



La Sicurezza delle Informazioni e Nuovo Regolamento Europeo

Davide Vedelago
Marco Rosina

dvedelago@Scuadra.it
mrosina@Scuadra.it

Il contesto in cui operiamo

Il contesto

L'Incremento del volume dei dati gestiti dalle aziende e dei canali a disposizione per accedervi hanno portato nuove opportunità



Al contempo, una crescita delle potenziali minacce ai requisiti di confidenzialità, integrità e disponibilità delle informazioni



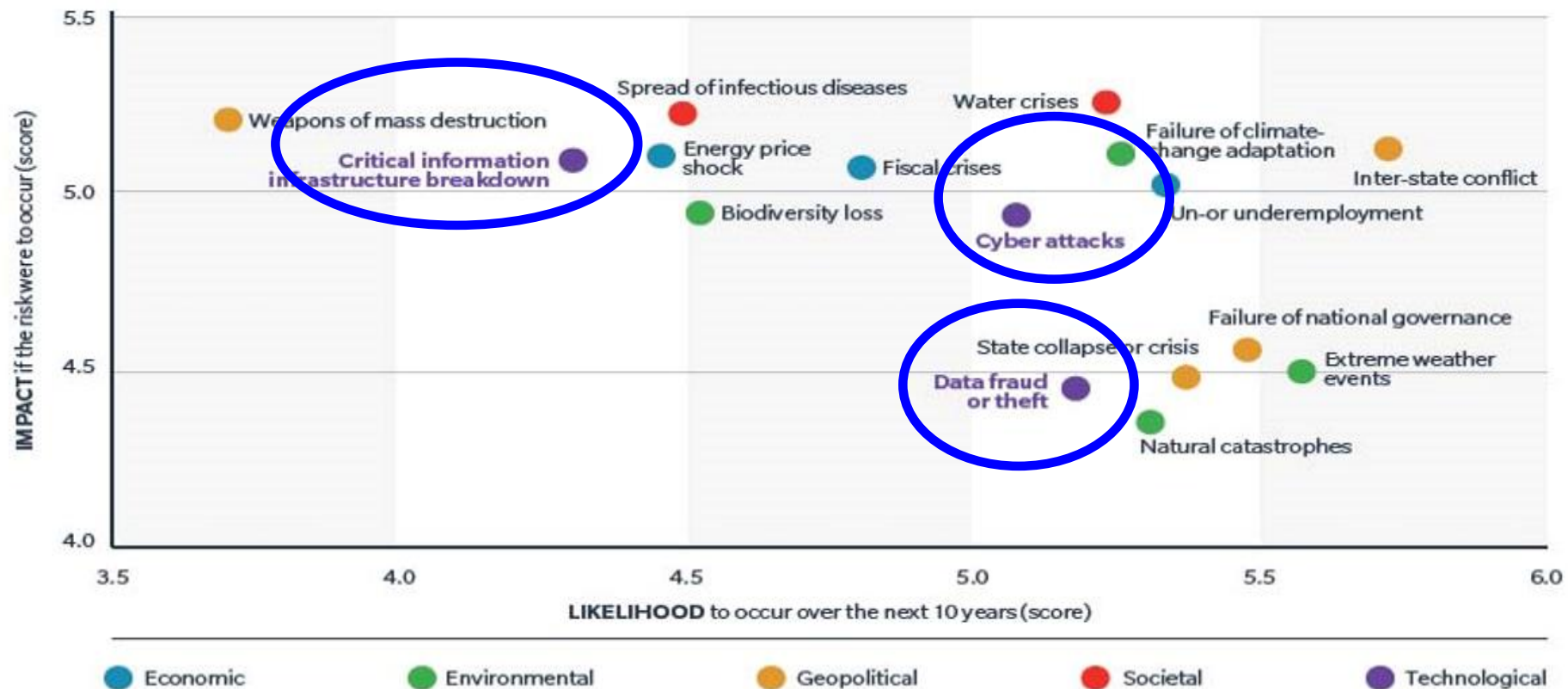
Diventa rilevante un approccio strutturato alla gestione delle informazioni, mitigare il rischio divulgazione o compromissione dell'informazioni e Data Breach



Il contesto

In the World Economic Forum's Global Risks 2015 report, cyber risk is firmly positioned as a major risk in terms of likelihood and impact: It is recognised as one of the top commercial risks along with geopolitics, the environment, and the economy.

