THALES

GDPR
e Cyber Security

Firenze, 14 Febbraio 2018

Luca Ronchini
Massimo Romairone

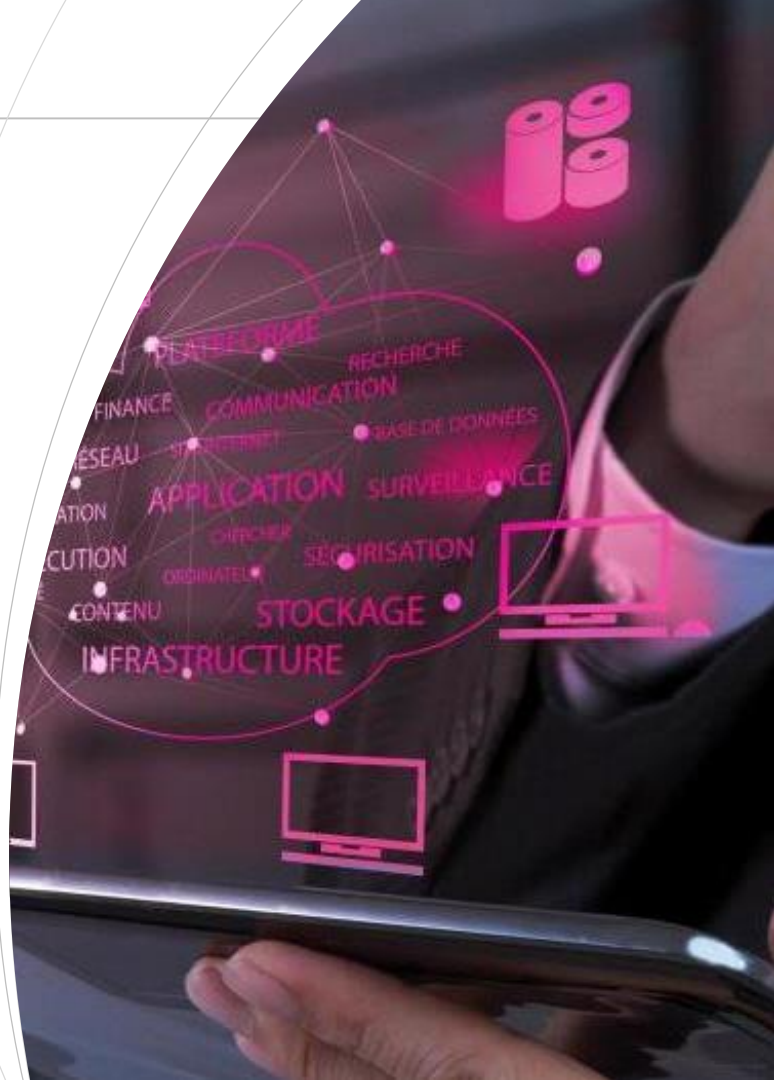
Critical Information Systems and Cybersecurity

- **5,000 tecnici IT & Security,** inclusi **1,500 specialisti cybersecurity**
- **Leader europeo nel mercato cybersecurity**
- **Leader mondiale nella protezione dei dati**
- **3 Cybersecurity Operation Centres – CSOC** (Francia, Olanda, Regno Unito)
- **1 CERT-IST** (Computer Emergency Response Team – Industry, Services and Tertiary sector)
- **5 Data Centre** ad alta sicurezza in Francia e Regno Unito
- **Prodotti con elevato grado di sicurezza** (confidenziale o top secret) per **50 paesi,** incluse nazioni NATO
- Soluzioni e prodotti per 200 clienti, inclusa la protezione dell'**80% delle transazioni bancarie mondiali.** Sicurezza per **19 delle 20 più grandi banche mondiali**
- **Cybersecurity per 9 dei10 Giganti Internet**
- **Gestione & cybersecurity** dei sistemi informativi critici di **130 clienti**
- **Laboratori di Ricerca Thales**

Thales Cyber Security e GDPR

Il rapporto messo a disposizione da Thales - https://dtr.thalesesecurity.com/ - leader nello sviluppo di sistemi critici di gestione dell'informazione, nella Cyber Security e nella sicurezza e protezione dei dati, evidenzia i seguenti dati:

- ✓ l'anno scorso il 43% delle aziende avevano registrato una violazione dei dati e almeno il 32% degli stessi ne dichiaravano più di uno.
- ✓ il 60% degli intervistati affermano che i propri sistemi IT sono stati violati in passato.
- ✓ 88% delle aziende analizzate si considera vulnerabile alle minacce di attacchi e violazioni alle strutture di gestione dei propri di dati, con il 37% che dichiara di essere "molto" o "estremamente 'vulnerabile.



