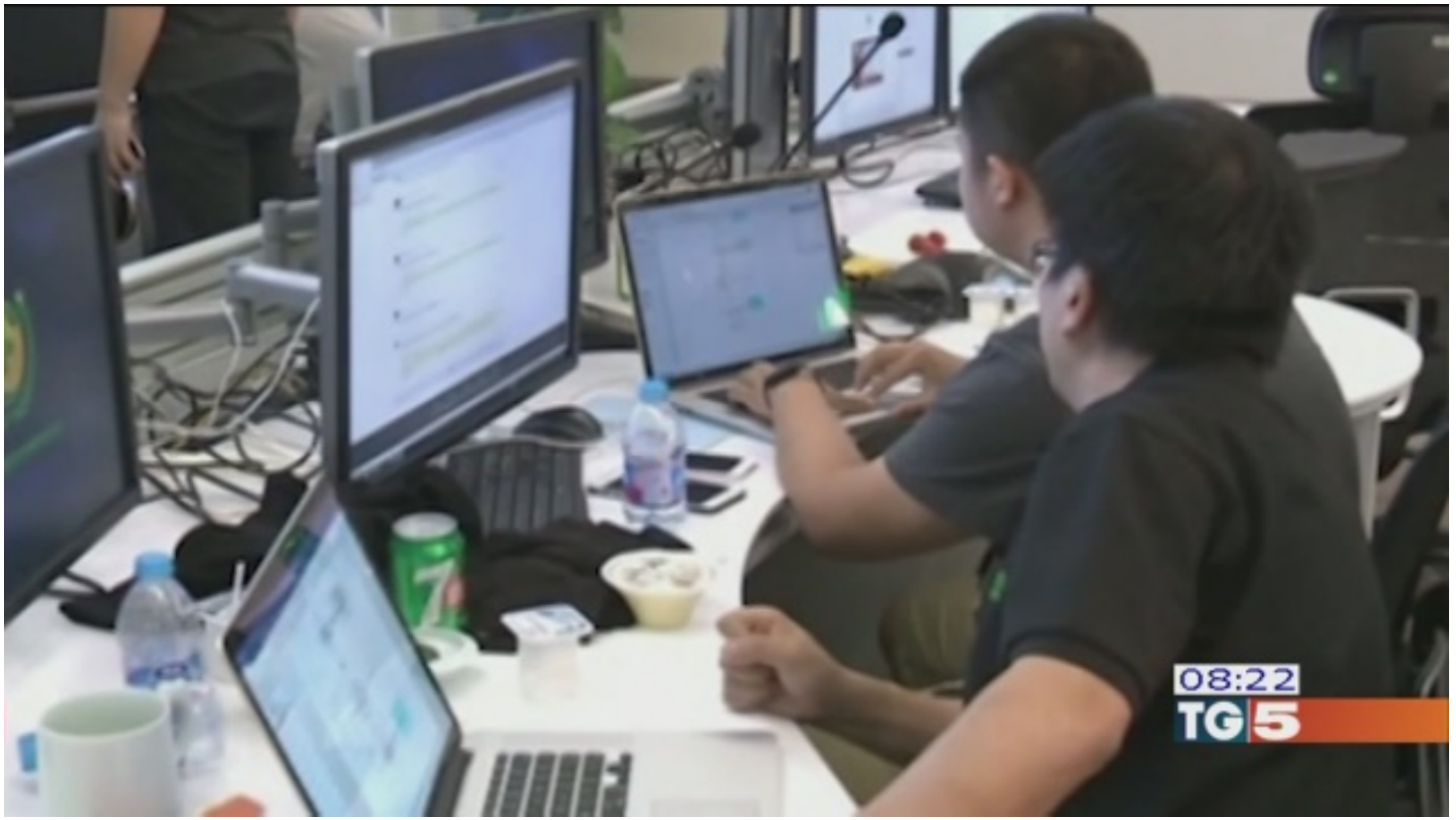
TMC
Top Management Consulting

DATA & PRIVACY RISK

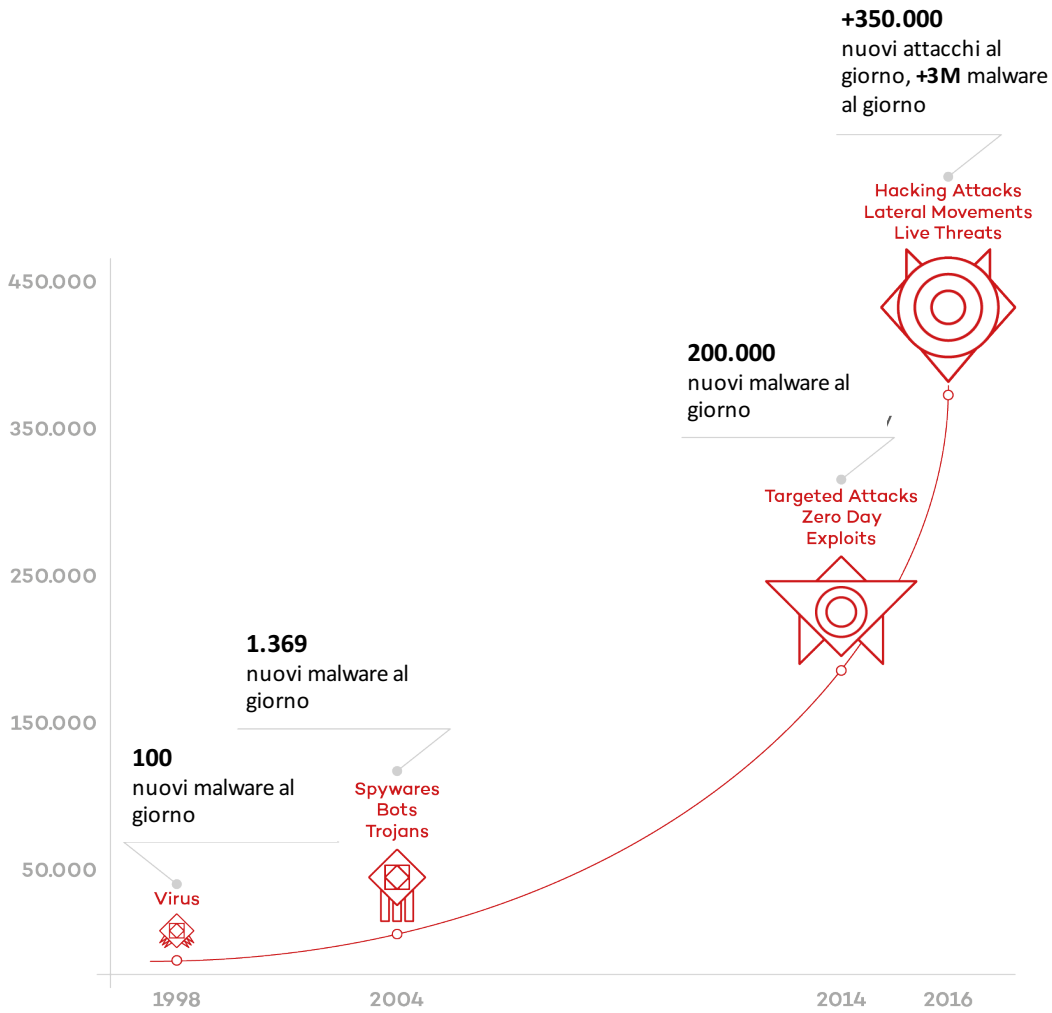
Come tutelare i propri dati di business nel rispetto del nuovo Regolamento Europeo sulla protezione dei dati (GDPR - Reg. UE 679/2016 *)*

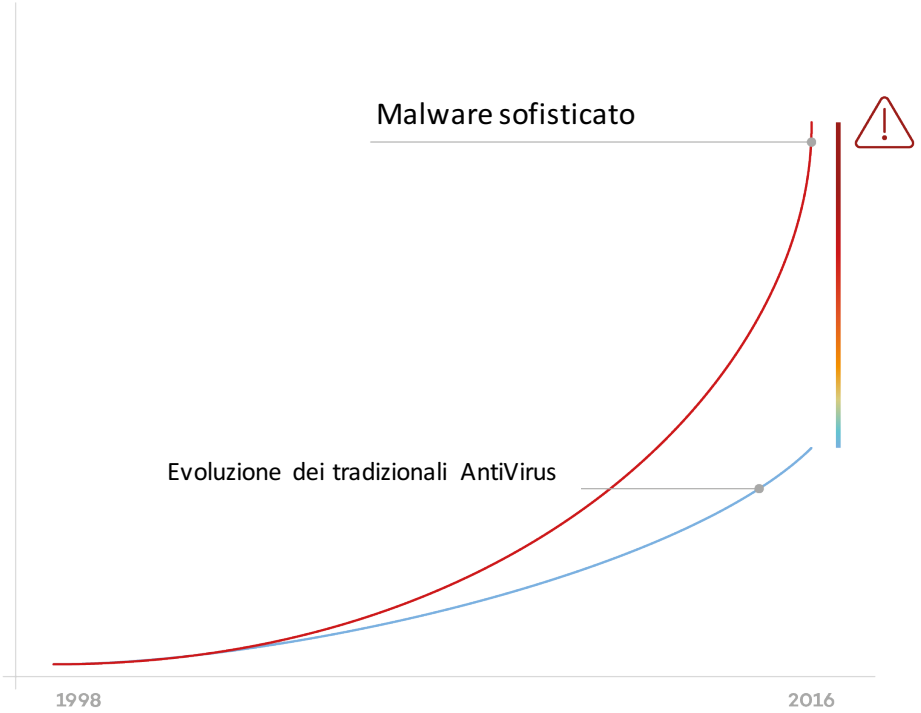
TMC
Top Management Consulting

TMC
Top Management Consulting



Evoluzione degli attacchi e fattore di successo





Fonte Panda Software

Alcuni dati del 2017

- ***Il 31,9% dei computer degli utenti ha subito, nell'anno, almeno un attacco web riconducibile alla classe dei malware***
- *Le soluzioni KL hanno respinto 758.044.650 attacchi lanciati attraverso siti Internet dislocati in ogni parte del mondo*
- *Sono stati riconosciuti come dannosi, da parte del modulo Anti-Virus Web, 261.774.932 URL unici*
- *Il 29,1% degli attacchi web neutralizzati è stato condotto attraverso risorse web malevole situate negli Stati Uniti*
- *Il modulo Anti-Virus Web ha rilevato 69.277.289 oggetti nocivi unici*
- *Gli encryptor hanno preso di mira 1.445.434 computer di utenti unici*
- *Le soluzioni KL hanno bloccato tentativi di lanciare malware capace di sottrarre denaro tramite il banking online su 2.871.965 dispositivi*
- *Il modulo Anti-Virus File ha rilevato, in totale, 4.071.588 programmi dannosi o potenzialmente indesiderabili*

Le statistiche sulle minacce mobile possono essere consultate nel report "Evoluzione del malware mobile nel 2016"

Rapporto Clusit 2017

Dilaga il cybercrime che colpisce il 100% delle aziende

Secondo il rapporto Clusit 2017, l'anno scorso gli attacchi gravi compiuti per finalità di cybercrime sono aumentati del 9,8%, con un incremento esponenziale soprattutto degli attacchi di phishing, cresciuti nell'ordine del 1.166%. I settori più colpiti? La sanità (+102%), seguita dalla grande distribuzione (+70%) e dalle banche (+64%).