FIGURE 2: TOP GLOBAL RISKS ACCORDING TO THE WORLD ECONOMIC FORUM



Note: Top 10 risks in terms of impact and the top 10 risks in terms of likelihood. Four Risks rank in the top 10 in terms of both impact as well as likelihood. Respondents were asked to rate each risk, based on its impact and likelihood, on a scale from 1 to 7.

Il contesto

FIGURE 4: RISK PROFILE FOR LARGE BUSINESSES



Il contesto: Italia

ATTACCHI HACKER

dati di gennaio 2017 rispetto a gennaio 2016

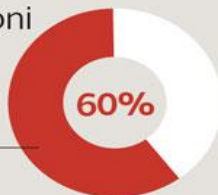
crimini informatici

+30%

spionaggio e furto di informazioni

+40%

organizzazioni
che risultano nel mirino



SPESA A CARICO DELLE AZIENDE

danni da hackeraggio in milioni di euro

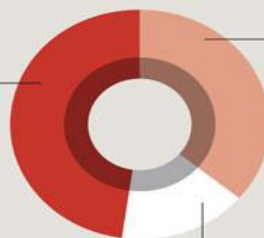


CHI COMPIE I REATI

associazioni
criminali

48%

hacker
36%



competitor
16%

COSA TEMONO I MANAGER?

risposta multipla

interruzione operatività
aziendale

55%

perdita di dati personali

50%

informazioni
alla concorrenza

42%

problemi di immagine

36%

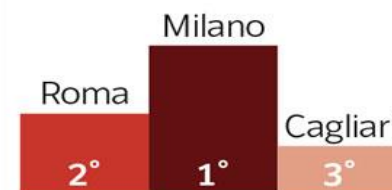
costo per danni
da hackeraggio

34%

utilizzo improprio
di dettagli finanziari

32%

LE CITTÀ COINVOLTE



Fonte: ricerca del Security Lab di Bicocca

centimetri





La classificazione delle informazioni

Il ciclo di vita delle informazioni

L'informazione è una notizia, dato o elemento che consente di avere conoscenza più o meno esatta di fatti, situazioni, modi di essere. In senso più generale, anche la trasmissione dei dati e l'insieme delle strutture che la consentono.



Classificazione delle informazioni

C - PUBBLICHE

NON RICHIEDONO ALCUN
CONTROLLO ESSENDO
DESTINATE AD UNA
FRUIZIONE PUBBLICA
(dati CCIAA, web)

B - DIFFUSE INTERNAMENTE ALL'AZIENDA

SONO A DISPOSIZIONE
DEL PERSONALE
AZIENDALE ED AGLI
ESTERNI AUTORIZZATI IN
FUNZIONE DEL RUOLO



A - RISERVATE

INFORMAZIONE CHE
VIENE SERBATA O
RISERVATA
ESCLUSIVAMENTE A
DETERMINATE PERSONE

INFORMAZIONI RIVOLTE
A DESTINATARI
SPECIFICI E SONO
RIGOROSAMENTE
DISCIPLINATE DAL
PRINCIPIO DELLA
NECESSITÀ DI SAPERE

Classificazione delle informazioni



NORMATIVA
ITALIANA SULLA
PRIVACY

NUOVA
NORMATIVA
EUROPEA
SULLA PRIVACY

REGOLAMENTI
AUTORITA'
GARANTE

Classificazione delle informazioni: esempi

- Volume d'affari
- Numero di dipendenti
- Bilanci
- Statistiche di produzione
- I piani strategici aziendali;
- Gli accordi societari;
- Progetti di investimento;
- I dati relativi al personale quali assenze, presenze, ferie, malattie e retribuzioni;
- Parametri aziendali di prestazione e di produttività;
- Accordi e contrattualistica di impresa;
- Il know-how relativo alla produzione, ai processi ed i brevetti;
- I manuali e le procedure aziendali;
- Le banche dati fornitori, clienti, dipendenti;
- Listini di acquisto e di vendita
- Documentazione tecnica di prodotto.
- Gli accordi e contratti commerciali;