Cyber Risks

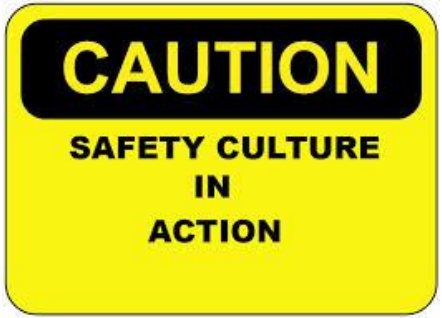
Complexity and interdependencies
- Highly interconnected -> increased dependencies -> increased vulnerabilities
- Complex detection

Heterogeneous
- Different protocols and adapted to business needs

Remote access required for maintenance
- Could be a risk

Not evolving
- Once deployed they are rarely updated

Built on standards without security mechanisms
- Operating system not patched
- Protocols (ModBUS, TCP, DNP3, OPC …)



Systems are not designed with cyber risks in mind

Business processes do not integrate this dimension
- Quality procedures (zero default)
- Safety procedures
- Maintenance procedures

Personnel is not trained neither informed

OPEN

THALES

Thales Cyber Security Approach

Methodology

8 Security Steps for a secure Critical Infrastructure

1. Establish Cybersecurity Design Principles
2. Create a Strong Perimeter
3. Deploy System Security and Detection/Recovery controls
4. Meet Cybersecurity Standards
5. Embed Cybersecurity in the Development Lifecycle
6. Conducting Risk Assessments and Penetration Testing
7. Maintain Operational Conditions
8. Mandate Safety Protection

Thales Cyber Security e GDPR

Il Regolamento EU 2016/679 – GDPR, che entrerà ufficialmente in vigore in tutta Europa in data 25 Maggio 2018, introduce le seguenti novità principali novità:

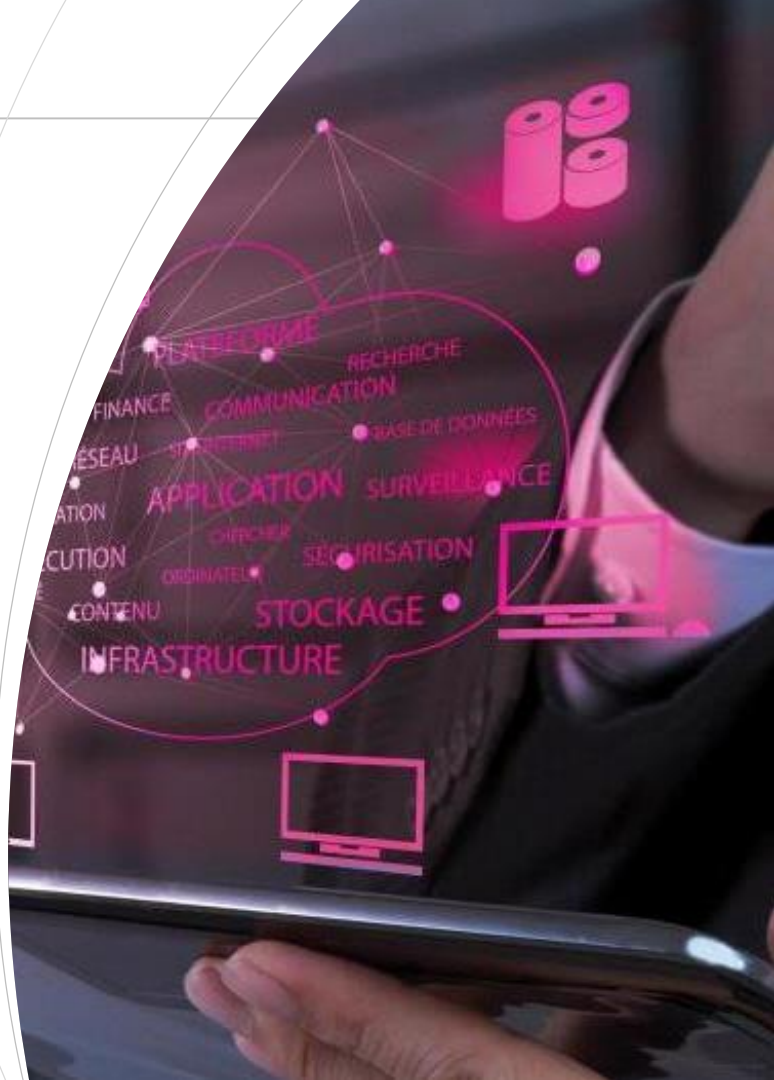
- ✓ introduzione sanzioni in caso di violazione dei dati;
- ✓ estensione definizione di dato personale sensibile;
- ✓ introduzione figura del DPO (***Data Protection Officer***) e sua responsabilità civile;
- ✓ obbligo di valutazione preventiva del rischio;
- ✓ notifica in caso di ***data breach*** all'autorità e al cittadino;
- ✓ semplificazione rapporti con il Garante della Privacy per aziende con sedi in più Paesi della UE