L'evidenza principale dell'edizione 2017 del Rapporto è che ormai ***tutte le aziende sono sotto attacco, indipendentemente dalla dimensione o dal settore merceologico di appartenenza****.* ***"La probabilità di essere attaccati è pari a uno, ormai, basta che i malintenzionati abbiano il tempo sufficiente per agire*** *– commenta* ***A.Z.M., membro del Consiglio Direttivo del Clusit****. La definitiva consacrazione delle logiche di crime-as-a-service, infatti, permette anche ai criminali comuni di allargare il perimetro delle proprie attività illecite al web semplicemente affittando infrastrutture e strumenti di attacco dai produttori solo per il periodo strettamente necessario, a fronte del versamento di una percentuale dei proventi illeciti".*

Attaccanti competenti che usano tutte le armi

1. Intelligence (su persona e azienda)

– Sorgenti aperte

– Sorgenti chiuse

2. Psicologia

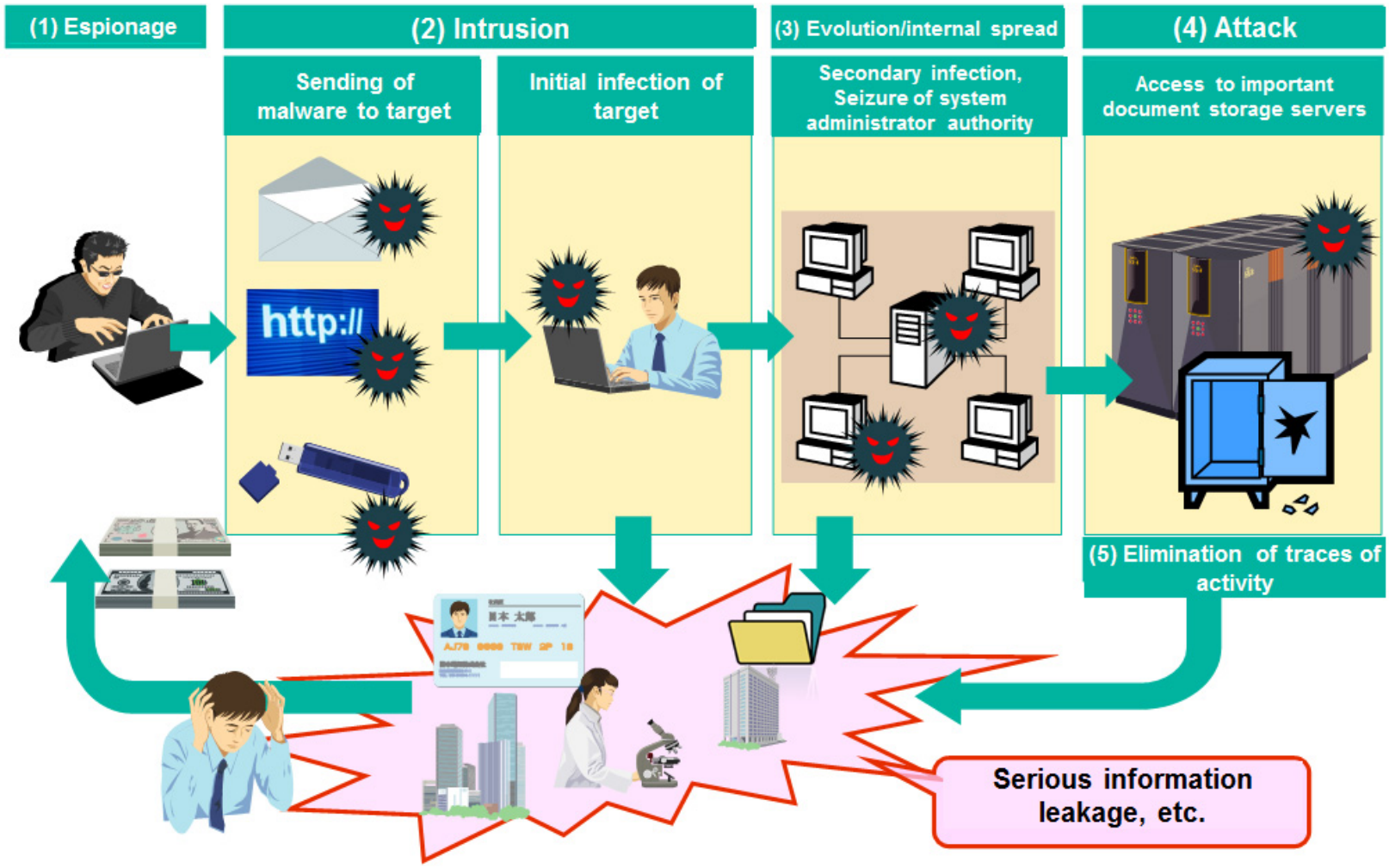
– spear phishing che sfrutta fiducia, scarsa osservanza delle regole, abitudini, ideologia, timori, bramosia di guadagni, insoddisfazione, narcisismo, ecc.

3. Tecnologia

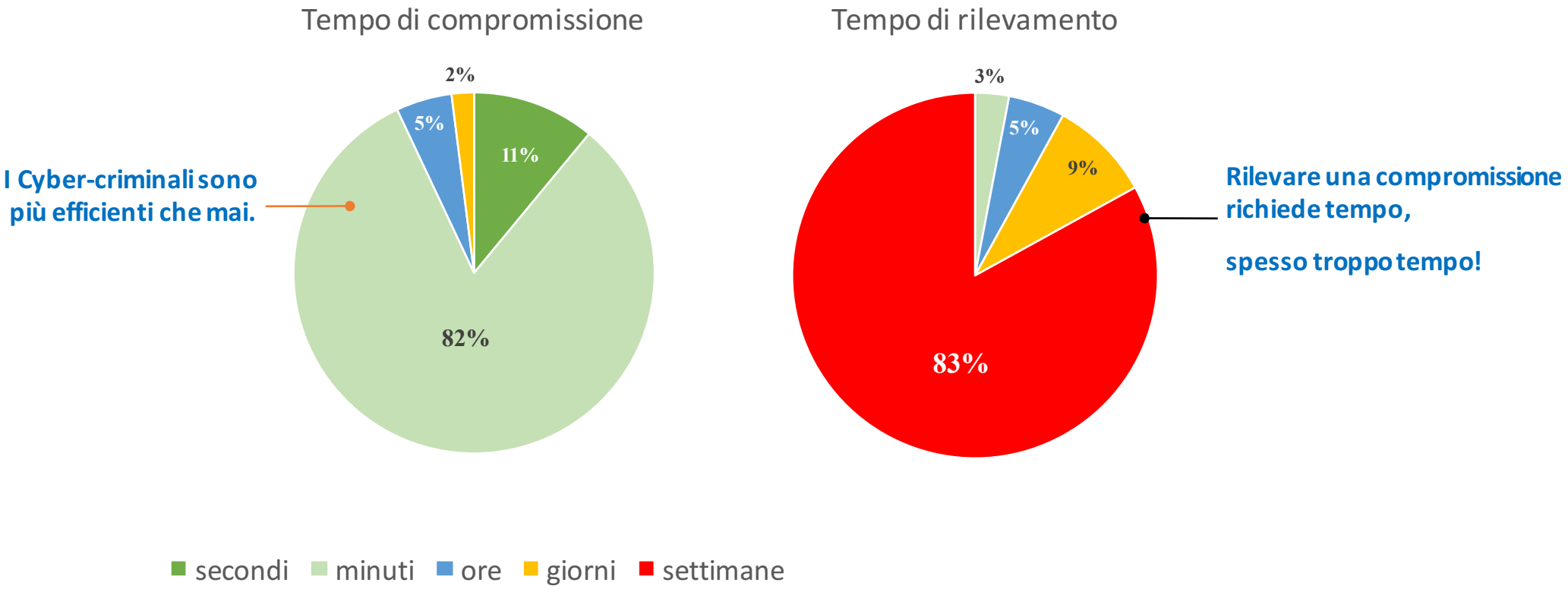
– malware inviato attraverso multipli canali di comunicazioni e sfruttando (multiple) vulnerabilità del software

TMC
Top Management Consulting

Analisi di un tipo di attacco e dei suoi effetti



Due differenti velocità ed il gap aumenta sempre



TMC
Top Management Consulting

Possibili conseguenze di un attacco

- I documenti presenti sul computer vengono **cifrati**
- I documenti diventano **illeggibili**
- I **nostri** dati vengono **rubati** e messi in rete o venduti a terze parti
- I dati dei **Clienti** vengono rubati e messi in rete o rivenduti
- I **dati personali o particolari** vengono venduti o manipolati
- I server o i mobile dovranno essere riformattati con potenziali perdite di dati
- Tutto il lavoro presente sul computer non esiste più
- Il **backup**, per chi ne è dotato, a quale data risale? E i backup sono stati a loro volta compromessi?
- Formule, disegni, progetti, brevetti vengono rubati e rivenduti
- Mail e documenti possono essere messi in rete con danno di immagine o reputazione dell'azienda e/o personale

Possibili costi di un attacco (data breach)

Costi di ripristino

Riprogettazione e aggiornamento sistemi informatici e di sicurezza, Lavoro straordinario, Riqualificazione del personale, Recupero e ridigitazione dati esterni

Interruzione di attività

Fermo di produzione, Impossibiità di erogare I servizi, Perdita di fatturato, Pagamento di penali per mancata consegna…

Responsabilità civile

Contenzioso legale (class action), Rivalsa di Clienti o dipendenti

Costi di notifica

Esame informatico forense, Stampa, spedizione e altre comunicazioni, Servizio di monitoraggio del credito

Sanzioni amministrative

Per la nuova privacy dal 2% al 4% del fatturato

Danno reputazionale

Danno all'immagine, Perdita di credibilità e di fiducia, Deprezzamento delle azioni

Costi per tutelare il brand e la reputazione

Legale, Pubbliche relazioni, Pubblicità e relative comunicazioni

TMC
Top Management Consulting

Chi viene colpito e perché?

