

C81 – designazione del " responsabile" come forma di *accountability*

Per garantire che siano rispettate le prescrizioni del presente regolamento, il titolare quando affida delle attività di trattamento ad un responsabile del trattamento deve accertarsi che lo stesso presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche ed organizzative che soddisfino i requisiti del regolamento.

Responsabilità per *culpa in eligendo*

Le novità del GDPR

Principio di Accountability – Art. 37-38-39

Art. 37.1 – designazione del responsabile della protezione dei dati (DPO)

Per taluni tipi di trattamento deve essere individuato un DPO che sorvegli l'osservanza degli obblighi derivanti dal regolamento.

Tale previsione, oltre a voler garantire che i trattamenti avvengano nel rispetto delle norme del GDPR, pare voler dare ulteriore attuazione alla necessità di combinare l'adozione di misure adeguate con la sorveglianza sulla loro efficacia, in modo da comprovarla anche di fronte all'autorità di controllo.

Coinvolgimento

E' necessario prevedere che il DPO sia coinvolto negli incontri con il middle/top management dell'azienda e che sia informato tempestivamente di progetti e decisioni che impattano il trattamento di dati personali. A supporto di tali fasi è possibile prevedere opportuna normativa interna che ne definisca le modalità di coinvolgimento (indicazioni fornite dal WP29).

Il parere del DPO deve essere tenuto nella **debita considerazione;** in caso di disaccordo, il WP 29 raccomanda di **documentare le motivazioni alla base delle condotte difformi rispetto a quelle raccomandate**.

Disponibilità di risorse

L'organizzazione deve sostenere l'attività del DPO fornendo le risorse necessarie, assicurando il supporto del consiglio di amministrazione, garantendogli un tempo sufficiente per occuparsi delle tematiche relative al trattamento e alla protezione dei dati personali (soprattutto se la funzione del DPO è assegnata part-time), mettendo a disposizione risorse finanziarie, infrastrutturali e umane, diffondendo all'interno dell'azienda *"awareness"* in merito il ruolo del DPO e alle relative responsabilità, facilitando la collaborazione con le altre funzioni aziendali, sostenendo la formazione continua e l'aggiornamento professionale, strutturando, a seconda delle dimensioni dell'azienda, un team dove ogni membro ha delle responsabilità definite e formalizzate (indicazioni fornite dal WP29).

Le novità del GDPR

Indipendenza

Il DPO non deve ricevere, all'interno dell'azienda, alcuna indicazione in merito all'esercizio delle proprie funzioni. Il DPO deve, quindi, ricoprire una funzione gerarchica adeguata affinché sia assicurata l'indipendenza delle sue analisi e valutazioni. Resta ferma la responsabilità ultima del titolare/responsabile del trattamento in tema di *compliance*.

Conflitti di interesse

È necessario che le attività svolte dal DPO **non generino conflitti di interesse con altre attività a suo carico**. Il titolare/responsabile del trattamento è opportuno che identifichi le attività incompatibili con il ruolo del DPO, definisca regole interne per evitare tali conflitti, che dichiari l'assenza di potenziali conflitti di interesse, che istituisca opportuni presidi di controllo interno per evitare conflitti di interesse (indicazioni fornite dal WP29).

Conflitto di interesse → con ruolo manageriale di vertice:

- Amministratore Delegato
- Responsabile Finanziario
- Direttore Marketing
- Responsabile IT

Recentemente, il Garante privacy tedesco ha comminato una multa ad un'azienda per aver designato DPO il proprio manager IT.

Attività in carico al DPO 1/2

I principali compiti del DPO sono:

- **Informare** e fornire **consulenza** al Titolare o al Responsabile riguardo agli obblighi derivanti dal Regolamento
- sorvegliare l'**osservanza della normativa comunitaria e nazionale** nonché delle **politiche** del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi **l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale** che partecipa ai trattamenti e alle connesse attività di controllo;
- **cooperare** e agire da **punto di contatto per l'Autorità di controllo** sulle questione relative alla protezione dei dati, incluso il meccanismo di consultazione preventiva (art. 36);
- fornire, se richiesto, un **parere** in merito alla **valutazione d'impatto** sulla protezione dei dati e sorvegliarne lo svolgimento.