Si valuta alla fine del 2017 solo il 27% delle imprese italiane conosce gli obblighi della nuova normativa sulla protezione dei dati personali che entrerà in vigore a maggio del 2018, appena il 9% ha già avviato un progetto per adeguarsi. In pochi casi è già previsto un budget e sono stati decisi cambiamenti organizzativi. (Fonte: Osservatorio Security & Privacy sull'applicazione del GDPR in Italia)

Thales Cyber Security e GDPR

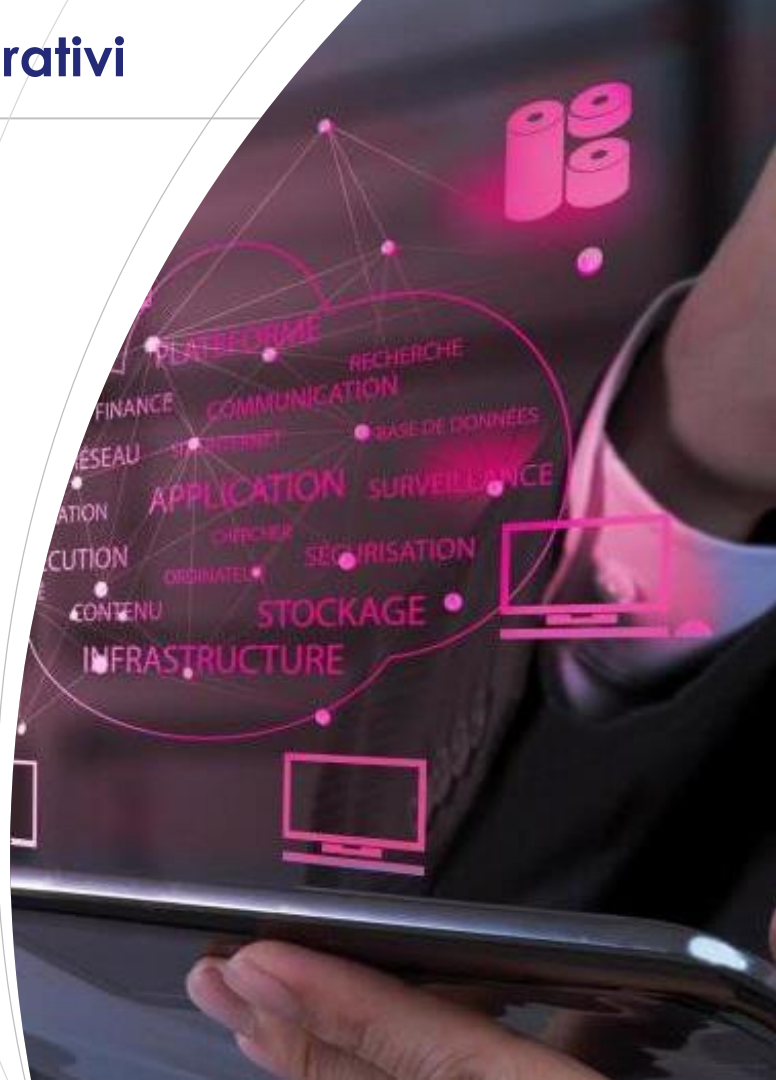
Thales ha sviluppato una serie di metodologie, servizi e tecnologie in grado di supportare le aziende che devono rispondere ai requisiti di conformità del GDPR.

Thales, sulla sicurezza dei dati e, più in generale, sulle tematiche di Cyber Security, ha sviluppato tecnologie, competenze ed esperienze in tutto il mondo nell'ambito di infrastrutture critiche come ad esempio Power Energy/Nuclear Plant, Trasporti Ferroviari, Metropolitane, Aeroporti, Banche, Industria Automobilistica, Difesa, Pubblica Amministrazione locale e centrale, Aziende di Produzione, gestendo progetti di piccole, medie e grandi dimensioni.