Security Data Governance

Gestione operativa della riservatezza

Security Data Governance

- Sono consapevole dei requisiti di data protection?
 - Rispetto i requisiti di legge e i regolamenti?

Normative e regolamenti

- D. Lgs. 8 Giugno 2001, n. 231
- D. Lgs. 30 Giugno 2003, n. 196
- Regolamenti Autorità Garante
- Regolamento europeo 679/2016

Standard

- ISO 2700x
- ISO 2230x
- ITIL

Security Data Governance

Per Security Data Governance si intende l'insieme di PROCESSI e di STRUMENTI tesi a GARANTIRE l'efficace GESTIONE, in termini di VALORIZZAZIONE e di PROTEZIONE, delle informazioni aziendali

Security Data Governance: I benefici

- Più CONOSCENZA e CONTROLLO sul patrimonio informativo aziendale
- RIDUZIONE RISCHI di compromissione patrimonio informativo aziendale
- PIANIFICAZIONE strutturata di interventi MIGLIORATIVI sui processi e infrastruttura IT
- RIDUZIONE dei COSTI di GESTIONE delle informazioni non *business critical* e costi collegati a PROCEDIMENTI SANZIONATORI
- CONSAPEVOLEZZA personale vs il LIVELLO di RISERVATEZZA delle informazioni e procedure da adottare per la loro tutela

Security Data Governance: le minacce

Risorse Umane



Asset
informativi
strategici
incustoditi



Social
Engineering



Disattenzione
/incuria nel
modificare i
dati



Hacking



Dipendenti o
collaboratori
infedeli

Ambiente



Tecnologia



Malfunzionamento
compromissione
HW e SW



SW
malevolo



Le misure da intraprendere

Le misure da intraprendere

**MISURE
ORGANIZZATIVE**

**MISURE
TECNOLOGICHE**

Le misure da intraprendere: Misure Organizzative

Modello
Gestione delle
informazioni

Policy,
procedure,
adempimenti

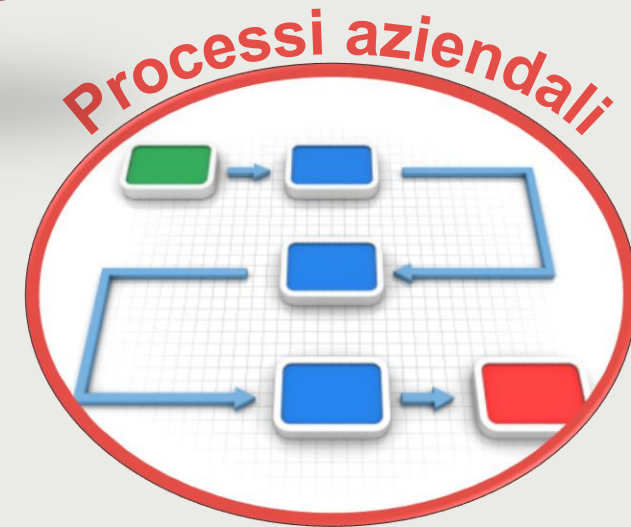
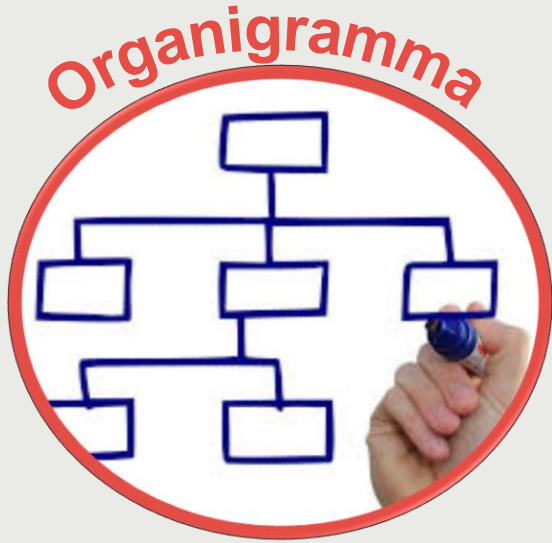
Formazione
comunicazione
sensibilizzazione