Le novità del GDPR

DPO – Configurazione

DPO esterno

Il DPO può assolvere i suoi compiti anche sulla base di un **contratto esterno di servizi**, stipulato con *persona fisica o giuridica*.

Team Specialistico

Ciascun soggetto appartenente al team deve possedere *tutti i requisiti richiesti dal RGPD*.

Le linee guida raccomandano una **diversificazione e ripartizione di compiti** nel team cosi da garantire *efficienza nell'attività*, prevedendo un **referente "unico"** quale interfaccia del cliente (Titolare/Responsabile).

Le novità del GDPR

Principio di Accountability – Art. 37-38-39

.

C82; art. 30 – registro delle attività di trattamento

Per dimostrare che si conforma al presente regolamento, il titolare o il responsabile deve tenere un registro delle attività di trattamento effettuate, il quale dovrà contenere, tra l'altro, una descrizione delle finalità, delle categorie di interessati e di dati personali, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate

C85 – *data breaches e* principio di responsabilizzazione

Non appena a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo, senza giustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è venuto a conoscenza, a meno che il titolare non sia in grado di *dimostrare* che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche.

Il GDPR: il regime sanzionatorio

- La mancata conformità al nuovo Regolamento Europeo comporta sanzioni e rischi di natura eterogenea. Il GDPR si occupa direttamente della sole sanzioni amministrative essendo quelle penali rimesse alla potestà dei singoli Stati membri.

Sanzioni

La violazione delle disposizioni elencate di seguito è soggetta a sanzioni amministrative pecuniarie **fino a 20.000.000 EUR o (per le imprese) fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore:

- i principi di base del trattamento, comprese le condizioni relative al consenso,
- i diritti degli interessati,
- i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale,
- obblighi relative a specifiche situazioni di trattamento identificate nel Regolamento e oggetto di legislazioni degli Stati membri,
- l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati.

Rischi

La mancata conformità espone inoltre l'azienda a differenti tipologie di rischi:

- **Rischi reputazionali** - Perdita di fiducia sul mercato e indebolimento del brand, Perdita di potenziali clienti, pubblicazione di provvedimenti prescrittivi, ordinanze, ingiunzioni e/o sentenze penali di condanna su media nazionali, internazionali e/o di settore,
- **Rischi economici** - Richieste di risarcimento danni, contenziosi con partner commerciali o clienti, spese legali per la gestione dei procedimenti correlati alla privacy,
- **Rischi operativi** - Ispezioni da parte dell'Autorità Giudiziaria, blocco parziale o totale dei trattamenti di dati personali.

Le sanzioni amministrative

L'impostazione del codice privacy D.lgs n. 196/2003

- Art. 161-166 ⇨ MATRICE INTEGRALMENTE INTERNA

➢ Fattispecie specificamente determinate

➢ Sanzioni determinate entro limiti edittali (minimo/ massimo)

➢ Determinazione del quantum ex art. 11 L. n. 689/1981:

*"Nella determinazione della sanzione amministrativa pecuniaria fissata dalla legge tra un limite minimo ed un limite massimo e nell'applicazione delle sanzioni accessorie facoltative, si ha riguardo alla **gravità** della violazione, all' **intervento** svolto dall'agente per l'eliminazione o attenuazione delle conseguenze della violazione, nonché alla **personalità** dello stesso e alle sue condizioni economiche".*

Le sanzioni amministrative

Le previsioni del codice privacy D.lgs n. 196/2003

ILLECITO	SANZIONE AMMINISTRATIVA
Omessa o inidonea informativa all'interessato (Art. 161, D. Lgs. 30 giugno 2003, n. 196)	- da 3.000 a 18.000 euro per violazione dei dati ex art. 13; - da 3.000 a 18.000 euro per violazione dei dati sensibili o giudiziari, - da 5.000 a 30.000 e fino al triplo se risulta inefficace per le condizioni economiche del contravventore
Altre fattispecie: [violazione art. 16, 1° comma lett. B) o di altre disposizioni in materia di disciplina del trattamento dei dati personali]; (Art. 162, D. Lgs. 30 giugno 2003, n. 196)	- da 5.000 a 30.000 euro
Altre fattispecie [violazione art. 84 1° comma] (Art. 162, D. Lgs. 30 giugno 2003, n. 196)	- da 5.000 a 3.000 euro
Omessa o incompleta notificazione (Art. 163, D. Lgs. 30 giugno 2003, n. 196)	- da 10.000 a 60.000 euro Sanzione accessoria: pubblicazione ordinanza - ingiunzione
Omessa informazione o esibizione al Garante (Art. 164, D. Lgs. 30 giugno 2003, n. 196)	- da 4.000 a 24.000 euro