Chiunque …per gioco ….o per soldi!!!

TMC
Top Management Consulting

QUINDI LA DOMANDA NON E' **SE** ……. MA **QUANDO**?!!

Ed avrò fatto tutto il possibile per difendermi?

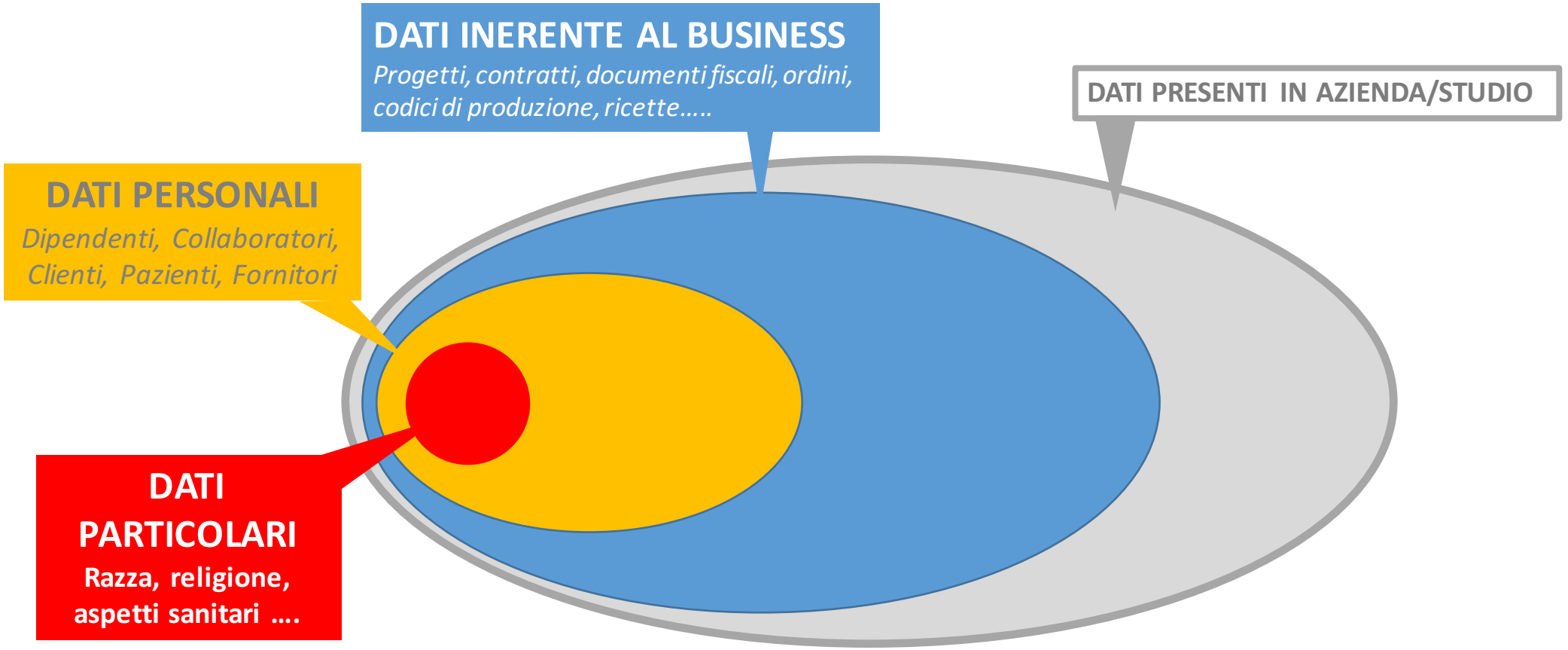
Saprò reagire tempestivamente?

Avrò fatto tutto in regola per non essere sanzionato?

Avrò attivato una copertura assicurativa adeguata?

TMC
Top Management Consulting

Ma quali sono i dati a rischio?



Ma qual'é il vero obiettivo di un attacco

Rubare i dati

- e metterli gratuitamente in rete (per sfregio, per gioco, per ragioni politiche, …)
- o rivenderli a terze parti (call center, ditte di profilazione, direct marketing,..)

Rubare Know-how

- Formule, disegni, progetti, brevetti, contratti, nomi di clienti, fatture vengono rubati e rivenduti

Rubare soldi

- Mediante richieste di riscatto dei dati (es. criptolock)
- Mediante il blocco dei servizi e la richiesta di un riscatto per il suo sblocco
- Mediante l'utilizzo improprio dei dati bancari

TMC
Top Management Consulting

Cosa prescrive il nuovo Regolamento Europeo sulla protezione dei dati (GDPR - Reg. UE 679/2016)

AVV. Riccardo Facchin

Legal consultant di TMC

Privacy: le origini e l'evoluzione normativa

1861: sentenza dei giudici inglesi -> right to be alone

→ privacy come diritto di estromettere chiunque altro dalla propria sfera privata

1948: ONU Dichiarazione universale dei Diritti dell'Uomo
1950: Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali – Consiglio d'Europa (**Art. 8 Diritto al rispetto della vita privata e familiare**)
1981: Convenzione n. 108 del Consiglio d'Europa per la protezione delle persone rispetto **al trattamento automatizzato di dati** a carattere personale
1995: Direttiva 95/46/CE del Parlamento e del Consiglio d'Europa; L. 75/1996 e DPR 318/99; D. Lgs. 196/2003 e successivi atti normativi di semplificazione; Provvedimenti del Garante;

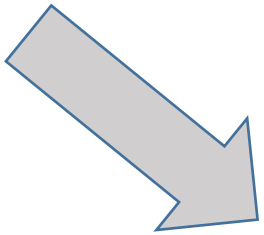
→ Privacy 1.0 **privacy come diritto della personalità; dal segreto al controllo** (società dell'informazione);

GDPR - Reg. UE 679/2016
99 articoli; 173 consideranda

General Data Protection Regulation

→ Privacy 2.0 (nativi digitali, social network, mobile apps, fidelity card): la **privacy come negoziazione sociale** - "public by default" (es. social network) VS "privacy by design" (progettare la privacy sin dall'inizio)

Decreto Legislativo 196/2003
dalla protezione del dato personale



GDPR, Capo VIII, artt. 77-84
alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

TMC
Top Management Consulting

General Data Protection Regulation

GDPR - Reg. UE 679/2016

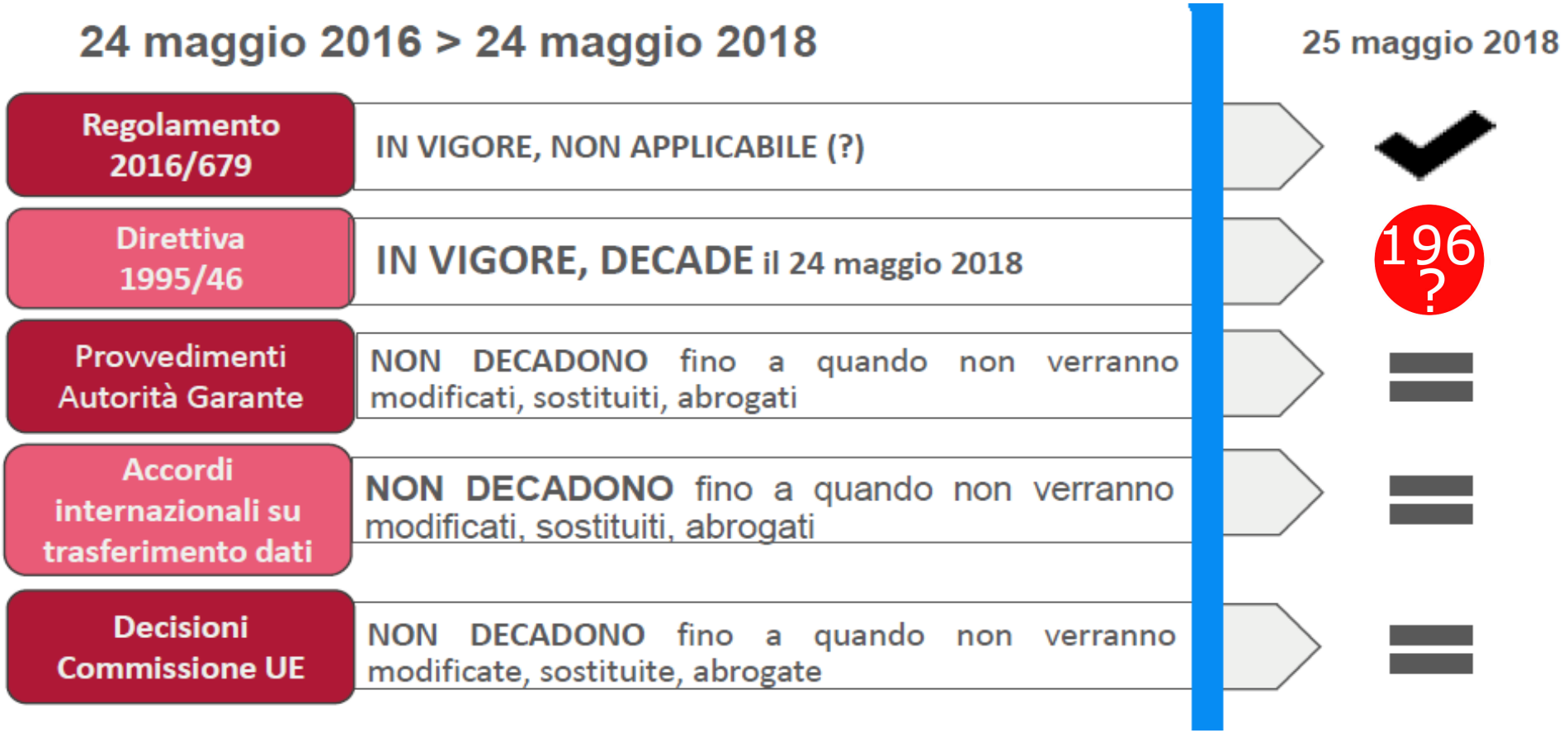
1.1. Il diritto alla protezione dei dati

Punti salienti

- Ai sensi dell'articolo 8 della CEDU, il diritto alla protezione dei dati personali relativamente alla raccolta e all'utilizzo degli stessi è parte del diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza.
- La Convenzione n. 108 del Consiglio d'Europa è il primo strumento internazionale giuridicamente vincolante che tratta in maniera esplicita della protezione dei dati.
- Il diritto dell'UE ha disciplinato per la prima volta la protezione dei dati attraverso la direttiva sulla protezione dei dati.
- **Il diritto dell'UE ha riconosciuto la protezione dei dati come un diritto fondamentale dell'uomo.**

Il diritto alla protezione della sfera privata di un individuo contro le ingerenze altrui, soprattutto da parte dello Stato, è stato sancito per la prima volta da uno strumento giuridico internazionale nell'articolo 12 della Dichiarazione universale dei diritti dell'uomo (UDHR) delle Nazioni Unite (ONU) del 1948 riguardante il rispetto della vita privata e familiare. L'UDHR ha influito sullo sviluppo di altri strumenti relativi ai diritti dell'uomo in Europa.