Le misure da intraprendere: il modello di gestione

Modello Gestione delle informazioni

- Classificare le informazioni (riservate, interne, pubbliche)
- Individuare e Analizzare le informazioni
- Identificare chi ha accesso ai dati (Ruolo)
- Definire la modalità di conservazione
- Identificare l'idoneo luogo di conservazione
- Dichiarare le modalità di trasferimento e fruizione
- Identificare i responsabili del processo

Le misure da intraprendere: il modello di gestione



Le misure da intraprendere: policy e procedure

Policy, procedure, adempimenti

- Definire policy, regolamenti, linee guida
- Indicare le informazioni a cui ciascun ruolo può aver accesso
- Definire il regolamento per la gestione delle informazioni riservate
- Inserire clausole di riservatezza
- Stipulare contratti dettagliati con obblighi e responsabilità
- Definire il regime sanzionatorio

Le misure da intraprendere: policy e procedure

Consulenti:
clausola
riservatezza

Azienda: codice
etico, regolamento,
clausole non
concorrenza e
riservatezza, regime
sanzionatorio

**Fornitori
sensibili:**
clausola
riservatezza,
manuale di
fornitura

Le misure da intraprendere: segregazione fisica



- Segregazione delle informazioni riservate in aree protette (area server, R&D, Archivio, Ufficio del personale ...)
- Accesso con RFID in base al profilo
- Monitoraggio accessi

Security Data Governance : codice etico

Che cosa si intende per divulgazione dannosa delle informazioni riservate o di proprietà?

- La divulgazione di una proposta di un cambiamento a livello organizzativo o esecutivo potrebbe influire sul morale del personale e interferire con i piani di [REDACTED]
- La divulgazione di una negoziazione riservata tra [REDACTED] e un cliente potrebbe offrire alla concorrenza l'opportunità di interferire e, potenzialmente, dare il tempo di creare soluzioni equivalenti, nonché violare un eventuale accordo di riservatezza con il cliente.

Un nuovo collaboratore non ha ancora accesso a [REDACTED] Posso prestargli la mia password?




No, deve attendere che gli venga fornita la sua password. La password è la chiave che permette l'utilizzo della firma elettronica che implica vincoli legali e quindi sei responsabile di qualsiasi attività svolta con la tua password.






















Grazie a un controllo accurato sulle password e alla richiesta di modifica periodica, proteggiamo i nostri dati

Investiamo nella creazione di asset e proteggiamo le informazioni riservate e di proprietà di [REDACTED]

