Misure di Sicurezza Adeguate - Art. 32

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati da trattamenti derivanti da:

Distruzione, Perdita o Modifica dei Dati

Divulgazione non autorizzata dei Dati

Accesso ai Dati in modo accidentale o illegale

Chiunque abbia accesso ai dati personali agisce sotto la responsabilità del Responsabile o dell'Incaricato del trattamento, e da essi è istruito in tal senso.

Protezione fisica delle aree e dei locali

- Le misure antintrusione (intese come perimetrazione, compartimentazione dei locali e la video-sorveglianza di edifici e locali)

- Le misure antincendio (da considerare obbligatorie ai sensi del D.Lgs 81/08 -D.lgs 106/09)

Protezione fisica delle aree e dei locali

- UPS Gruppi di continuità per PC
- UPS per le linee telefoniche
- Protezione degli archivi cartacei e conservazione sicura dei supporti di memorizzazione (disco rigido rimovibile, cd/dvd, pen drive)
- Regole per il controllo degli accessi fisici ai locali dell'azienda

LA SICUREZZA DEL TRATTAMENTO- art 32

- **SCOPO**
  - Garantire la sicurezza dei dati e prevenire rischi di danni agli Interessati

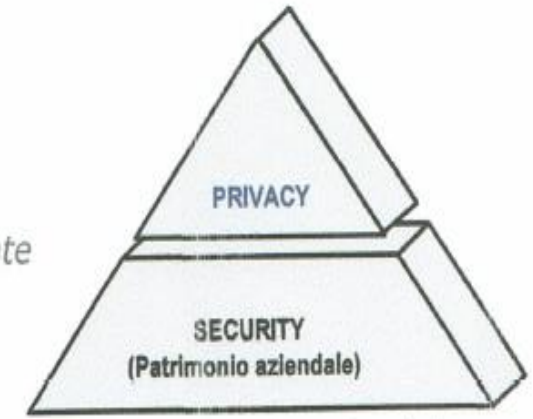
- **DESTINATARI DELLA NORMA**
  - Titolare
  - Responsabile
  - Incaricato

- **RESPONSABILITA'**
  - ***TITOLARE E RESPONSABILE***
    - ✓ Individuare e adottare le Misure di Sicurezza
    - ✓ Fornire agli Incaricati istruzioni/formazione al riguardo
    - ✓ Vigilare su efficacia
  - ***INCARICATI***
    - ✓ Trattare i dati secondo le istruzioni ricevute
    - ✓ Comportamento consapevole dei rischi

La Sicurezza Del Trattamento
COSA DEVE ESSERE FATTO

- **RISK ASSESSMENT**
  - *Relativo agli strumenti*
  - *Relativo al contesto*
  - *Relativo al comportamento*

- **MISURE DI CONTRASTO DEI RISCHI**
  - *Adottare misure di sicurezza che comprendano*
    - *Garanzia di*
      - ✓ *disponibilità dei dati*
      - ✓ *integrità dei dati*
      - ✓ *riservatezza dei dati*
      - New ✓ *resilienza dei sistemi e dei servizi*
    - *Uso di pseudonomi e cifratura dei dati*
    - *Ripristino tempestivo in caso di incidente*
  - *Effettuare Test di efficacia*



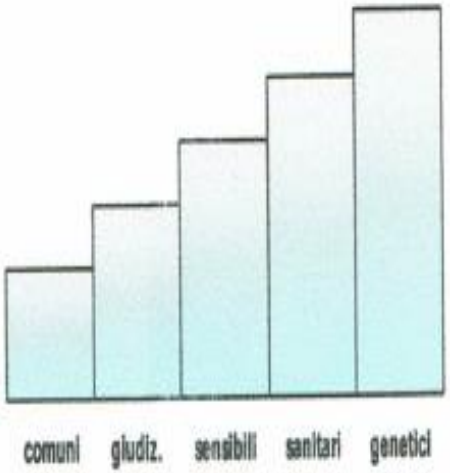
- **OTTICA DA SEGUIRE**
  - ***Proteggere la privacy*** *e non (solo) la sicurezza del patrimonio aziendale*