GDPR - Reg. UE 679/2016 – il cronoprogramma



GDPR - Reg. UE 679/2016 – i concetti chiave

DATO PERSONALE
qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente

DATO PERSONALE PARTICOLARE
dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale**, i dati genetici, i dati biometrici** intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

TRATTAMENTO
qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati applicate a dati personali o insiemi di dati personali, come

- la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione, la distruzione.

PROFILAZIONE
qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica

ACCOUNTABILITY

Dal Dizionario di Economia e Finanza Treccani

ACCOUNTABILITY

Responsabilità incondizionata, formale o non, in capo a un soggetto o a un gruppo di soggetti (accountors), del risultato conseguito da un'organizzazione (privata o pubblica), sulla base delle proprie capacità, abilità ed etica. Tale responsabilità richiede giudizio e capacità decisionale, e si realizza nei confronti di uno o più portatori di interessi (account-holders o accountees) con conseguenze positive (premi) o negative (sanzioni), a seconda che i risultati desiderati siano raggiunti o disattesi. L'accento non è posto sulla responsabilità delle attività svolte per raggiungere un determinato risultato, ma sulla definizione specifica e trasparente dei risultati attesi che formano le aspettative, su cui la responsabilità stessa si basa e sarà valutata. La definizione degli obiettivi costituisce, dunque, un mezzo per assicurare l'accountability.

Insieme al concetto di responsabilità, l'accountability presuppone quelli di **trasparenza** e di **compliance**.

TRASPARENZA intesa come accesso alle informazioni concernenti ogni aspetto dell'organizzazione, fra cui gli indicatori gestionali e la predisposizione del bilancio e di strumenti di comunicazione volti a rendere visibili decisioni, attività e risultati.

La **COMPLIANCE** si riferisce al rispetto delle norme ed è intesa sia come garanzia della legittimità dell'azione sia come adeguamento dell'azione agli standard stabiliti da leggi, regolamenti, linee guida etiche o codici di condotta. Sotto questi aspetti, l'accoutabillity può anche essere definita come l'obbligo di spiegare e giustificare il proprio comportamento.

OBBLIGHI DEL TITOLARE DEL TRATTAMENTO (art. 24)

TITOLARE DEL TRATTAMENTO:
colui che determina le finalità e i mezzi del trattamento di dati personali

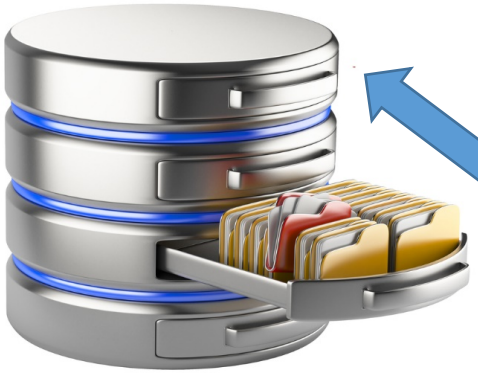
- Identificare **gli interessati e le attività di trattamento**, la loro finalità, i tempi ed i mezzi del trattamento (cd. **Registro dei trattamenti**) e garantisce il rispetto dei principi fondamentali
- Individuare **le persone autorizzate** al trattamento in base alle loro competenze specifiche e fornisce loro idonee istruzioni e formazione.
- **Individuare e Contrattualizzare** opportunamente i Responsabili (esterni) del trattamento
- Svolgere i **processi valutativi** per la nomina del **DPO**, l'effettuazione **DPIA**, la gestione del **data breach** e mettere in atto **adeguate misure tecniche e organizzative** per assicurare e dimostrare la conformità al Regolamento nonché il rispetto dei principi privacy **by design / by default**
- **Vigilare** sulla correttezza del trattamento

GDPR - Reg. UE 679/2016 – i flussi fondamentali

- Privacy by design/by default
- Risk Approach

- Organizzazione e Ruoli
- Accountability
- Processi di valutazione

DATI PERSONALI



Esercizio diritti proattivi

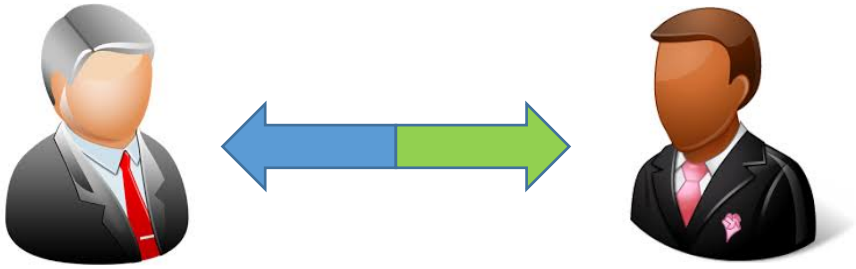
INTERESSATI

TITOLARE DEL TRATTAMENTO

Colui che **determina le finalità ed i mezzi** del **trattamento** dei **dati personali**

Rispetto e garanzia dei diritti fondamentali

DIRITTI DELL'INTERESSATO



TITOLARE DEL TRATTAMENTO

INTERESSATO

- Cliente / Utilizzatore / Utente
- Dipendente / Collaboratore
- Fornitore / Subappaltatore

IL TITOLARE DEVE GARANTIRE ALL'INTERESSATO

- **Principio dell'informazione preventiva**
- **Principio del controllo proattivo e monitoraggio (termine di risposta all'interessato 1 mese, estendibile)**
- **Principio del consenso previo al trattamento**

GDPR - Reg. UE 679/2016 – diritti dell'interessato

INTERESSATI

Principio dell'informazione preventiva

- trattati in modo lecito, corretto e **trasparente** nei confronti dell'interessato
- raccolti per finalità determinate, esplicite e legittime,
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati **(«minimizzazione dei dati»)**

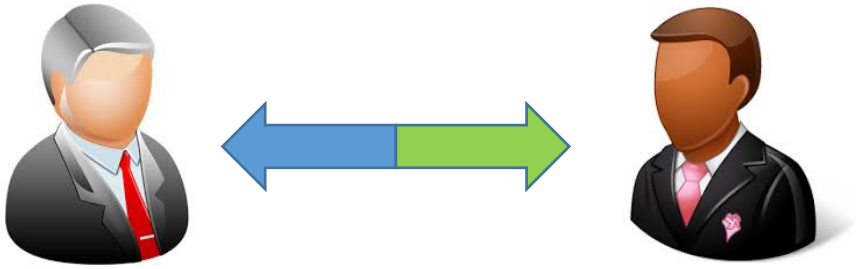
Principio del controllo proattivo e monitoraggio

- Soggetti a richiesta di accesso, modifica, cancellazione o esercizio del **diritto all'oblio**
- trattati in maniera da garantire **un'adeguata sicurezza dei dati personali che il** titolare del trattamento deve essere in grado di comprovare **(«responsabilizzazione»).**
- Diritto **alla portabilità** per trasmettere ad un altro titolare del trattamento i propri dati

Principio del consenso previo al trattamento

- Dev'essere libero (non coartato), informato, specifico (per singola finalità), non implicito (non necessariamente scritto ma inequivocabile), non presunto (no opt-out)
- **Revocabile con garanzia di una procedura non più complessa di quella adottata per la raccolta**
- Non serve nell'ambito di un contratto di cui è parte l'interessato (se i dati trattati sono comuni)

DIRITTI DELL'INTERESSATO



TITOLARE DEL TRATTAMENTO

INTERESSATO

- Cliente / Utilizzatore / Utente
- Dipendente / Collaboratore
- Fornitore / Subappaltatore

INFORMATIVA ALL'INTERESSATO

GDPR: rafforzamento del concetto di consenso informato (ex ante – ex post)