Security Data Governance : norma ISO 27001:2014

SICUREZZA DELLE INFORMAZIONI AUDIT CONFORMITA' ALLA NORMA ISO 27001:2014

se >= 90% 
se >= 70% 
se < 70% 

DESCRIZIONE	PUNTI	MAX	INDICE
<u>A SINTESI GENERALE</u>	293	480	 61%
<u>A.5 Politiche per la sicurezza delle informazioni</u>	4	10	 40%
<u>A.6 Organizzazione della sicurezza delle informazioni</u>	12	20	 60%
<u>A.7 Sicurezza delle risorse umane</u>	17	30	 57%
<u>A.8 Gestione degli asset</u>	25	50	 50%
<u>A.9 Controllo degli accessi</u>	59	65	 91%
<u>A.10 Crittografia</u>	4	10	 40%
<u>A.11 Sicurezza fisica e ambientale</u>	28	45	 62%
A.11.2 Apparecchiature	28	45	 62%
<u>A.12 Sicurezza delle attività operative</u>	34	60	 57%
A.12.1 Procedure operative e responsabilità	12	20	 60%
A.12.2 Protezione dal malware	3	5	 60%
A.12.3 Backup	4	5	 80%
A.12.4 Raccolta di log e monitoraggio	10	20	 50%
A.12.5 Controllo del software di produzione	0	0	N/A
A.12.6 Gestione delle vulnerabilità tecniche	5	10	 50%
A.12.7 Considerazioni sull'audit dei sistemi informativi	0	0	N/A
<u>A.13 Sicurezza delle comunicazioni</u>	22	35	 63%
<u>A.14 Acquisizione, sviluppo e manutenzione dei sistemi</u>	25	35	 71%
<u>A.15 Relazioni con i fornitori</u>	10	25	 40%
<u>A.16 Gestione degli incidenti relativi alla sicurezza delle informazioni</u>	20	35	 57%
<u>A.17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa</u>	9	20	 45%
<u>A.18 Conformità</u>	24	40	 60%

- Conformità a standard internazionali e norme tecniche
- Indice Sintetico globale
- Indici specifici per area
- Obiettivi di miglioramento
- Audit periodici

Security Data Governance : formazione e comunicazione

**Formazione
comunicazione
sensibilizzazione**

- **Condividere gli obiettivi di tutela delle informazioni**
- **Formare il personale in merito ai rischi di utilizzo del PC, Web, Posta elettronica, Social, etc.**
- **Rendere pubbliche policy e regolamenti**
- **Condividere il regime sanzionatorio**