La Sicurezza Del Trattamento
IL LIVELLO DI SICUREZZA

QUALITA' DELLE MISURE

- *Livello di protezione "ADEGUATO"*
- *Tenuto conto di*
  - *Stato dell'arte e sviluppi tecnici*
  - *Natura dei dati,*
  - *Contesto e strumenti adottati*
  - *Probabilità e gravità dei rischi.*
  - *Bilanciamento costi vs rischi*

New



MONITORAGGIO

- *Livello di "adeguatezza" delle misure, in continua evoluzione*

La Sicurezza Del Trattamento
COPERTURA

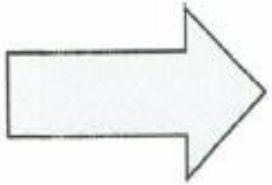
- **PRIMA DI INIZIARE IL TRATTAMENTO**

- **DURANTE TUTTE LE OPERAZIONI DI TRATTAMENTO**
  - *Raccolta, conservazione, trasmissione, elaborazione ...*

- **QUALUNQUE SIA LO STRUMENTO / MODALITA'**
  - ***Elettronici:*** *server centralizzati, cloud, informatica individuale, PC, smartphon, tablet, etc...*
  - ***Cartacei***
  - ***Altro:*** *fax , stampanti ...*

La Sicurezza Del Trattamento
COMPORTAMENTO DEI DIPENDENTI

- **PREVENIRE ILLECITA DIVULGAZIONE**
  - *A Terzi*
  - *A Colleghi: Principio del Need to Know*
  - *Clean Desk Policy*
- **PROTEGGERE DATI vs STRUMENTI**
  - *Segretezza e robustezza Psw, utilizzo PIN*
  - *Screen saver,*
  - *Controllo e custodia degli strumenti*
- **PROTEGGERE DATI vs LUOGHI/ACQUISIZIONI INVOLONTARIE**
  - *Distanze di cortesia/ Open Space/Aree chiuse*
  - *Presidio Stampanti, Copiatrici, Fax ...*
  - *Separazione dati sensibili da dati comuni*
  - *Distruggi documenti*



CONSAPEVOLEZZA/FORMAZIONE

La Sicurezza Del Trattamento
AZIONI E DOCUMENTAZIONE

- **AMBITI DI INTERVENTO**
  - *Logici*
  - *Tecnici e di sicurezza fisica*
  - *Organizzativi e procedurali*
  - *Di processo*
  - *Di Formazione / Informazione*
  - *Audit*

New

- **ACCOUNTABILITY**
  - *Obbligo di documentare e fornire prova*

New

- **POSSIBILI SEMPLIFICAZIONI PER PMI**
  - *Adesione a Codici Condotta art 40, Cerificazione art 39*

Misure di Sicurezza Adeguate – Art. 32

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati da trattamenti derivanti da:

Distruzione, Perdita o Modifica dei Dati

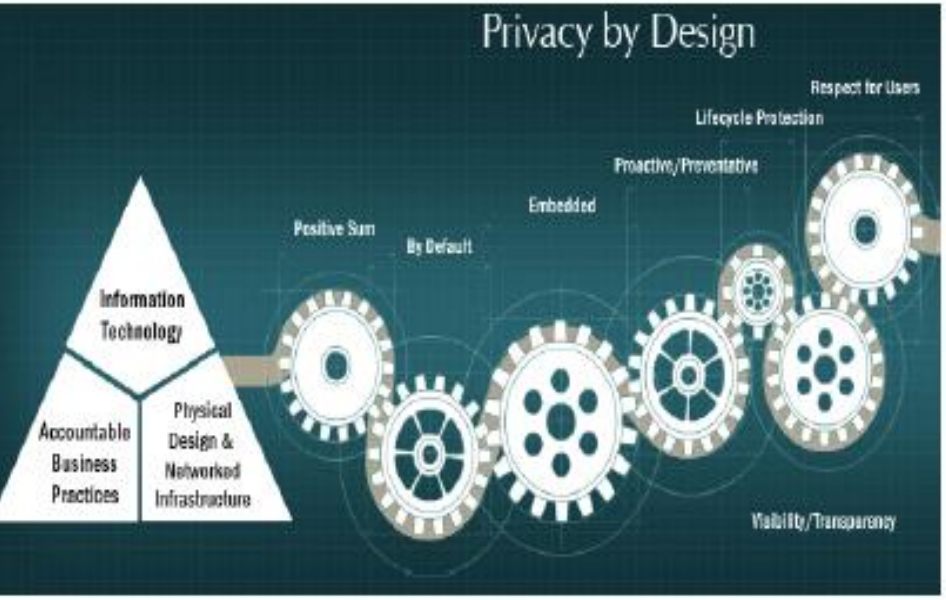
Divulgazione non autorizzata dei Dati

Accesso ai Dati in modo accidentale o illegale

Chiunque abbia accesso ai dati personali agisce sotto la responsabilità del Responsabile o dell'Incaricato del trattamento, e da essi è istruito in tal senso.

Privacy By Design e By Default – Art. 25

in dalla progettazione bisogna prevedere che le misure volte alla protezione dei dati personali
ano integrate nell'intero ciclo di vita tecnologico, dalla primissima fase di ideazione fino alla sua
ealizzazione, al suo utilizzo ed allo smaltimento finale.



Privacy By Design:
Individuazione di misure tecniche e organizzative adeguate per la protezione dei dati, già durante la fase di progettazione

Privacy By Default:
Garantire che siano trattati di default solo i dati personali necessari per ogni specifica finalità del trattamento

Pseudonimizzazione

Minimizzazione

Minimizzazione

Limitazione delle finalità

Integrazione delle garanzie a tutela dei diritti degli Interessati

Si potrà utilizzare un meccanismo di certificazione approvato per dimostrare la conformità del processo a tali requisiti.

New

REGISTRO DEI TRATTAMENTI- art 30

Obbligo di documentazione

CHI E' OBBLIGATO

- *il Titolare e anche il Responsabile*

IN COSA CONSISTE

- *Un Registro delle attività di trattamento in forma scritta anche elettronica:*
- *A disposizione del Garante*

COSA DEVE CONTENERE

- *Quadro di Censimento e di sintesi: Nome del Titolare (o del Responsabile e del Titolare per cui si agisce) Descrizione delle attività effettuate dal Titolare (o per conto del Titolare), Finalità, Categorie dei dati, Destinatari dei dati, Misure di sicurezza adottate, Termini per la cancellazone dei dati, Destintari extra UE e loro misure di garanzia ...*

ECCEZIONI ESTREMAMENTE LIMITATE

- *Non applicabile < 250 dipendenti a meno che :*
  - ✓ *il trattamento non sia occasionale, includa "dati particolari" o possa provocare rischi per diritti e libertà degli interessati,*

Simil DPS- assegnazione compito a struttura per gestione e aggiornamento

Registro delle attività di trattamento - Art. 30

Il Registro delle Attività di Trattamento (**PRIVACY BOOKING**) sarà un documento di tipo dinamico ed una sorta di memoria storica dell'azienda in materia di sicurezza dei Dati.

Nome e contatti di ogni Responsabile (esterni e interni)

Finalità di Trattamento

Categorie di Interessati e di Dati trattati

Categorie di destinatari a cui i dati sono comunicati

Informazioni sui trasferimenti verso paesi terzi

Termini per la cancellazione dei dati

Misure di sicurezza tecniche e organizzative

Backup & Recovery

Reg. Informatico

Policy e Procedure

Formazione

Registro delle attività di trattamento – Art. 30

Il Registro delle Attività di Trattamento (Privacy Booking) sarà un documento di tipo dinamico ed una sorta di memoria storica dell'azienda in materia di sicurezza dei Dati.