Thales Cyber Security e GDPR: ambiti operativi

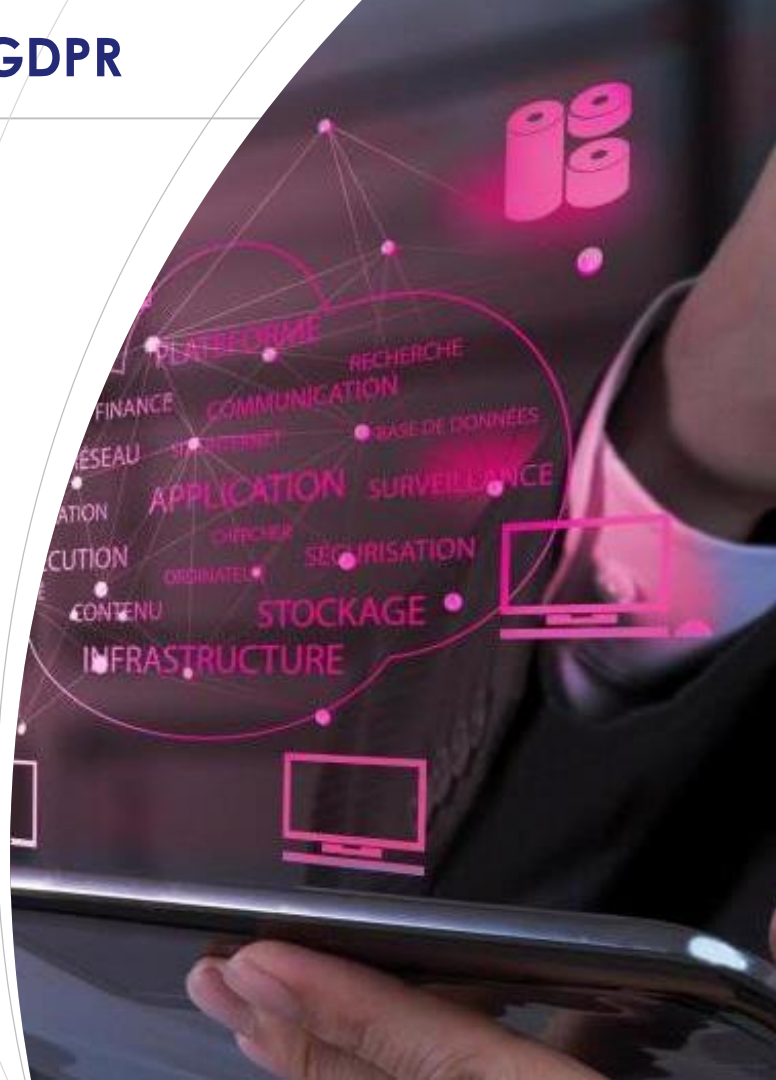
- **Business Company (Piccole, Medie e Grandi)**
- **Infrastrutture critiche :**
  - **Power Plant, Nuclear Plant**
  - **Transportation (Metro, Tranvie, Treni)**
  - **Aeroporti**
  - **Oil & Gas**
  - **Aerospazio/ Spazio**
  - ➢ **Specificità: SCADA / ICS /Industrial IoT**
- **Difesa**
- **Finance /Bank**
- **Industry**



Thales Cybersecurity – Scenari di azione GDPR

Thales in veste di:

- **Produttore di tecnologie (HW+SW) di cyber security (protezione dati, encryption,**
- **Consulenza, design, progettazione**
- **Integratore di soluzioni**
- **Sviluppo progetti**



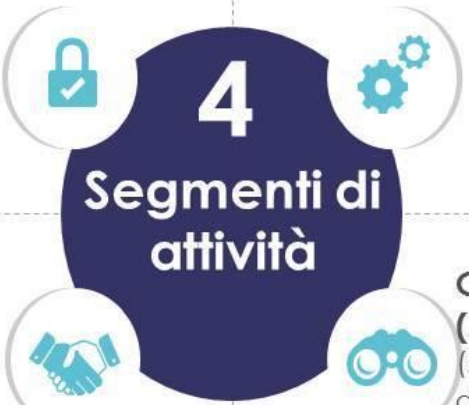
Thales Cyber Security e GDPR - Approccio

Protezione dei dati
Sensibili ma non classificati (TeS/Vormetric)

- Leader mondiale

Soluzioni e tecnologie di Cyber Security

- Francia, Norvegia e Paesi NATO



Cyber Security Consulting

- Centro di Competenza in Francia
- Sviluppo del Mercato in 10 Paesi UE entro il 2020 (UK, Paesi Bassi, Belgio, Portogallo, **Italia** …)

Cyber Security Operations (Managed SOC)
(sorveglianza e manitenimento delle condizioni di sicurezza)

- Centro di Competenza in Francia
- Sviluppo del Mercato in 10 Paesi UE entro il 2020 (UK, Paesi Bassi. Belgio, Portogallo, Norvegic , **Italia …**)