Security Data Governance : misure tecnologiche

**Sicurezza
Perimetrale /
infrastrutturale**



**Gestione degli
accessi e profili**



Log & Monitoring



**Disaster recovery
& Business
continuity**



Database security

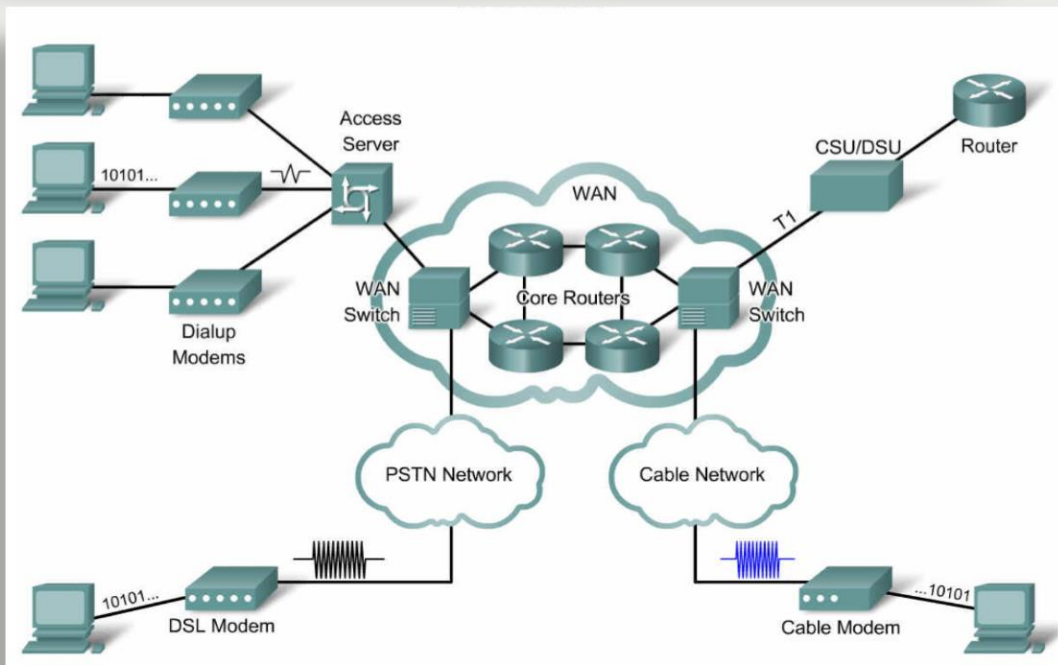


Crittografia



Security Data Governance : sicurezza di rete

Soluzioni di sicurezza Perimetrale / infrastrutturale



- Mappa di rete
- Manutenzione ed aggiornamento
- Monitoraggio delle risorse
- Controlli periodici
- Ambienti idonei
- Separazione reti
- VPN

Security Data Governance: Misure Tecnologiche

Gestione degli accessi e profili

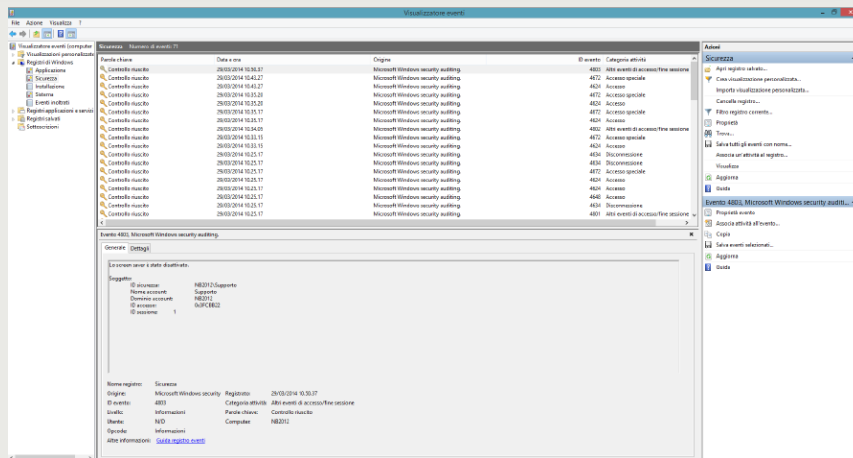


- Rilascio delle credenziali
- Conservazione password
- Profilazione utenti
- Group Policy
- Profilazione ADS
- Organigramma privacy

Security Data Governance: Log & Monitoring

Log & Monitoring

- Log eventi
- Filtri traffico
- Assistenza remota
- Log ADS
- Notifiche
- Verifiche
- Finestre di accesso



Le misure da intraprendere: sicurezza di rete



Security Data Governance: Misure Tecnologiche

Disaster recovery

- **Necessità aziendali**
- **Test ripristino**
- **Tempi/punti ripristino**
- **Localizzazione**



Security Data Governance: Misure Tecnologiche

Business continuity



- **Valutazione processi**
- **Criticità**
- **BIA**
- **Alta affidabilità**
- **Gestione intervento**

Database security

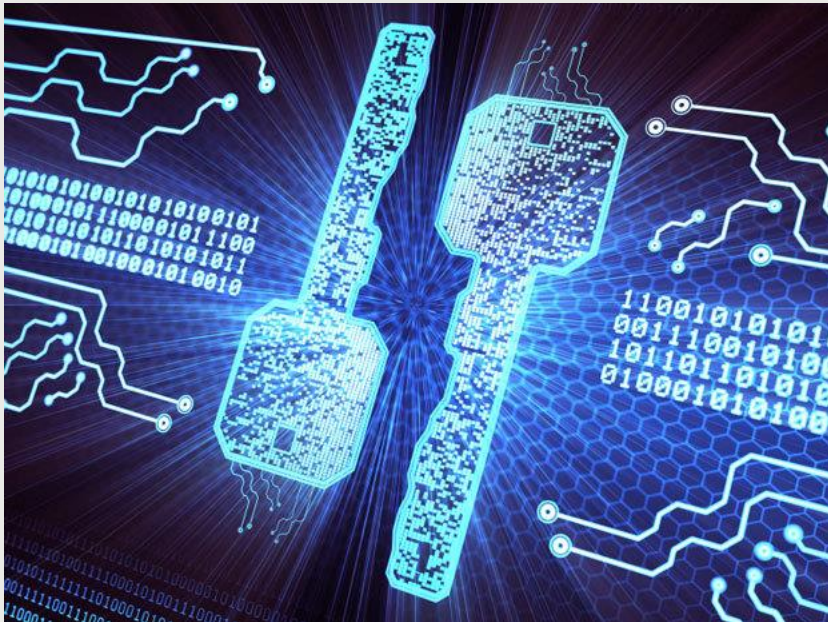
- Policy accesso ad hoc
- Log
- Backup
- Cifratura
- Ambienti test/sviluppo