Le sanzioni amministrative:

L'impostazione del GDPR

- Considerando 11: un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri (finalità di armonizzazione del sistema sanzionatorio)

- Individuazione specifica delle fattispecie a rilevanza sanzionatoria

- Individuazione delle sanzioni NEL SOLO MASSIMO EDITTALE (fino a ..)

  N.B.
  Possibile contrasto con il principio costituzionale di legalità dell'agire della PA.
  Opportuno un intervento del legislatore nazionale sul punto, tuttavia, a quanto consta,
  il legislatore ha scelto di non intervenire in merito.

- Nella discrezionalità dell'Autorità Garante è previsto, in considerazione di particolari circostanze, l'ammonimento, come misura alternativa alla sanzione.

Le sanzioni amministrative:

I soggetti destinatari ex GDPR

- Soggetti destinatari delle sanzioni sono i titolari o i responsabili del trattamento

➢ art. 4: sia persone fisiche che persone giuridiche + organismi di certificazione o monitoraggio

➢ La sanzione può essere irrogata ad una persona fisica che operi all'interno del contesto aziendale?

- Si, ma in via "eccezionale ", in generale destinataria della sanzione è la persona giuridica.
- Il WP29 con opinion del 2010 ha sottolineato come “nell’ottica strategica dell’attribuzione delle responsabilità, e per dare agli interessati un’entità di riferimento più stabile e più affidabile per l’esercizio dei loro diritti ai sensi della direttiva, sarebbe preferibile considerare come titolare del trattamento la società o l’organismo in quanto tali piuttosto che una specifica persona al loro interno. Sono la società e l’organismo a dovere, in ultima analisi, essere considerati titolari del trattamento dei dati e degli obblighi derivanti dalla normativa sulla protezione dei dati, a meno che non vi siano elementi chiari che indichino che indichino che a rispondere di ciò sia una persona fisica".

Le sanzioni amministrative

Criteri applicativi ex GDPR

- Art. 83 comma 3: CUMULO GIURIDICO

➢ nell'ipotesi in cui vengano rilevate più violazioni di norme all'interno del medesimo trattamento o in relazione a trattamenti collegati tra loro, l'importo della sanzione non potrà in nessun caso superare l'importo previsto per la violazioni più grave.

- PROBLEMI APPLICATIVI

➢ la disposizione, chiara nella definizione della regola del cumulo giuridico, non dà però spunti per la determinazione dei concetti di identità di trattamento e, soprattutto, di trattamenti collegati né le linee guida del WP 29 si sono espresse a riguardo. Su tale questione sarà dunque necessario attendere i primi provvedimenti del Garante.

Le sanzioni amministrative

Criteri applicativi ex GDPR

CRITERI PER LA DETERMINAZIONE DELLA SANZIONE- ampliata discrezionalità dell'Autorità Garante

- **Cons. 13:** nella determinazione della sanzione l'Autorità Garante dovrà innanzitutto tener presente le esigenze specifiche delle micro, piccole e medie imprese e considerare
  - non solo la gravità dell'infrazione commessa,
  - ma anche il fatturato dell'azienda che si intende sanzionare.

- **Cons. 148:** sancisce la necessità di tener conto della **condizione soggettiva del destinatario della sanzione qualora si tratti di persona fisica.** In questo caso infatti se l'infrazione commessa non è di particolare gravità o se comunque la sanzione pecuniaria risulti sproporzionata, la DPA potrà rivolgere un semplice ammonimento.