Nome e contatti di ogni Responsabile (esterni e interni)

Finalità di Trattamento

Categorie di Interessati e di Dati trattati

Categorie di destinatari a cui i dati sono comunicati

Informazioni sui trasferimenti verso paesi terzi

Termini per la cancellazione dei dati

Misure di sicurezza tecniche e organizzative

Backup & Recovery

Reg. Informatico

Policy e Procedure

Formazione

Registro delle attività di trattamento – Art.

Gli obblighi di cui all'Art.30 non si applicano alle aziende con meno di **250 dipendenti**, tran
seguenti casi:

Trattamento con rischi per diritti e libertà dell'Interessato

Trattamento non occasionale dei dati

Trattamento di categorie particolari di dati

Trattamento di dati relativi a condanne penali e reati

Data Breach Notification – Art. 33

Liberi PROFESSIONISTI
www.professionistiliberi.org

Nel caso in cui si verifichi una violazione di dati personali, il Titolare del Trattamento ha l'Obbligo di Notifica, che dovrà essere eseguito sia ai diretti interessati, che all'Autorità Garante per la protezione dei dati personali, entro ~~24 ore~~ 72 ore. Attualmente in Italia tale obbligo trova applicazione per le sole organizzazioni che forniscono servizi di comunicazione elettronica.

Soggetti Interessati

Autorità Garante

~~Conservazione Registro Pubblico delle tipologie di violazioni notificate~~

La decorrenza delle 72 ore parte dal momento in cui il Titolare viene a conoscenza della violazione, a meno che sia improbabile che essa presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora non siano rispettate tali tempistiche, la notifica all'Autorità Garante va corredata da una giustificazione motivata.

Data Breach Notification – Art.33

La comunicazione all'Interessato non è richiesta nei casi di:

Utilizzo di misure tecniche e organizzative adeguate per rendere i dati incomprensibili ai soggetti non autorizzati (cifratura)

Successiva adozione di misure atte a scongiurare il sopraggiungere di rischi per i diritti e le libertà degli interessati

Comunicazione particolarmente difficoltosa o onerosa per il Responsabile

In questo caso occorre procedere a comunicazione pubblica o misura simile

Data Protection Officer – Art. 37

Il Data Protection Officer, che potrà essere interno od esterno all'organizzazione, avrà il compito di progettare e mantenere un sistema organizzato e sicuro di gestione dei dati personali. Tale figura dovrebbe poter adempiere alle proprie funzioni in maniera indipendente.

Per chi sarà Obbligatorio?

Pubblica Amministrazione
Molto più di un'icona.

Pubbliche Amministrazioni

~~Grandi Aziende Private (oltre 250 dipendenti)~~

In Caso di Trattamento di Dati di ~~più di 5.000~~ Interessati su larga scala

In Caso di Trattamento di Dati Particolari su larga scala

Facoltatività per ciascuno Stato membro di introdurre la figura del DPO come obbligatoria.

Enti pubblici o gruppi d'imprese possono nominare un unico DPO per più stabilimenti/autorità.

I Compiti del DPO – Art. 39

Informare e consigliare Titolare, Responsabili e dipendenti

Sorvegliare l'attuazione e l'applicazione del Regolamento

Sorvegliare l'attuazione e l'applicazione delle politiche aziendali

~~Garantire la conservazione del Registro delle Attività di Trattamento~~

~~Controllare che le violazioni dei dati siano notificate~~

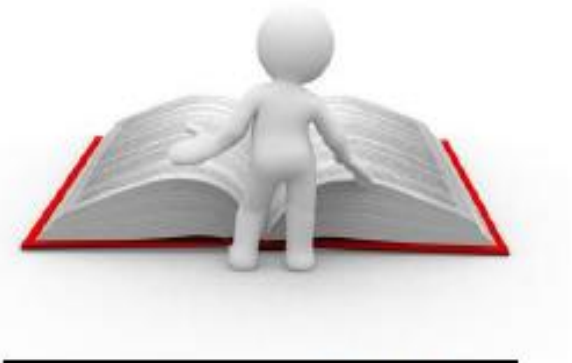
Verificare e fornire un parere sulla valutazione d'impatto

Cooperare con l'Autorità di controllo

Fungere di punto di contatto tra l'Autorità e gli Interessati

Il DPO opera considerando i rischi inerenti al trattamento, tenendo conto della relativa natura, campo di applicazione, contesto e finalità.