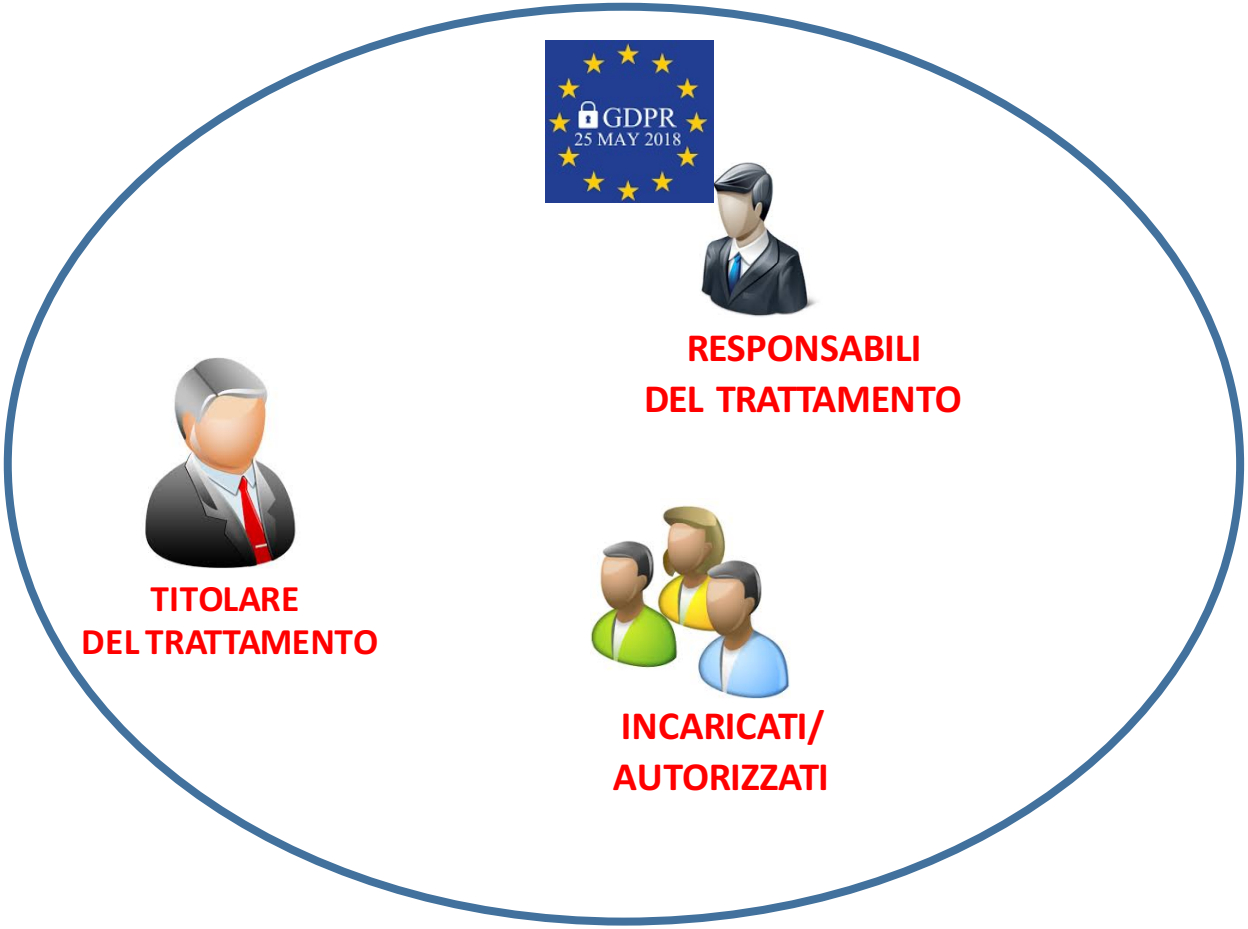
- Base giuridica: contratto (o atto giuridico)

- Requisiti: chiarezza, semplicità, senza reiterazioni, facilmente accessibile

- Contenuto: dati di contatto del DPO, base giuridica del trattamento, trasferimento dati in Paesi terzi, periodo di conservazione, accesso, cancellazione, rettifica, portabilità, strumenti di reclamo e ricorso, finalità, durata e conservazione dei dati trattati

- Tempi dell'informativa: non oltre 1 mese (dalla raccolta non dalla registrazione)

GDPR - Reg. UE 679/2016 – I RUOLI



ADEMPIMENTI CONTRATTUALI: IL RESPONSABILE

TITOLARE DEL TRATTAMENTO

nomina

RESPONSABILE DEL TRATTAMENTO

- La nomina deve essere disciplinata da un contratto, in cui sono stipulati l'argomento e la durata del trattamento, la natura e i motivi del trattamento, il tipo di dati personali e le categorie degli interessati, i doveri e i diritti
- Deve specificare le misure di sicurezza adeguate che il responsabile è tenuto a garantire ex art. 32
- Deve specificare le istruzioni che il responsabile deve seguire
- In caso di delega a sub responsabili: è richiesta l'accettazione espressa del titolare
- Deve prevedere che gli autorizzati del responsabile si impegnano a rispettare un patto di riservatezza
- Deve prevedere che anche il responsabile rediga un suo registro dei trattamenti
- Deve prevedere che anche il responsabile nomini un DPO nei casi dovuti

ADEMPIMENTI CONTRATTUALI

TITOLARE DEL TRATTAMENTO

INTERESSATO

RESPONSABILE DEL TRATTAMENTO

DIPENDENTI, AGENTI, PARTNER, COLLABORATORI ESTERNI

CLIENTI

FORNITORI, SUBAPPALTATORI

ADEMPIMENTI CONTRATTUALI

TITOLARE DEL TRATTAMENTO

C'E' UN PROBLEMA CON I DATI?
AH, IO NON SO NULLA CHIEDETE AL TECNICO!

STIA TRANQUILLO SIAMO A POSTO IL SOFTWARE FA TUTTO ED ABBIAMO L'ANTIVIRUS!

TECNICO ESTERNO NON OPPORTUNAMENTE CONTRATTUALIZZATO

= SANZIONI !!!

CONTRATTI CON I FORNITORI DI SERVIZI
(REVISIONE DELLE CLAUSOLE)

- base giuridica: contratto
- contenuto: adozione meccanismi di controllo e monitoraggio del sistema, conformità al GDPR, adozione misure di sicurezza ex ante/ex post, predisposizione misure di intervento in caso di violazione

PREVISIONE CLAUSOLE DI GARANZIA

ADEMPIMENTI FORMALI:
IL REGISTRO DEI TRATTAMENTI (art. 30)

INFORMAZIONE MINIME

Attività di trattamento	Titolare/Responsabile	Finalità	Descrizione categorie di interessati e dati personali	Categorie di destinatari	Eventuale trasferimento dei dati a paesi terzi	Termini ultimi per la cancellazione dei dati	Descrizione delle misure di sicurezza adottate ex art. 32
gestione amministrativa personale dipendente: rilevazione presenze tramite APP	xy spa	rilevazione presenze	dipendenti e collaboratori		holding xy presso stabilimento USA	in base alla normativa per la gestione LUL	APP conformi (segnalazione attivazione GPS, informativa privacy, consenso al trattamento)

INFORMAZIONI AGGIUNTIVE

Attività di trattamento	Dato particolare	L'attività principale comporta prevede che il Dato particolare sia trattato su vasta scala	Rischio elevato per i diritti e le libertà fondamentali	L'attività principale comporta il monitoraggio regolare e sistematico su larga scala degli interessati	Trattamento automatizzato (es. profilazione)	Sorveglianza su larga scala di zona accessibile al pubblico
Es. gestione amministrativa personale dipendente – rilievi presenze	SI (geolocalizzazione)	SI	SI	NO	NO	NO

ADEMPIMENTI SOSTANZIALI: I PROCESSI VALUTATIVI

Se Dipendenti > 250 o trattamento comporta rischio elevato o comprende dati particolari	Registro trattamenti (art.30)
Se il Titolare è un ente pubblico o tratta dati particolari su larga scala, ecc.	DPO (art. 37)
Se il trattamento comporta un rischio elevato…	DPIA (analisi del rischio con contenuti minimi prefissati) – Art. 35
Se DPIA evidenzia un rischio elevato senza misure di attenuazione in campo	Consultazione preventiva (art. 36)
Livello di sicurezza adeguato al rischio	Analisi del rischio → Misure di sicurezza adeguate **(art. 32), che prevedano, se del caso:**

pseudononimizzazione o cifratura

contromisure **per garantire** riservatezza, integrità, disponibilità (vedi analisi rischio in quanto sono i principi cardine della sicurezza informatica) → dal punto di vista IT comporta l'esigenza di effettuare **un assessment IT**

ripristino disponibilità e accesso dati → disaster recovery (procedure organizzative e contromisure con soluzioni informatiche, strumenti di incident response,)

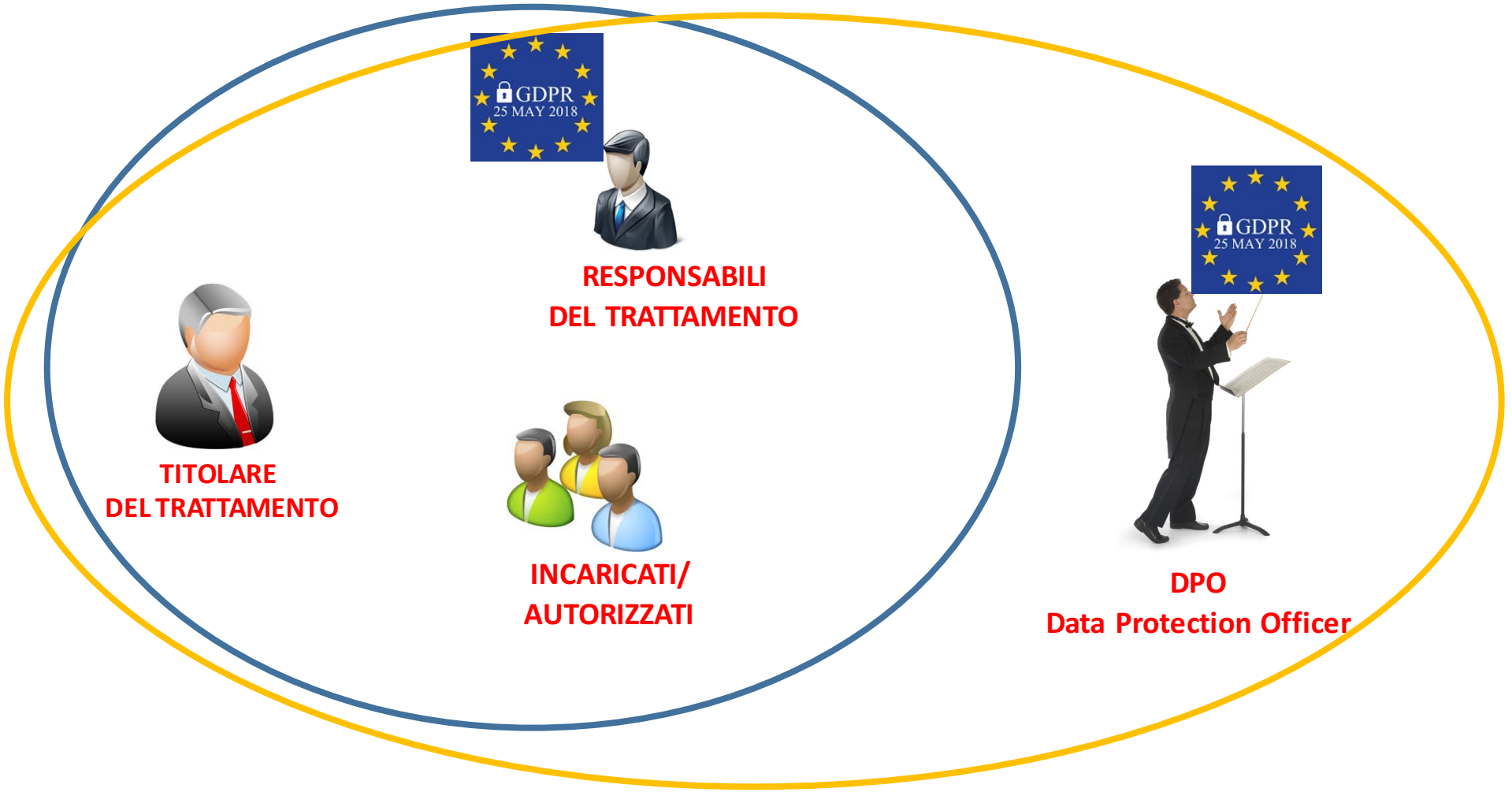
procedure per test**, verifica e valutazione efficacia delle misure tecniche e organizzative** → Procedure/policies, strumenti e soluzioni per **l'Audit sicurezza e IT (penetration test, sw analisi log, ecc.)**