Thales Cyber Security e GDPR - Approccio

Functional audit & Governance

- Audits ISO 2700x
- GDPR
- ISMS deployment
- Activity continuity
- Crisis management

Infrastructures & Applications Architectures

- Design Secure architectures
- Architecture audit
- Security governance
- Security accreditation processes

Forensic, Reverse & Penetration testing

- Incidents response
- Reverse Engineering
- Penetration testing
- Vulnerability assessment
- Technical audits
- Source code audits

Safety & Security Evaluation

- Hardware labs (CC)
- Software labs
- Safety labs (CNES)
- Multiple Banking certifications

Thales Cyber Security e GDPR - Approccio

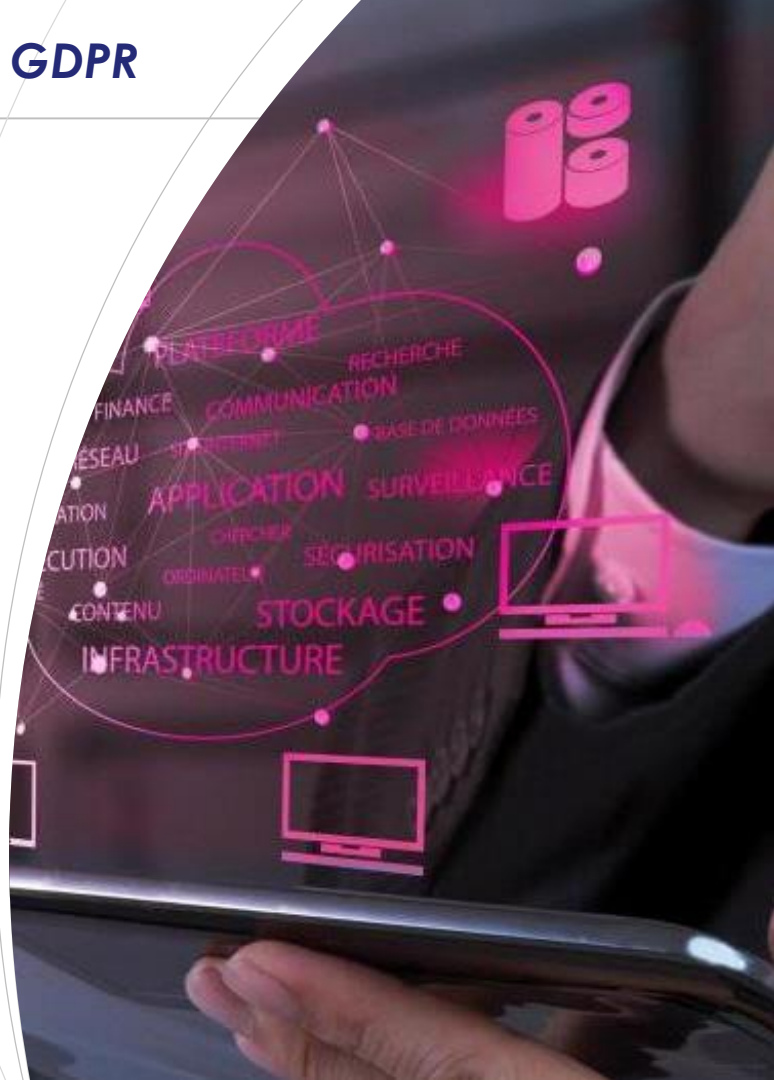
L'approccio di Thales si basa su una serie di principi fondamentali di seguito descritti.

- **Model:** il team Thales opererà a stretto contatto con l'azienda per educare e divulgare la conoscenza sui requisiti chiave del GDPR e sul potenziale impatto che può avere sul business. Utilizzando strumenti quali workshop, presentazioni, questionari e interviste individuali, Thales supporterà l'azienda nei processi di definizione e generazione di un modello di dati aziendale completo.
  Assessment: Thales supporterà l'azienda nella formulazione di una valutazione di conformità nei confronti dei requisiti del GDPR.
- **Report:** il team Thales supporterà l'azienda nella redazione di una relazione finale che descriverà i risultati delle attività di modellazione dei dati e delle gap analysis rispetto alle matrici di conformità GDPR. L'obiettivo sarà quello di permettere all'azienda di ottenere una sintesi di alto livello che evidenzierà dove le misure tecniche e organizzative devono essere aggiornate o migliorate per raggiungere una conformità al GDPR.
- **Risk Based:** le non conformità saranno valutate in termini di rischio relativo sia per l'interessato sia per l'organizzazione, in modo tale che le successive attività di adeguamento e implementazione tecnica possano essere pianificate e indirizzate nel rispetto della conformità a questi rischi e del rischio residuo.