(segue…)

Le sanzioni amministrative: criteri applicativi ex GDPR

- **Art. 83 comma 2: criteri cui devono attenersi le Autorità nazionali**

- **l'entità del pregiudizio** da intendersi come afferente alla natura, gravità e durata della violazione. In tale determinazione assumeranno rilievo anche le finalità del trattamento nonché le conseguenze delle violazione in termini sia qualitativi che quantitativi;
- **l'elemento soggettivo**, vale a dire il carattere doloso o colposo della condotta.;
- **le modalità della condotta**, cioè le azioni poste in essere dal titolare o dal responsabile per attenuare il danno subito dall'interessato.
- il grado di responsabilità del titolare o del responsabile con specifico riferimento alle prescrizioni in materia di **privacy by design e by default**;
- la sussistenza **di precedenti violazioni** commesse dal titolare o dal responsabile;
- il grado di cooperazione con la DPA (c.d. ravvedimento operoso).
- le categorie di dati personali coinvolti nella violazione.
- Il modo in cui la DPA ha preso conoscenza della violazione, in particolare con riguardo all'obbligo di notificazione di data breach;
- la sussistenza di precedenti provvedimenti correttivi di cui all'art. 58 co. 2 disposti relativamente allo stesso oggetto;
- l'adesione a codici di condotta approvati ai sensi dell'art. 40 o a meccanismi di certificazione approvati ai sensi dell'art. 42 ("esimente");
- eventuali altri fattori aggravanti o attenuanti.

Le sanzioni amministrative:

Le fattispecie ex GDPR - doppio regime

- Previsione di un doppio regime sanzionatorio nel quale è fissato il solo limite massimo della sanzione → ampliata discrezionalità in capo alle Autorità di Controllo.

I LIVELLO – comma 4 art. 83

- Sanzione max € 10.000.000 o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente se superiore.

→ in caso di violazione di

OBBLIGHI DEL TITOLARE E DEL RESPONSABILE

Le sanzioni amministrative

Le fattispecie ex GDPR - doppio regime

- I LIVELLO - fattispecie

— art. 8, consenso dei minori in relazione ai servizi della società dell'informazione;
— art. 11, trattamento che non richiede l'identificazione;
— art. 25, privacy by design;
— art. 26, contitolarità del trattamento;
— art. 27, rappresentante del titolare o del responsabile;
— art. 28, responsabile del trattamento;
— art. 29, titolare e responsabile del trattamento;
— art. 30, registro dei trattamenti;
— art. 31, cooperazione del titolare e del responsabile con la DPA;
— art. 32, misure di sicurezza adeguate;
— art. 33, notifica data breach alla DPA;
— art. 34, comunicazione data breach all'interessato;
— art. 35, DPIA;
— art. 36, consultazione preventiva in caso di trattamento che presenti rischio elevato;
— art. 37, designazione DPO;
— art. 38, posizione DPO;
— art. 39; compiti DPO.

Le sanzioni amministrative

Le fattispecie ex GDPR - doppio regime

- II LIVELLO – comma 5 dell'art. 83

➢ il regolamento prevede sanzione fino a € 20.000.000 o, per le imprese, fino al 4% del fatturato mondiale annuo dell'esercizio precedente se superiore, in caso di violazione di norme su:

✓ PRINCIPI

✓ DIRITTI DELL'INTERESSATO

✓ TRASFERIMENTO DATI ALL'ESTERO

✓ POTERI DELL'AUTORITA' GARANTE

Le sanzioni amministrative

Le fattispecie ex GDPR - doppio regime

- **II LIVELLO – FATTISPECIE**
  - PRINCIPI:
    - art. 5, principi del trattamento;
    - art. 6, liceità del trattamento;
    - art. 7, condizioni per il consenso;
    - art. 9, trattamento di categorie particolari di dati.
  - DIRITTI DELL'INTERESSATO:
    - art. 12, trasparenza e modalità per l'esercizio dei diritti dell'interessato;
    - artt. 13-14, informazioni e accesso ai dati personali;
    - art. 15, diritto di accesso dell'interessato;
    - art. 16, diritto di rettifica;
    - art. 17, diritto di cancellazione;
    - art. 18, diritto di limitazione del trattamento;
    - art. 19, obbligo di notifica in caso di esercizio dei diritti dell'interessato;
    - art. 20, diritto alla portabilità;
    - art. 21, diritto di opposizione;
    - art. 22, processo decisionale automatizzato (profilazione).