OBBLIGHI DEL TITOLARE DEL TRATTAMENTO (art. 24)

TITOLARE DEL TRATTAMENTO:
colui che determina le finalità e i mezzi del trattamento di dati personali

- Identificare **gli interessati e le attività di trattamento**, la loro finalità, i tempi ed i mezzi del trattamento (cd. **Registro dei trattamenti**) e garantisce il rispetto dei principi fondamentali
- Individuare **le persone autorizzate** al trattamento in base alle loro competenze specifiche e fornisce loro idonee istruzioni e formazione.
- **Individuare e Contrattualizzare** opportunamente i Responsabili (esterni) del trattamento
- Svolgere i **processi valutativi** per la nomina del **DPO**, l'effettuazione **DPIA**, la gestione del **data breach** e mettere in atto **adeguate misure tecniche e organizzative** per assicurare e dimostrare la conformità al Regolamento nonché il rispetto dei principi privacy **by design / by default**
- **Vigilare** sulla correttezza del trattamento

GDPR - Reg. UE 679/2016 – I RUOLI



DPO – DATA PROTECTION OFFICER

Chi è il Data Protection Officer (DPO)

Il Data Protection Officer sarà una **figura professionale con particolari competenze in campo informatico, giuridico, di valutazione del rischio e di analisi dei processi**.

Il compito principale del DPO è l'osservazione, la valutazione e la gestione del trattamento dei dati personali allo scopo di far rispettare le normative europee e nazionali in materia di privacy.

(WP29) Si evince chiaramente che il soggetto prescelto debba possedere comprovata esperienza sulla legislazione relativa alla protezione dei dati personali sia nazionale che europea, sulle prassi oltre che una approfondita conoscenza del Regolamento. Nel caso, poi, di un ente pubblico o di un organismo pubblico, il DPO dovrebbe anche avere una buona conoscenza delle regole e delle procedure dell'organizzazione amministrativa.

Articolo 37: Compiti del DPO

1. **Informare e consigliare tutte le figure coinvolte nel trattamento** in merito agli obblighi derivanti dal Regolamento.

2. **Vigilare sull'osservanza del Regolamento**, l'attribuzione delle responsabilità, la formazione del personale e gli audit connessi.

3. **Contribuire alla eventuale redazione della DPIA** - Data Protection Impact Assessment e tenere nella debita considerazione i rischi associati alle operazioni di trattamento.

4. **Cooperare con l'Autorità di Controllo e fungere per quest'ultima da punto di contatto.**

Abilità richieste al DPO

1. Analizzare i principi di Privacy by Design applicati ai sistemi informativi
2. Gestire reclami e richieste da parte dei Clienti
3. Gestire le richieste provenienti dalle autorità
4. Effettuare le notifiche e le consultazioni preventive richieste in materia di privacy
5. Elaborare e comunicare la strategia per il trattamento e la protezione dei dati personali

LA VIGILANZA SUL SISTEMA

Le conoscenze richieste

- Le firme elettroniche
- I principi di PbD
- I diritti degli interessati ed il diritto all'oblio
- Le reti informatiche
- Le reti di telecomunicazione
- Le responsabilità connesse al trattamento dei dati personali I requisiti legali in materia di protezione dei dati personali in Italia ed Europa
- I requisiti legali in materia di trattamento e protezione dei dati personali in ambito pubblico, giudiziario, sanitario, per scopi storici, statistici o scientifici
- I requisiti legali in materia di trattamento e protezione dei dati personali nei vari ambiti
- I sistemi di videosorveglianza
- Le metodologie di DPIA e PIA
- Le tecniche crittografiche
- Le tecniche di anonimizzazione e de-anonimizzazione
- Le tecniche di pseudonimizzazione
- Le tecnologie IOT
- Le tecnologie RFID
- Le tecnologie di geolocalizzazione
- Le tecnologie di identificazione
- Le tecnologie di identificazione biometriche
- Le tecnologie di tracciamento delle operazioni
- Le possibili minacce alla protezione dei dati personali
- Gli standard per la gestione dei dati personali

DPO – DATA PROTECTION OFFICER

Ciò che invece è certo è che tale figura può essere rivestita, oltre che da un libero professionista, anche da un dipendente del titolare del trattamento (o del responsabile del trattamento).

Esiste infatti una evidente discrasia tra la figura del dipendente, che si porta sulle spalle tutti gli oneri e gli obblighi di subordinazione previsti dalla legge, e l'articolo 38 del Regolamento lì dove sancisce la **posizione di assoluta indipendenza del DPO**. E' chiaro che, con questi presupposti, la funzione garanzia richiesta al DPO parte già in evidente difficoltà applicativa.

L'articolo 38 dice: **il DPO non deve trovarsi in alcuna situazione di conflitto di interessi.** E qui preferiamo una interpretazione più funzionale che "politica". Il legislatore europeo in sostanza cerca di evitare facili nomine effettuate per affinità (o sovrapposizione) di mansioni pratiche: **non risulterà conforme alla legge l'eventuale nomina a DPO del responsabile che si occupa di ICT.**
Allo stesso modo, stante un possibile conflitto di interessi, si ritiene che **non possa essere nominato DPO l'amministratore delegato, il responsabile operativo, il responsabile finanziario o sanitario, il direttore marketing e quello delle risorse umane.**

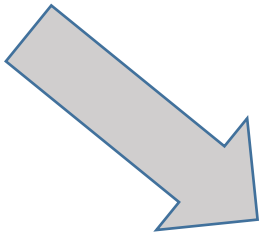
GDPR e Decreto Legislativo 231/2001

CENNI

nell'ambito di reati informatici, l'adeguamento alla nuova normativa GDPR, nell'ottica della *compliance*, favorirà la razionalizzazione delle procedure di gestione e, dunque, la revisione dei modelli 231 esistenti a presidio contro i rischi derivanti dalla gestione delle informazioni.

IL SISTEMA SANZIONATORIO

Decreto Legislativo 196/2003
dalla protezione del dato personale



GDPR, Capo VIII, artt. 77-84
alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

IL SISTEMA SANZIONATORIO

(GDPR,Capo VIII, artt. 83-84)

1) Sanzioni amministrative pecuniarie fino ad Euro 10.000.000,00, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore > FATTISPECIE (artt. 8, 11, da 25 a 39, 42 e 43 GDPR)

2) Sanzioni amministrative pecuniarie fino ad Euro 20.000.000,00, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore > FATTISPECIE (artt. 5, 6, 7, 9, da 12 a 22, da 44 a 49, […] GDPR)

IL SISTEMA SANZIONATORIO

(GDPR, Capo VIII, artt. 83-84)

Condizioni generali per infliggere sanzioni amministrative pecuniarie

- natura, gravità e durata della violazione
- carattere doloso o colposo della violazione
- misure tecniche adottate ex ante/ex post
- precedenti violazioni
- categorie di dati personali interessate dalla violazione
- etc..

...ALTRE SANZIONI

1) Risarcimento del danno (danno materiale, danno immateriale, responsabilità civile): inversione onere probatorio

2) Sanzioni eventualmente previste dagli Stati membri (GDPR, Capo VIII, art. 84)

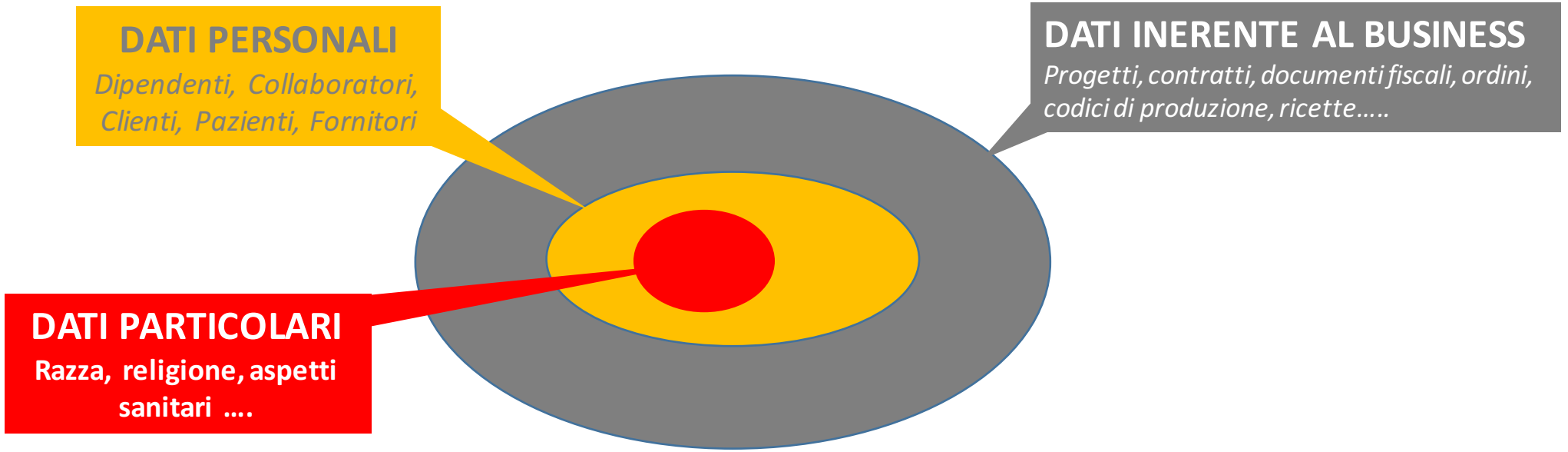
3) Poteri correttivi delle autorità di controllo (GDPR, Capo VI, art. 58)

TMC
Top Management Consulting

Cosa dobbiamo fare per difendere i nostri dati e rispettare il nuovo Regolamento Europeo?