Modello di implementazione della conformità GDPR

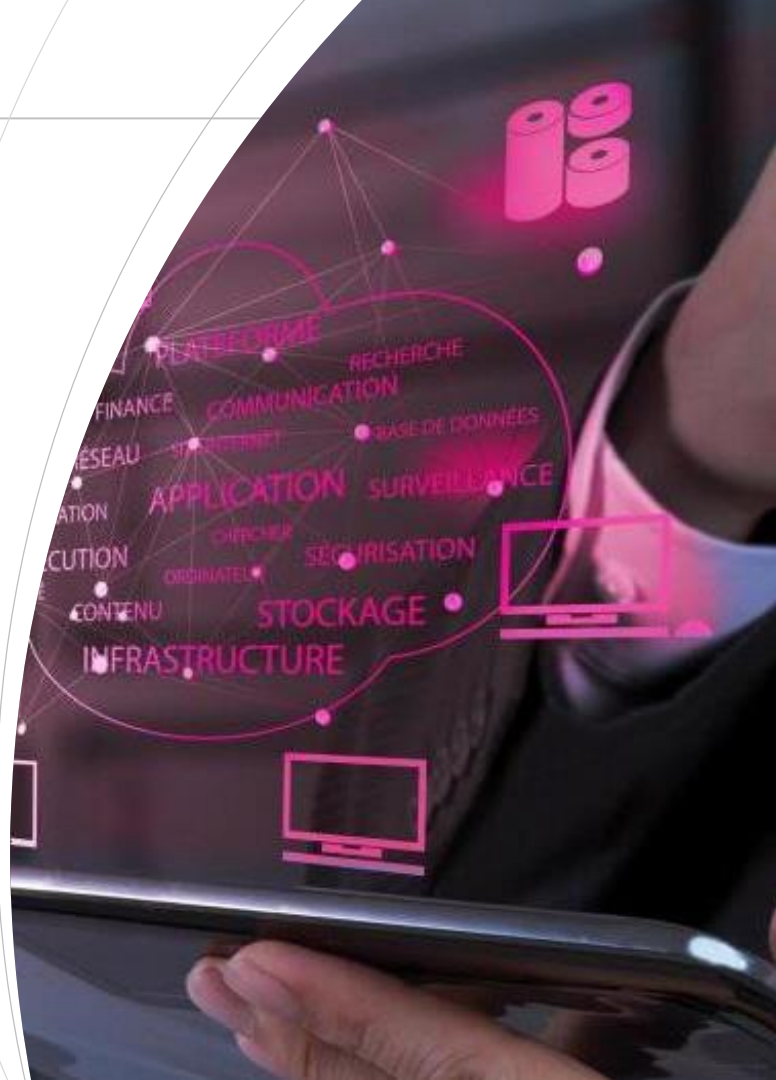
Thales ha sviluppato un proprio modello di attività per l'implementazione della conformità GDPR che si compone di 3 macro aree di intervento:

- Risk Analysis e valutazione impatti
- Protezione e adattamento Governance
- Gestione dei Key process



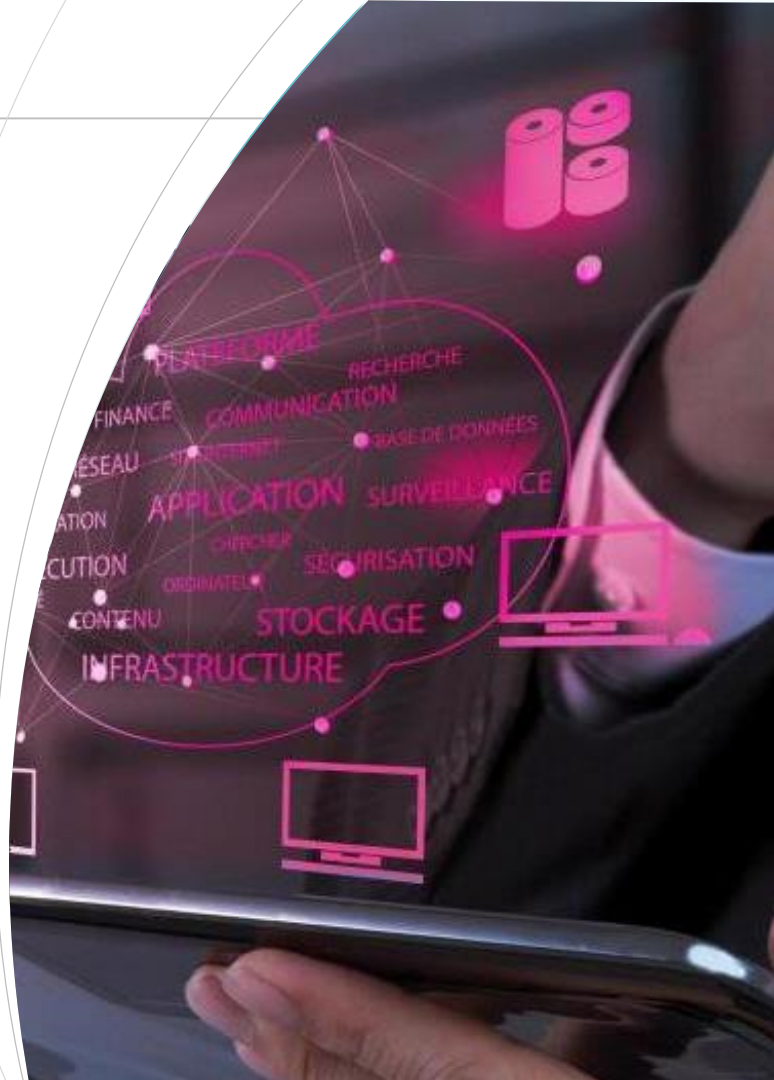
Risk Analysis e Valutazione degli Impatti