Le Competenze del DPO – Art. 37



Conoscenza Specialistica della Normativa

Conoscenza delle Pratiche in materia di Protezione dei Dati

Adempiere ai Compiti dell' Art. 39

Padronanza Requisiti Tecnici

Specifica Conoscenza del Settore

Analisi, Audit e Consultazioni

Collaborazione e Spiccate Capacità Relazionali

Formazione Avanzata Specializzata

Questi requisiti minimi era presenti in modo esplicito soltanto nel testo del Parlamento Europeo (75 bis). Nel testo definitivo si fa riferimento solo alle tre competenze riportate in alto.

Il DPO è una figura autonoma e indipendente dall'organizzazione e riferisce direttamente al vertice gerarchico.

New

Il Data Protection Officer Art 37-39 (1/4)

ADERISCO Liberi PROFESSIONISTI www.professionistiliberi.org

NUOVA CATEGORIA PROFESSIONALE

- *Figura di Garanzia Aggiuntiva interna all'Azienda*
- *Diversa dal Responsabile del trattamento e dal Compliance Manager*

CHI E' OBBLIGATO A NOMINARLO

- *Il Titolare e il Responsabile*

QUANDO E' OBBLIGATORIA LA NOMINA

- *Enti Pubblici*
- *Privati - Quando le attività principali consistono:*
  - ✓ *Trattamenti che per loro natura, ambito di applicazione e/o finalità richiedono il monitoraggio regolare e sistematico di interessati su larga scala,*

    oppure
  - ✓ *Trattamento su larga scala di "dati particolari" o "dati "penali"*

Il Data Protection Officer (2/4)

New

- **REQUISITI**
  - **PROFESSIONALITA':** *Qualità professionali, conoscenze giuridiche, informatiche ...*
  - **ESPERIENZA:** *Competenza specialistica di normativa e pratiche privacy*
  - **CAPACITA':** *di assolvere i Compiti previsti dall'art 39 del Regolamento*

- **CHI PUO' RICOPRIRE IL RUOLO**
  - *Dipendente del Titolare o del Responsabile*
  - *oppure*
  - *Un Esterno con "contratto di servizi"*

New

Il Data Protection Officer (3/4)

- **CONOSCIBILITA'**
  - *Dati di contatto comunicati al Garante*
  - *Indicati nell'Informativa*
- **GARANZIE**
  - *Deve essere tempestivamente e adeguatamente coinvolto nelle questioni privacy*
  - *Supportato con le risorse necessarie a svolgere i compiti*
  - *Indipendente e autonomo nel ruolo. Non deve ricevere istruzioni*
  - *Riferisce direttamente al vertice gerarchico*
  - *Può essere contattato direttamente dagli interessati*
  - *Può svolgere altri incarichi purchè no conflitto di interessi*
  - *Non può essere rimosso per l'adempimento dei propri compiti*

New

Il Data Protection Officer (4/4)
COMPITI

"Piccolo Garante" in Azienda

- **INFORMAZIONE E CONSULENZA**
  - Al Titolare, al Responsabile , agli Incaricati in merito ai loro obblighi
- **SORVEGLIANZA**
  - In merito all'osservanza del Regolamento e delle Policies aziendali e l'attribuzione delle responsabilità;
    - ✓ quindi: il rispetto dei diritti dell'interessato Informativa, Consenso, Accesso ai dati/ delle Misure di sicurezza/ della Notifica delle violazioni/ del principio di privacy by design/ della valutazione di impatto / della conservazione della documentazione, l'effettuazione dei controlli...)
  - Sensibilizza il personale e ne cura la formazione, inclusi gli auditors
- **SUPPORTO E INDIRIZZO**
  - Fornisce, se richiesto, parere in merito alla Valutazione di Impatto e ne sorveglia il seguito
- **RELAZIONI CON ESTERNO**
  - Coopera col Garante: le sue coordinate devono essere notificate
  - Punto di contatto con gli Interessati- coordinate nell'Informativa