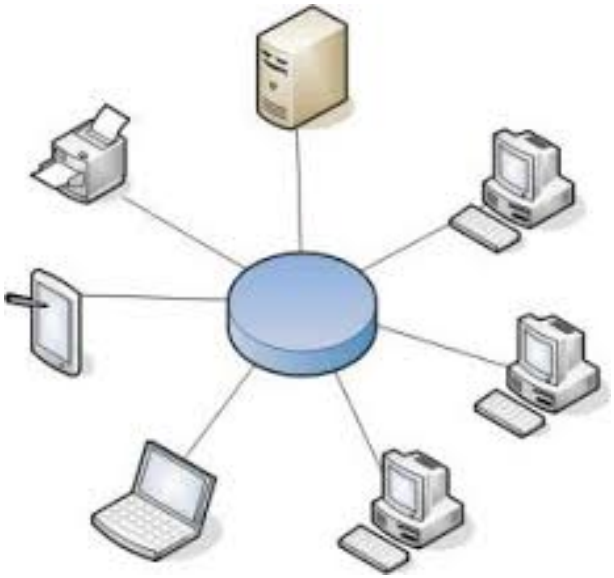
7 PASSI PER UN'ADEGUATA DIFESA

1. IDENTIFICARE BENE QUALI DATI DEVO DIFENDERE



7 PASSI PER UN'ADEGUATA DIFESA

2. IDENTIFICARE BENE DOVE SONO I DATI DA DIFENDERE



7 PASSI PER UN'ADEGUATA DIFESA

3. ANALIZZARE I RISCHI

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
NETWORK AND TECHNICAL RESOURCES	☐ Low	1
	☐ Medium	2
	☐ High	3
PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA	☐ Low	1
	☐ Medium	2
	☐ High	3
PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA	☐ Low	1
	☐ Medium	2
	☐ High	3
BUSINESS SECTOR AND SCALE OF PROCESSING	☐ Low	1
	☐ Medium	2
	☐ High	3

ANALISI DEL RISCHIO - MISURA DEGLI IMPATTI

ISO/IEC 29134

LEVEL OF IMPACT	DESCRIPTION
Low	Gli interessati possono incontrare alcuni piccoli inconvenienti superabili senza particolari problemi (perdita di tempo per re-inserimento di dati, fastidi, irritazioni, ecc.).
Medium	Gli interessati possono incontrare notevoli inconvenienti superabili con qualche difficoltà (costi extra, impossibilità temporanea di accesso ai servizi di business, di preoccupazioni e timori ed incomprensioni, stress, minori fastidi fisici, ecc.).
High	Gli interessati possono incontrare notevoli conseguenze superabili solo anche se con gravi difficoltà (appropriazione indebita di fondi, blacklist da istituzioni finanziarie, i danni alla proprietà, la perdita di occupazione, citazione in giudizio, il peggioramento della salute, ecc.).
Very high	Gli interessati possono incontrare proplemi significativi, o anche conseguenze irreversibili e non superabili (incapacità di lavorare a lungo termine psicologico o disturbi fisici, morte, ecc.).

ANALISI DEL RISCHIO – VALUTAZIONE CONTESTO

Top Management Consulting

KEYMAP

CONTESTO

Quale forma giuridica ha la Società?

srl

Di che tipo è la proprietà della Società?

Privata

La Società è controllata da soggetti terzi?

No

La Società è quotata in borsa?

No

La società possiede marchi o brevetti?

No

In quale settore opera la Società?

Raffinerie, prodotti chimici, gomma, plastica, industrie farmaceutiche

Qual è la tipologia dei Clienti della Società?

Aziende Nazionali, Aziende Internazionali

La Società opera negli USA o Canada?

No

Numero Dipendenti

18

Numero Collaboratori a contratto

18

Fatturato anno precedente (MLN?)

1,1

Fatturato previsto anno in corso (MLN?)

1,2

Struttura di vendita

Diretta

Numero Anagrafiche Clienti, Dipendenti, Collaboratori e Fornitori gestite nei sistemi azie

AMMINISTRAZIONE SISTEMA INFORMATIVO

Il ruolo di Amministratore di sistema è stato documentato ed attribuito in modo
lo ricoprono?

No

Le utenze privilegiate da Amministratore sono distinte da quelle non privile
Registrano i file di log? Sono assegnate ognuna a una specifica persona?

Parzialmente

Prima di collegare un nuovo dispositivo alla rete sono sostituite le credenziali
un amministratore autorizzato?

No

Sono stati identificati e documentati i profili e le autorizzazioni per accedere
sicurezza delle informazioni?

Parzialmente

Esiste un sistema per la registrazione, profilazione degli utenti e la gesti
opportuna politica degli accessi?

Si

Esiste un sistema per impedire che vengano utilizzate credenziali deboli,
sufficiente frequenza e ne venga impedito il riutilizzo?

Parzialmente

Sono stati identificati, classificati e registrati le applicazioni e i programmi so
delle informazioni trattate?

No

Sono stati identificate le applicazioni ed i programmi software, con le relativ
dispositivo (whitelist)?

No

Questo è un progetto di GRCteam S.r.l. e TMC S.r.l.

KEYMAP

KEYMAP

POSTA ELETTRONICA

Come è gestita la posta elettronica?

Su un mail server interno

Sono sempre utilizzati ed aggiornati i programmi di Antispam?

Si, quasi sempre

ORGANIZZAZIONE PER LA SICUREZZA DELLE INFORMAZIONI

La Società possiede la certificazione ISO9001 o analoga per lo specifico settore di appartenenza?

Si

La Società possiede la certificazione ISO27001?

No

Esiste un organigramma aziendale?

Si

Le mansioni, i ruoli e le responsabilità sono identificate, documentate ed attribuite in modo specifico?

Si

Esistono procedure documentate per la gestione della sicurezza dei dati?

Parzialmente

Il rispetto delle procedure e la loro efficacia è periodicamente verificato?

Parzialmente

Le procedure e le responsabilità per la sicurezza dei dati sono state opportunamente ed esplicitamente spiegate ai dipendenti e ai collaboratori?

Parzialmente

Il personale interno ed esterno è stato addestrato sui rischi che possono insorgere durante la manipolazione e trattamento dei dati?

Parzialmente

Nelle lettere di assunzione e/o nelle mansioni sottoscritte dal personale esistono vincoli specifici inerenti alla sicurezza e riservatezza delle informazioni? Ed in particolare, se trattate, per le informazioni personali o particolari?

Si

DATI PERSONALI E PARTICOLARI

La Società tratta dati personali o particolari?

ANALISI DEL RISCHIO
VALUTAZIONE DEL RISCHIO SPECIFICO

		Livello di impatto		
		Basso	Medio	Alto / Molto alto
Probabilità di occorrenza di un evento	Bassa			
	Media			
	Alta			

RISCHIO SPECIFICO – CONTROMISURE IDONEE

Misure tecniche di sicurezza

	Dispositivi mobili / portatili	
Q.1	Deve essere definita e documentata una procedura di gestione pei dispositivi mobili e portatili che definisce regole chiare per il loro corretto utilizzo.	1
Q.2	I dispositivi mobili che accedono al sistema informativo devono essere pre-registrati e pre-autorizzati.	1
Q.3	I dispositivi portatili devono essere soggetti agli stessi livelli di procedure di controllo di accesso (al sistema informativo) della altre apparecchiature.	1
Q.4	Devono essere chiaramente definite specifiche responsabilità e ruoli per la gestione dei dispositivi mobili.	2
Q.5	L'organizzazione deve essere in grado di cancellare da remoto i dati personali (associati al suo utilizzo) su un dispositivo mobile la cui sicurezza sia stata messa a repentaglio.	2
Q.6	I dispositivi mobili devono consentire la separazione tra utilizzo personale e aziendale attraverso contenitori software sicuri.	2
Q.7	I dispositivi portatili, quando non in uso, devono essere fisicamente protetti contro il furto.	2
Q.8	Per l'accesso ai dispositivi mobili devono venir prese in considerazione tecniche di autenticazione a due fattori	3
Q.9	I dati personali memorizzati in un dispositivo mobile (utilizzato per l'elaborazione di dati aziendali) devono essere cifrati.	3
	Correlati a ISO 27001:2013 - A. 6.2 i dispositivi mobili e il telelavoro	

RISCHIO SPECIFICO – CONTROMISURE IDONEE

Misure tecniche di sicurezza

	Risorse umane	
	Riservatezza del personale	
I.1	L'organizzazione deve assicurare che tutti i dipendenti comprendano le proprie responsabilità e gli obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità devono essere chiaramente comunicati durante la fase di pre-impiego e/o del processo di inserimento.	1
I.2	Ai dipendenti deve essere chiesto preventivamente di esaminare e accettare la politica di sicurezza dell'organizzazione e di firmare i relativi accordi di riservatezza e di non divulgazione.	2
I.3	I dipendenti coinvolti in trattamenti di dati personali ad alto rischio devono essere legati a specifiche clausole di riservatezza (tramite il contratto di lavoro o altro atto giuridico).	3
	Correlati a ISO 27001:2013 - A.7 Sicurezza delle risorse umane	

TMC
Top Management Consulting

7 PASSI PER UN'ADEGUATA DIFESA

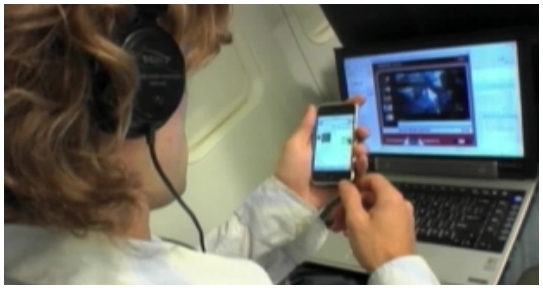
4. AGGIORNARE ED AFFILARE LE ARMI

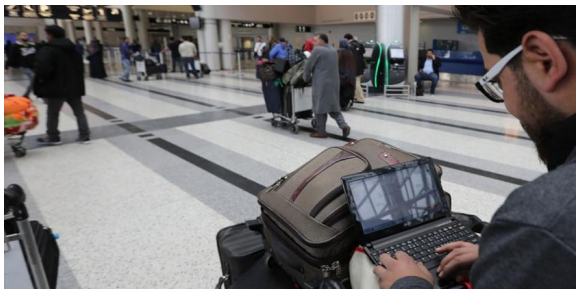
Non a caso si parla di attacco informatico
perché si tratta di una vera e propria guerra ed in guerra
le armi sono importanti.