Security Data Governance: Misure Tecnologiche

Crittografia

- Dispositivi mobili
- Supporti removibili
- Mail
- Archivi
- Firma digitale



Regolamento Europeo Protezione Dei dati GDPR 679/2016

Attuale impianto normativo



- **D. Lgs. 30 Giugno 2003, n. 196**
- **Allegato B Misure minime di sicurezza**
- **Provv. Amministratori di sistema**
- **Provv. Videosorveglianza**
- **Provv. Localizzazione dei veicoli**
- **Linee guida**
- **Autorizzazioni generali**

Reg. UE 679/2016

«Protezione delle persone fisiche con riguardo al trattamento dei dati personali e libera circolazione di tali dati»



- Obiettivo: armonizzazione normativa UE
- Self-executing = direttamente esecutivo
- Entrata in vigore 24 maggio 2016
- Applicabile dal 25 maggio 2018
- Integrabile dai legislatori nazionali

Reg. UE 679/2016

Ambito di applicazione

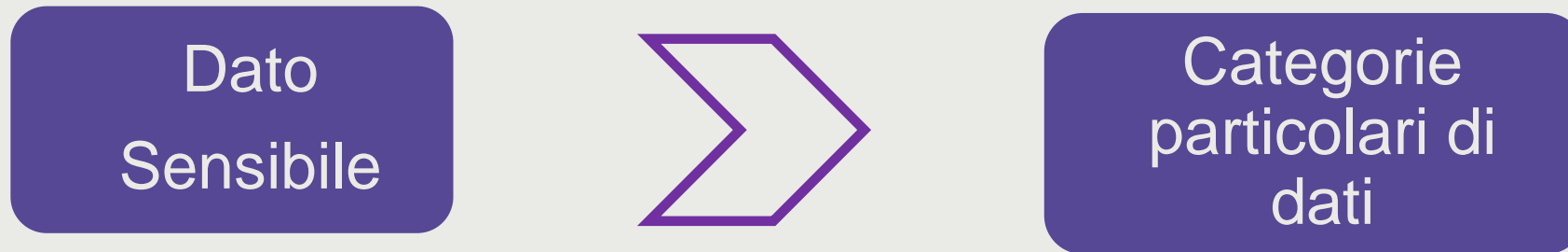
Trattamento dei DATI PERSONALI dei residenti nell' Unione Europea operato da un RESPONSABILE anche non stabilito nell'UE se:

- Offerta di Beni o servizi ai residenti UE
- Avviene la profilazione del comportamento degli interessati

DATI PERSONALI: *qualsiasi informazione riguardante una persona fisica identificata o identificabile*

Reg. UE 679/2016

Categorie particolari di dati



E' VIETATO TRATTARE DATI PERSONALI che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Reg. UE 679/2016

Categorie particolari di dati

IL DIVIETO NON SI APPLICA SE (alcuni esempi)

- **Esiste un consenso esplicito**
- **E' necessario assolvere obblighi o esercitare diritti da parte del titolare del trattamento e dell'interessato**
- **E' necessario tutelare l'interesse vitale dell'interessato o di altra persona fisica**
- **E' necessario per la tutela di un interesse pubblico**
- **E' necessario per interventi di medicina preventiva o medicina del lavoro**