Le sanzioni amministrative

Le fattispecie ex GDPR - doppio regime

- **II LIVELLO – FATTISPECIE**
  - TRASFERIMENTO DATI ALL'ESTERO:
    - art. 44, principi generali;
    - art. 45, trasferimento sulla base di una decisione di adeguatezza;
    - art. 46, trasferimento soggetto a garanzie adeguate;
    - art. 47, trasferimento sulla base di BCR;
    - art. 48, trasferimento o comunicazioni non autorizzati;
    - art. 49, deroghe in specifiche situazioni;
  - POTERI DELLA DPA
    - art. 58 co. 1, violazione degli ordini della DPA;
    - art. 58 co. 2, illegittima negazione d'accesso alla DPA.

Le fattispecie penalmente rilevanti:D.lgs n. 196/2003

ILLECITO	SANZIONE PENALE
Trattamento illecito di dati (Art. 167, D. Lgs. 30 giugno 2003, n. 196)	- Reclusione da 6 a 18 mesi (se dal fatto deriva nocumento); - Reclusione da 6 a 24 mesi (se il fatto consiste nella comunicazione e/o diffusione). - Reclusione da 1 a 3 anni (se il fatto costituisce reato più grave: al fine di trarre profitto per se o altri o per arrecare danno).
Falsità nelle dichiarazioni e notificazioni al Garante (Art. 168, D. Lgs. 30 giugno 2003, n. 196)	- Reclusione da 6 mesi a 3 anni.
Inadeguatezza delle Misure minime di sicurezza (Art. 169, D. Lgs. 30 giugno 2003, n. 196)	- Arresto fino a 2 anni
Inosservanza di provvedimenti del Garante (Art. 170, D. Lgs. 30 giugno 2003, n. 196)	- Reclusione da 3 mesi a 2 anni.
Inosservanza delle disposizioni di cui all'art. 4 e 8 Statuto dei lavoratori (Art. 171 D.lgs 30 giugno 2003 n. 196 che rimanda all'art. 38 Statuto dei lavoratori)	- Ammenda da euro 154 a euro 1.549 - Arresto da 15 giorni ad un anno (anche congiuntamente)

La tutela penale ex D.lgs n. 196/2003

Art. 167 Trattamento illecito dei dati

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

CARATTERISTICHE DELLA FATTISPECIE:

- è un **reato proprio**, può essere commesso solo dal Titolare del trattamento;
- è un **reato di danno** e non di mero pericolo;
- la norma non descrive la condotta, ma **la fattispecie criminosa viene desunta dal richiamo generico alle disposizioni che regolano il trattamento**;
- la norma ha **carattere sussidiario** essendo applicabile solo quando la condotta non integri una fattispecie di reato più grave;
- è richiesto il **dolo specifico:** "al fine di trarre profitto con altrui danno". Sul punto la giurisprudenza ha inteso il danno in senso ampio facendovi rientrare tutte le ipotesi di effetto pregiudizievole per l'interessato derivante dalla arbitraria condotta lesiva altrui. Rientrano in tali ipotesi anche i casi di **fastidio e turbamento**.

La tutela penale ex D.lgs n. 196/2003

Art. 168 Falsità nelle dichiarazioni e comunicazioni al Garante

1. Chiunque, nelle comunicazioni di cui all'articolo 32-bis, commi 1 e 8, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, **dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi,** è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni

CARATTERISTICHE DELLA FATTISPECIE:

- la norma ha **carattere sussidiario** essendo applicabile solo quando la condotta non integri una fattispecie di reato più grave;

La tutela penale ex D.lgs n. 196/2003

Art. 169 Misure di sicurezza

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni.
2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

CARATTERISTICHE DELLA FATTISPECIE:

- la fattispecie fa riferimento al rispetto delle misure minime individuate all'**allegato B** del Codice Privacy
- la norma ha **carattere sussidiario** essendo applicabile solo quando la condotta non integri una fattispecie di reato più grave.

La tutela penale ex D.lgs n. 196/2003

Art. 170 Inosservanza dei provvedimenti del Garante

1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni.

CARATTERISTICHE DELLA FATTISPECIE:

- la norma NON ha carattere sussidiario, bensì fattispecie **può concorrere** con altre norme eventualmente violate.

La tutela penale ex D.lgs n. 196/2003

Art. 171 Altre fattispecie

1. La violazione delle disposizioni di cui all'articolo 113 e all'articolo 4, primo e secondo comma, della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della legge n. 300 del 1970.