Armi che sono sempre più sofisticate e tecnologiche

7 PASSI PER UN'ADEGUATA DIFESA

Il nostro modo di lavorare si è evoluto ….





…..e le «armi» necessarie per difendere il nostro business sono molte, diverse e sempre più evolute e sofisticate

NON POSSIAMO PERMETTERCI DI IGNORARLO!!

- Net Intrusion Detection System
- Firewall
- Anti virus
- Anti spyware
- Backup e disaster recovery
- Software di Emulazione terminali
- Intrusion Detection System
- Protezione Wi-fi
- Criptazione
- SW sentinella

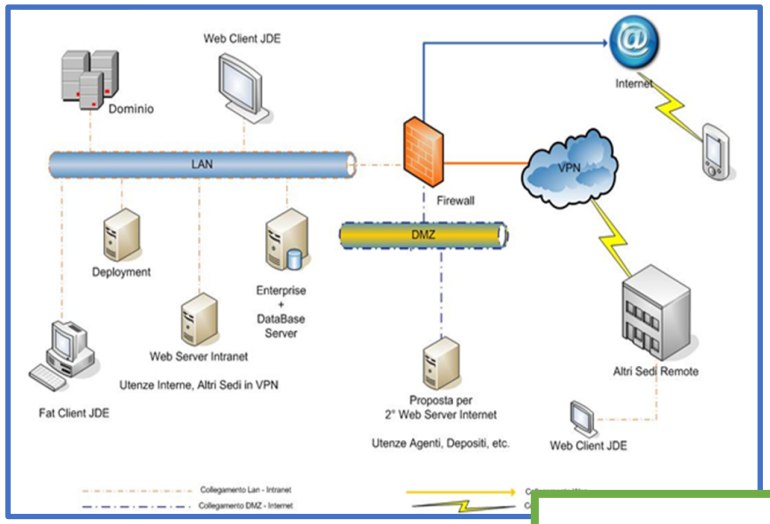
7 PASSI PER UN'ADEGUATA DIFESA

5. ADEGUARE LE INFRASTRUTTURE

Oggi i dati sono nei server dell'Azienda,
e nei dispositivi mobile dei dipendenti

Fuori ci sono i virus che attaccano gli internauti
ed i loro mobile (end point)

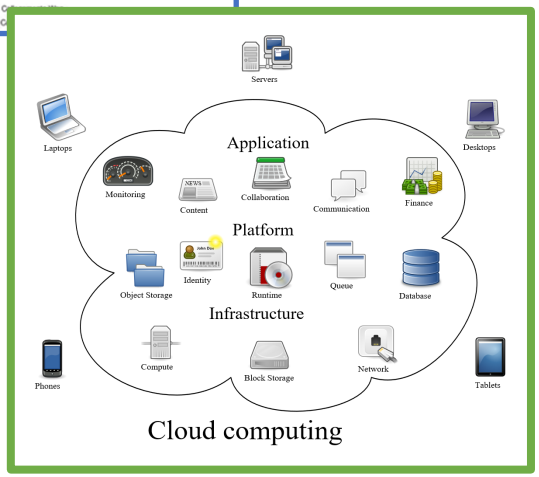
E gli eserciti di hacker che attaccano i server
con tempo e risorse infinite



La possibilità di salvarsi dipende, oltre che dalle tecnonologie adottate (le armi), da come sono progettate le infrastrutture del sistema informatico aziendale (le difese):

- Segmentazione delle reti;
- Policy di accesso dall'esterno;
- Disaster recovery;
- Sistemi evoluti di document management
- Gestione pw e autorizzazioni
- Zone protette

…… Cloud computing



TMC
Top Management Consulting

10 CONSIGLI UTILI

1. Installate un buon Antivirus , tenetelo costantemente aggiornato e usatelo su tutti i file che ricevete.
2. Fate il backup (almeno) dei vostri dati. Fatelo spesso. Fatelo SEMPRE
3. Installate gli aggiornamenti (patch) di Microsoft .
4. Non installate software superfluo o di dubbia provenienza.
5. Non aprite gli allegati non attesi, di qualunque tipo, chiunque ne sia il mittente, e comunque non apriteli subito, anche se l'antivirus li dichiara ''puliti''.
6. Tenete disattivati ActiveX , Javascript e Visual Basic Scripting . Riattivateli soltanto quando visitate siti di indubbia reputazione.
7. Non fidatevi dei link presenti nei messaggi di posta. Possono essere falsi e portarvi a un sito-truffa.
8. Non inviate posta in formato html e chiedete di non mandarvela
9. Non distribuite documenti word : trasportano virus e contengono vostri dati personali nascosti.
10. Per aumentare la sicurezza del browser è spesso consigliato togliere la memorizzazione automatica dei moduli e delle password .

7 PASSI PER UN'ADEGUATA DIFESA

6. DEFINIRE LE PROCEDURE DI DIFESA

Questo, ci «obbliga»

- *ad analizzare bene i processi aziendali ed a descriverli in modo chiaro e comprensibile*
- *a valutare le minacce, i rischi e gli eventuali danni*
- *a definire ed evolvere le strategie di protezione e difesa*
- *a definire e documentare le procedure*

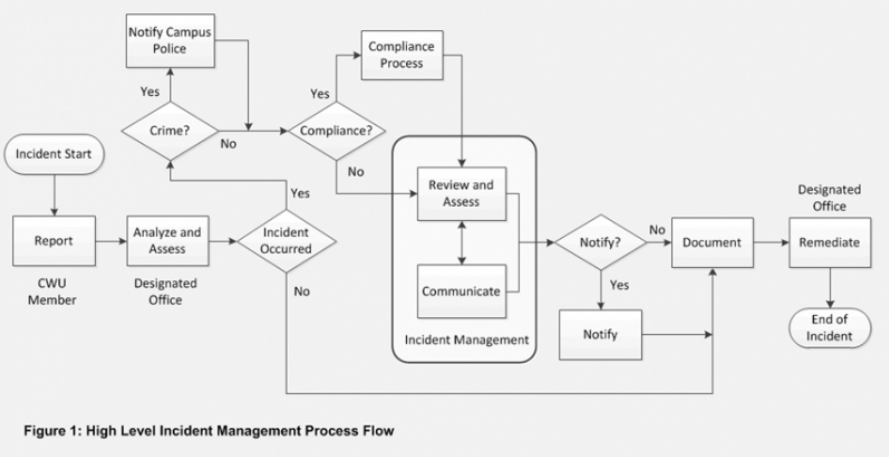


Figure 1: High Level Incident Management Process Flow

7 PASSI PER UN'ADEGUATA DIFESA

… in ogni tempo ed in ogni guerra, oltre alle armi ed alle strutture di difesa, quello che ha sempre fatto la differenza è stato …

… l'organizzazione, l'addestramento e la disciplina dei soldati!!!!

7 PASSI PER UN'ADEGUATA DIFESA

7. ADDESTRAMENTO CONTINUO DEL PERSONALE

Questo, ci «aiuta»

- *creare consapevolezza sui possibili rischi*
- *creare competenza sulle procedure da utilizzare*
- *Diminuire la distanza tra «praticità d'uso» e sicurezza*

PER FAR SÌ CHE OGNI PERSONA SAPPIA DISCIPLINARE E CONTROLLARE I PROPRI COMPORTAMENTI PER DIFENDERSI DALLE MINACCE E REAGIRE IN CASO DI ATTACCO

ALCUNI DATI 2017

36,2% FALLE NEL CODICE DEI SOFTWARE AZIENDALI
24,5% COMPORTAMENTO DEGLI UTENTI
20,8% STRUMENTI DI SICUREZZA OBSOLETI

Fonte: Rapporto Osservatorio Attacchi Digitali in Italia 2017. Pubblicato il 18/05/2017.

TMC
Top Management Consulting

In quale percentuale i dipendenti o i collaboratori interni sono, in modo colposo o doloso, coinvolti in crimini o danni informatici a scapito della propria azienda?

100%

TMC
Top Management Consulting

10 CONSIGLI UTILI PER APPROCCIARE LA NUOVA PRIVACY

1. Tutti i soggetti che trattano i dati devono **ricevere una lettera di incarico**
2. Se la gestione dei dati è affidata a società terze, bisogna **nominare i Responsabili Esterni**
3. E' opportuno che l'azienda predisponga e consegni un **Disciplinare per l'utilizzo degli strumenti informatici agli incaricati**
4. Il sito internet aziendale deve **rispettare la normativa sui cookies**
5. **L'installazione di telecamere** in azienda prevede informative e previa approvazione
6. **Le buste paga** devono essere gestite tutelando i dati dei dipendenti
7. Per utilizzare strumenti informatici bisogna adottare 3 misure minime: **password, antivirus e firewall**
8. **L'aggiornamento** dei sistemi operativi e degli altri software installati è obbligatorio
9. **Marketing e geolocalizzazione**: raccolta e utilizzo dei dati devono essere gestiti con cura
10. Gli incaricati al trattamento dati devono **essere formati**

TMC
Top Management Consulting

Cosa dobbiamo fare per difenderci e limitare i costi di un possibile attacco informatico?

Adeguare e tenere aggiornate le tecnologie

Formare ed addestrare il personale

Riprogettare le infrastrutture

Adeguare gli aspetti contrattuali

Adeguare le procedure ed i comportamenti alle norme di riferimento ed alle best practise del mercato

NEMMENO IL VOSTRO ANGELO CUSTODE SA DA DOVE INIZIARE?