Reg. UE 679/2016

Responsabilità

RESPONSABILE del trattamento attua

MISURE TECNICHE ed ORGANIZZATIVE ADEGUATE

- **Natura, ambito di applicazione, rischi e probabilità**
- **Garanzia del trattamento**
- **Dimostrabilità**
- **Conformità del regolamento**
- **Riesame, aggiornamento e verifica**

Reg. UE 679/2016

Accountability

Responsabile deve osservare il Principio di RENDICONTAZIONE:

- **Conservazione informazioni sui trattamenti**
- **Conformità al Regolamento**
- **Informazioni specifiche per ciascun trattamento:**

Finalità, modalità trattamento, consenso, obblighi normativi, periodo di conservazione dei dati, ecc..

Reg. UE 679/2016

Privacy By Design - by Default

Principio Incorporazione della privacy per il trattamento dei dati NECESSARI con misure ADEGUATE

- **Progettazione processi aziendali**
- **Adozione software**
- **Formulazione di procedure**
- **Regolamenti**

Reg. UE 679/2016

Data Privacy Impact Assessment (DPIA)

Valutazione IMPATTO (Data Privacy Impact Assessment) del trattamento **NECESSARIA** se sono presenti **RISCHI SPECIFICI** per i **DIRITTI** e le **LIBERTA'** degli interessati

Alcuni esempi:

- Valutazione sistematica e globale di dati relativi a persone fisiche
- Tratt. su larga scala categorie particolari dati
- Tratt. su larga scala dati relativi condanne penali e Reati
- Sorveglianza sistematica, larga scala, zone accessibili pubblico

Reg. UE 679/2016

Data Breach

Obbligo del Titolare del trattamento di comunicare la VIOLAZIONE DEI DATI:

- **all'Autorità di controllo**
- **Senza ingiustificato ritardo**
- **Con informazioni dettagliate su: titolare, dati, trattamento, misure adottate per porre rimedio**
- **In alcuni casi anche agli interessati (rischio per diritti e libertà personali)**

Reg. UE 679/2016

DPO

TITOLARE del trattamento DESIGNA un Responsabile della protezione dei dati (Data Protection Officer) in alcuni casi

- **Pubblica Amministrazione**
- **Aziende con elevato numero di interessati**
- **Trattamenti larga scala dati personali e particolari**
- **Trattamento dati relativi a condanne penali o reati**

Reg. UE 679/2016

DPO

posizione del DPO

- **Interfaccia dell'Autorità Garante**
- **Indipendente**
- **Autonomo**
- **Riferisce solo al Titolare del trattamento**
- **Risorse adeguate allo svolgimento dell'attività**

Reg. UE 679/2016

DPO

COMPITI del DPO

- Sensibilizzare Titolare in merito agli obblighi, misure tecniche ed organizzative
- Sorvegliare l'attuazione delle misure di protezione dei dati
- Formazione del personale incaricato
- Sorvegliare *Privacy By Design e by Default*
- Controllare che le violazioni dei dati siano documentate, notificate e comunicate

Reg. UE 679/2016

Certificazioni

Gli Stati e Autorità di Controllo devono incoraggiare:

- **Emissione norme nazionali o internazionali**
- **Evidenze sulla conformità al regolamento**
- **Meccanismi di certificazione**
- **Sigilli o Marchi di protezione**

Reg. UE 679/2016

Sanzioni

DEFINITE SOLO SANZIONE AMMINISTRATIVE

- Efficace, proporzionata, dissuasiva
- Registro sanzioni e violazioni (avvertimenti, sanzioni, soluzioni)
- Fino a 20.000.000 € o 4% fatturato consolidato mondiale

Domande



www.scuadra.it
info@scuadra.it

Grazie



www.scuadra.it
info@scuadra.it