CARATTERISTICHE DELLA FATTISPECIE:

- riguarda le ipotesi di trattamento illecito dei dati personali nel rapporto di lavoro. In particolare viene richiamato l'art. 113 dello Statuto che a sua volta richiama
  - **l'art. 8** ai sensi del quale "**è fatto divieto al datore di lavoro, ai fini dell'assunzione del dipendente come nel corso del rapporto di lavoro di svolgere indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore nonché su fatti non rilevanti ai fini della valutazione all'attitudine professionale del lavoratore" e**
  - **l'art. 4** che disciplina il controllo a distanza sull'attività lavorativa ponendo (a seguito della modifica intervenuta con il D.lgs 81/2015 – c.d. jobs act) quali condizioni/presupposti di liceità l'autorizzazione della DTL o l'accordo sindacale a meno che lo strumento di controllo non sia qualificabile come strumento di lavoro (ipotesi geolocalizzazione attravreso dispositivi).

- si tratta **di reati di pericolo** che si configurano nel momento stesso in cui viene predisposto il controllo illegittimo o l'indagine a prescindere dal loro effettivo utilizzo.

.

Il GDPR e i possibili futuri scenari

- **Il GDPR non si occupa direttamente delle sanzioni penali** essendo tale materia rimessa alla potestà degli Stati Nazionali

- In particolare il **considerando 149** prevede: "Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali in virtù ed entro i limiti del presente regolamento. Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente regolamento".

Il GDPR e i possibili futuri scenari

A fronte delle previsioni del GDPR, **le possibili scelte del legislatore nazionale riguardo** le sanzioni amministrative e penali legate al trattamento illecito dei dati personali implicano:

- per quanto attiene le sanzioni amministrative:

  - ✓ intervenire al fine di armonizzare la disciplina europea con i principi e le regole che disciplinano il diritto amministrativo interno (ad esempio prevedendo il **limite minimo delle sanzioni)**
  - ✓ lasciare l'intera disciplina alla fonte europea;

- per quanto attiene la responsabilità penale connessa al trattamento dei dati:

  - ✓ intervenire sull'apparato sanzionatorio esistente e previsto dal D.lgs 196/2003 per armonizzarlo alle previsioni del Regolamento (ad esempio per quanto attiene le misure di sicurezza, la fattispecie dovrebbe essere integralmente "riscritta" in quanto le misure di sicurezza vengono ancorate al criterio astratto dell'adeguatezza e viene eliminato il riferimento ad un set minimo di misure da adottare);
  - ✓ riscrivere integralmente la disciplina;
  - ✓ escludere la tutela penale lasciando la protezione del diritto alla riservatezza esclusivamente ai reati "tipici" previsti nel codice penale (es.il già citato art. 615 bis c.p.)

Il GDPR e i possibili futuri scenari

- ✓ A quanto consta, al momento, il legislatore ha scelto di abrogare integralmente il D.lgs 196/2003 a partire dal 25 maggio 2018 (data in cui il GDPR sarà pienamente efficace) per sostituirlo con un nuovo Decreto che andrà a disciplinare il trattamento dei dati personali unitamente (ed in conformità) al Regolamento Europeo.

- ✓ Nella prima bozza di tale Decreto Legislativo, approvato dal Governo, ma non ancora pubblicato, **mancava del tutto la disciplina delle sanzioni**.

- ✓ Secondo gli ultimi sviluppi sembra che il Testo sia sottoposto ad ulteriori modifiche con specifico riguardo alle sanzioni penali.

  - ➢ In particolare:
  - viene conservato, anche con riferimento ai limiti edittali, il reato di **trattamento illecito dei dati personal**i;
  - viene conservato, anche con riferimento ai limiti edittali, il reato di **falsità nelle dichiarazioni e comunicazioni al Garante;**
  - viene introdotta la nuova fattispecie di **comunicazione e diffusione illecita di dati riferibili a un ingente numero di persone**, che sarà punita con la reclusione da uno a sei anni;
  - viene introdotta la nuova fattispecie di **acquisizione fraudolenta di informazioni personali per trarne profitto**, sanzionata con la reclusione da uno a quattro anni.