Attività
Analisi obblighi di legge e regolamenti
Identificazione tipologia delle informazioni/categorie di dati
Elaborazione e implementazione della classificazione dei dati
Diagnostica ad uso interno
Politica dei dati/ sicurezza informatica
Analisi contratti Terze Parti (hosting dei dati, sub-contractors,ecc.)
Creazione funzione DPO (Data Protection Officer)



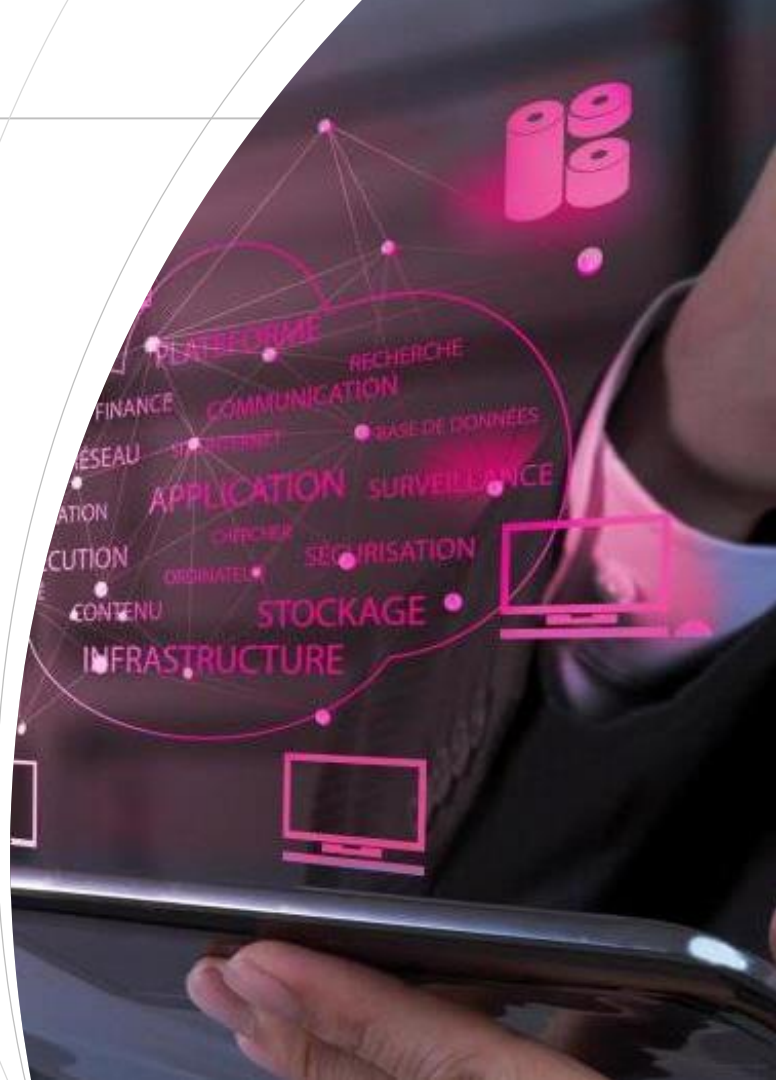
Protezione e adattamento Governance

Attività
Analisi per tipologia di situazione: «a riposo», in movimento, in uso
Livelli di protezione adeguati per la valutazione del rischio
Continuo aggiornamento dei rischi e dei sistemi di protezione associati