LE SANZIONI

QUADRO SANZIONATORIO AMMINISTRATIVO MUTATO

SANZIONI PENALI CONFERMATE E MODIFICATE

INTRODUZIONE NUOVE SANZIONI PENALI DA D.LGS 101/2018

LE VIOLAZIONI DELLA PRIVACY E IL SISTEMA SANZIONATORIO- art 77 segg

SANZIONE AMMINISTRATIVA

RISARCIMENTO DANNI

SANZIONE PENALE

DANNO DI IMMAGINE

LE SANZIONI AMMINISTRATIVE

- **AUTORITA' CHE LE INFLIGGE**
  - *Garante della Privacy*
- **SORGENTE**
  - *A seguito di indagini*
  - *A seguito di reclami*
- **CONTENUTO**
  - ***In casi lievi :*** *avvertimento, ammonimento*
  - ***Altro:*** *ingiunzione, inibizione del trattamento, sanzione pecuniaria*
- **OPPOSIZIONE**
  - *Ammesso ricorso all'A.G. contro decisione Garante*

Sanzioni – Art. 84

Il testo di Regolamento Europeo, rafforzato dal Parlamento Europeo, prevede sanzioni amministrative pecuniarie particolarmente elevate, anche proporzionate al volume di affari realizzato da una società, e dissuasive soprattutto per i Big Data.

Fino a 10.000.000 di € o

del fatturato mondiale annuo

- Violazioni degli obblighi del Responsabile e dell'Incaricato del Trattamento
- Violazione degli obblighi dell'organismo di certificazione
- Violazione degli obblighi dell'organismo di controllo

Fino a 20.000.000 di € o

del fatturato mondiale annuo

- Mancata osservanza di un ordine da parte dell'Autorità di controllo
- Violazione di nome su consenso, trasferimento verso paesi terzi e diritti degli interessati
- Mancata osservanza di leggi degli Stati membri

Il legislatore prevede un avvertimento scritto o una serie di verifiche periodiche presso il Responsabile, qualora questi abbia violato le norme per la prima volta e in caso di semplice colpa.

Le Sanzioni Amministrative
PECUNIARIE

New **PRINCIPI GENERALI**

- *Deve essere: effettiva, proporzionata, dissuasiva*

New **VALORE**

- *Notevolmente rafforzato*
- *Fino a 20 Milioni di euro*

o

- *Fino al 4% del Fatturato mondiale /anno precedente*

New **CRITERI**

- *Natura e gravità , durata*
- *Carattere intenzionale o colposo*
- *Recidività*
- *Altre aggravanti,/ attenuanti*

IL RISARCIMENTO DEL DANNO- art 82

- **CHI PUO' CHIEDERE IL RISARCIMENTO**
  - *Chiunque abbia subito un danno: Interessato o terzo*
- **COSA PUO' CHIEDERE**
  - *Danni patrimoniali*
  - *Danni non patrimoniali*
- **A CHI DEVE RIVOLGERSI**
  - *All'Autorità Giudiziaria.*
- **CONTRO CHI**
  - *Titolare o Responsabile autore della violazione*
- **ESONERO DA RESPONSABILITA'**
  - *Evento dannoso non imputabile*

New

SANZIONI PENALI –art 84

- **REGOLAMENTO UE**
  - *Non le contempla direttamente*
  - *Rimanda a leggi nazionali degli Stati membri*

- **LEGGI NAZIONALI**
  - *Pene detentive*
  - *Sottrazione profitti*

INADEMPIMENTO	D.Lgs n. 101/2018
Omessa o inidonea informativa All'interessato. (Art. 161)	ABROGATO
Assenza informativa nei casi di dati sensibili o giudiziari o in caso di trattamenti che presentano rischi specifici o di maggiore rilev	ABROGATO
Omessa o incompleta notificazione al Garante Privacy. (Art.163)	ABROGATO
Omessa informazione o esibizione di documenti richiesti dal garante Privacy. (Art.164)	ABROGATO
Trattamento illecito di dati personali. (Art. 167 c.1.)	**Reclusione da 6 mesi a 1 anno e 6 mesi**. La pena è diminuita se il Garante ha riscosso la sanzione amministrativa
Trattamento illecito di dati personali. (Art. 167 c.2)	**Reclusione da 1 a 3 anni**. La pena è diminuita se il Garante ha riscosso la sanzione amministrativa. .
Trattamento illecito di dati personali. (Art. 167 bis c.1) *(Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala)*	**Reclusione da 1 a 6 anni.**

CAPO III – Illeciti Penali
Art. 167 (*Trattamento illecito di dati)*

- 1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è **punito con la reclusione da sei mesi a un anno e sei mesi.**

- 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al rattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-*sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2- septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2- quinquiesdecies arreca nocumento all'interessato****, è punito con la reclusione da uno a*** **tre anni.**

CAPO III – Illeciti Penali
Art. 167 (*Trattamento illecito di dati)*

- 3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli
- 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.
- 6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.

CAPO III – Illeciti Penali

Art. 167 - *bis* (*Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala)*

- 1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-*ter, 2-sexies e 2-octies, è punito* **con la reclusione da uno a sei anni.**

- 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, **è punito con la reclusione da uno a sei anni,** quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.

CAPO III – Illeciti Penali
Art. 167–*ter*(*Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala)*

c.1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è pun**ito con la reclusione da uno a quattro anni.**

1 a 4 anni

CAPO III – Illeciti Penali

Art. 168 (*Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante)*

C 1. Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con **la reclusione da sei mesi a tre anni.**

C 2. Fuori dei casi di cui al comma 1, è punito con la **reclusione sino ad un anno** chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.

CAPO III – Illeciti Penali
Art. 170 (*Inosservanza di provvedimenti del Garante)*

C 1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera *f) del Regolamento, dell'articolo 2-septies,* comma 1, nonché i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163 è punito **con la reclusione da tre mesi a due anni.**

3 mesi a 2 anni

Reati informatici

- Reati compiuti per mezzo o nei confronti di un sistema informatico. L'illecito può consistere nel sottrarre o distruggere le informazioni contenute nella memoria del personal computer. In altri casi, invece, il computer concretizza lo strumento per la commissione di reati, come nel caso di chi utilizzi le tecnologie informatiche per la realizzazione di frodi. La prima normativa contro i cyber crimes L. 547/1993:

- Frode informatica (art. 640): consiste nell'alterare un sistema informatico allo scopo di procurarsi un ingiusto profitto (Phishing)
- Accesso abusivo a un sistema informatico o telematico (art. 615 ter) : condotta di colui che si introduce in un sistema informatico o telematico protetto da misure di sicurezza o vi si mantiene contro la volontàdi chi ha il diritto di escluderlo o violando le prescrizioni del titolare del sistema.
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici (art. 614 quater c.p.) : al fine di procurare a sé o ad altri un profitto o di arreca ad altri un danno, riproducendo, diffondendo, comunicando o consegnando codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni idonee

-

Reati informatici

- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies) chi si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione o l'alterazione.
- Intercettazione, impedimento o interruzione illecita di comunicazioni (artt. 617 quater e 617 quinquies) chi, senza essere autorizzato, intercetta, impedisce, interrompe o rivela comunicazioni informatiche e colui che installa apparecchiature dirette ad intercettare, interrompere o impedire comunicazioni informatiche.
- Falsificazione, alterazione, soppressione di comunicazioni e danneggiamento di sistemi (art. 617 sexies) Chi falsifica, altera o sopprime la comunicazione informatica acquisita e chi distrugge, deteriora, cancella, dati, informazioni o programmi informatici (articolo 635 bis c.p.).
-

Question Time


grazie