Gestione dei Key process

Attività
Detection
Valutazione e prevenzione
Investigazione
Identificazione degli scenari ed elaborazione dei piani di gestione di crisi
Selezione degli strumenti in funzione dei rischi e delle esigenze relativi ad ogni processo



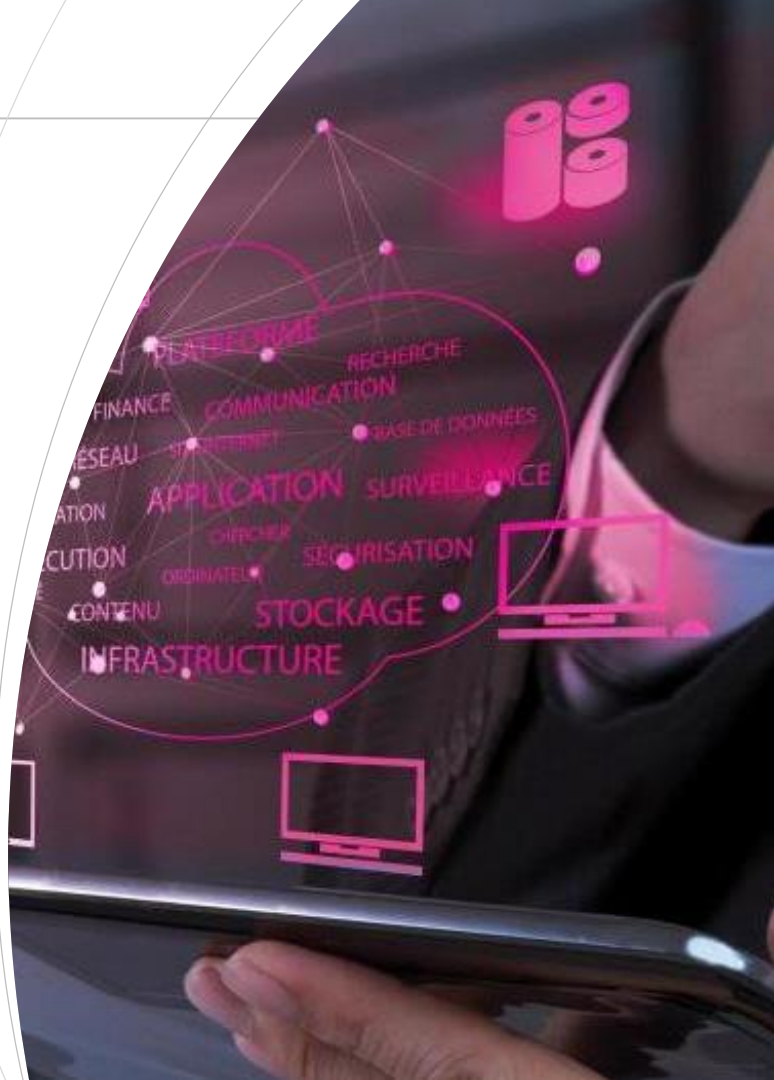
GDPR - Roles

Analisi dinamica del Rischio

Gestione organizzativa (Governance)

Gestione Tecnica (Tecnologie)

Trasferimento del rischio residuo (Assicurazione)



Data Protection: Thales Environment

DB/ File Encryption
Customer Records

Application Encryption
Encryption Integration

Big Data
Secure Analytics

Code Signing
Script Development

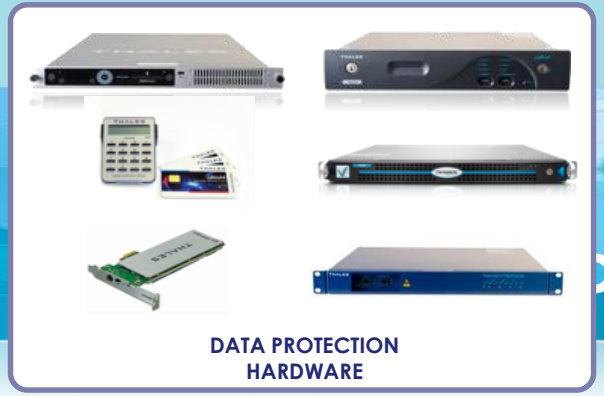
Tokenization Data Masking
PCI, PHI

Transaction Security
Payment related apps

Public Key Infra (PKI)
Internet of Things

Cloud Security
Cloud Migration

Use Cases



DATA PROTECTION HARDWARE

- Transparent Encryption
- Application Encryption
- Tokenization
- Encryption Gateway
- Key Management
- Security Intelligence

DATA PROTECTION SOFTWARE

Grazie per l'attenzione