GDPR

Le soluzioni tecnologiche a supporto dell'azienda e del DPO

OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

Chi è Opentech

Società leader di **Information Technology** che progetta e produce i propri software in Italia

Specializzata in prodotti per la Governance, l'Organizzazione, la Compliance, il Risk e l'Internal Audit

✓ Certificata **ISO 9001:2015** per la produzione di software e **l'erogazione di formazione** e servizi IT

Partner istituzionale

Microsoft

ABI FORMAZIONE

ISACA Serving IT Governance Professionals

ANDAF Associazione Nazionale Direttori Amministrativi e Finanziari

ROMA TRE UNIVERSITÀ DEGLI STUDI

SAPIENZA UNIVERSITÀ DI ROMA

AICOM Associazione Italiana Compliance

OPENTECH

CIO Applications Europe Top 10 Risk Management CONSULTING/SERVICES COMPANIES - 2019

Oggi ne parliamo insieme con:

- **L'Avv. Maurizio Rubini** - esperto di Compliance e Governance Aziendale
- **L'Ing. Giuseppe Puleo** - Manager Security Consultants Unit IBM Italia S.p.A.
- **L'Ing. Emanuele Greco -** Product Manger Opentech S.r.l.

OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

Programma

PRIMA PARTE

- Il GDPR
- I 7 principi del regolamento
- Cosa comporta il GDPR per le aziende
- La compliance al GDPR
- Il sistema sanzionatorio

SECONDA PARTE

- Art. 32 Sicurezza del trattamento
- Risk Management Approach
- Alcuni modelli di riferimento

TERZA PARTE

- «Strumenti base» per la privacy
- I processi privacy
- Governance integrata in azienda

OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

GDPR compliant ?

OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

Premessa

La tutela dei dati personali, fino a poco più di vent'anni fa, non conosceva in Italia nessuna regolamentazione.
Era il 1996 quando per la prima volta il legislatore italiano si è occupato di proteggere ognuno di noi dall'utilizzo improprio delle informazioni individuali. Il mondo era molto diverso da quello che è oggi e anche i dati riferiti alle persone erano limitati e di difficile reperimento. Erano essenzialmente informazioni identificative, dati oggettivi, di recapito ed erano contenuti in elenchi o archivi. Erano soprattutto dati statici, non modificabili e le possibilità di abuso erano limitate.
Le nuove tecnologie rendono sempre più facile raccogliere dati ed elaborarli confrontandoli con gli enormi database che si generano mentre noi usiamo gli oggetti collegati alla rete.
Proprio per effetto di questa evoluzione l'Unione Europea ha deciso di emanare un Regolamento Generale sulla tutela dei dati personali, che dal 2018 definisce regole uniche per tutti i trattamenti di dati effettuati nel territorio dei paesi membri dell'Unione.
Diventa quindi essenziale, e non solo per chi si occupa di questioni giuridiche, conoscere i principi che regolano l'uso dei dati personali: in questo modo sarà possibile individuare tempestivamente le questioni che possono derivare da una determinata attività e operare con sufficiente tranquillità, riducendo i rischi legali.

Il GDPR

Regolamento UE del Parlamento Europeo e del Consiglio n. 679 del 27 aprile 2016

1. **Oggetto**: insieme di norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché norme relative alla libera circolazione di tali dati.
2. **Ambito di applicazione:** tutti i trattamenti automatizzati e non, ad esclusione di:
   - attività extra UE;
   - politica estera e sicurezza comune;
   - finalità personali o domestiche;
   - prevenzione, indagine, accertamento reati, sicurezza pubblica.
3. **Ambito di applicazione territoriale**:
   - Stabilimento del titolare, titolare o responsabile del trattamento nella UE;
   - Titolare e responsabile fuori UE, qualora gli interessati siano in UE in caso di:
     - offerta di beni e servizi;
     - monitoraggio comportamento degli interessati.

OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

I 7 principi del regolamento

- Liceità e correttezza
- Trasparenza
- Limitazioni delle finalità dei trattamenti
- Minimizzazione
- Esattezza
- Limitazione della conservazione
- Integrità e riservatezza

OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

Principali definizioni: il dato personale

D. LGS. 196/2003

qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale

GDPR

qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

Principali definizioni: il trattamento dei dati

Cos'è il **trattamento** di un dato?

Qualsiasi attività di gestione del dato come:

- ✓ la raccolta,
- ✓ la conservazione,
- ✓ la modifica,
- ✓ la consultazione,
- ✓ la comunicazione,
- ✓ la cancellazione

su qualsiasi supporto

- informatico,
- cartaceo o analogico,

sia attraverso operatori sia con processi automatizzati.

OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

Cosa comporta il GDPR per le aziende ?

Tutti trattano dati personali, siano quelli dei clienti, dei prospect, dei dipendenti o dei fornitori; l'argomento attraversa sostanzialmente ogni attività umana. Finora siamo stati abituati a considerare la privacy come un adempimento, un obbligo da rispettare con comportamenti formali, affidati di solito alla supervisione di un legale.

Con il Regolamento Europeo cambia tutto: la privacy diventa un processo aziendale da gestire in tutte le sue fasi, da quella ideativa a quella esecutiva.

Il concetto alla base del cambiamento è semplice: i dati personali sono diventati l'equivalente della materia prima per l'economia tradizionale, l'elemento base da trasformare nel prodotto per il mercato. I dati sono il "petrolio" dell'era digitale, l'elemento che va elaborato per generare i fatturati delle aziende.

Oggi i dati personali servono a:

1. creare prodotti innovativi;
2. formulare offerte mirate ai consumatori, convertendo sconosciuti in clienti fidelizzati;
3. garantire sicurezza e migliorare l'efficienza aziendale;
4. controllare, profilare e analizzare.

In pratica cosa è cambiato ?

1. E’ cambiata **l’informativa** che diventa breve, priva di riferimenti normativi, deve essere comprensibile anche ai minori e contenere nuovi elementi, come l’origine dei dati e il tempo di conservazione previsto.
2. E’ cambiato **il consenso** al trattamento che cessa di essere necessariamente espresso e diventa un consenso inequivocabile e quindi desumibile in base ai comportamenti degli interessati.
3. Sono cambiati i ruoli del trattamento, con l’introduzione della figura del **Data Privacy Officer** (il responsabile per la protezione dei dati personali) che è un vero manager dei database aziendali e non un semplice garante interno del legittimo trattamento dei dati.
4. E’ sparito l’obbligo di notificazione al Garante ed è stato introdotto il **registro dei trattamenti**.
5. E’ sparito il Documento programmatico sulla sicurezza e nasce il **Documento di valutazione di impatto del trattamento dei dati**.
6. Sono stati introdotti nuovi diritti, come quello alla **portabilità dei dati**, per cui ogni interessato potrà trasferire da un titolare a un altro i dati che lo riguardano.
7. E’ diventato essenziale **progettare** la tutela dei dati personali e **documentare** l’attenzione verso l’analisi dei rischi connessi al trattamento dei dati personali.
8. Sono aumentate significativamente **le sanzioni** applicabili.

La compliance al GDPR

Per il GDPR deve essere dimostrata la sostanza degli adempimenti non il rispetto formale. Non basta avere adempiuto alle richieste normative, ma occorre essere in grado di DIMOSTRARLO.

Il titolare del trattamento mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al presente regolamento (art.24)

OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

L’obbligo di formazione

Anche su questo tema il regolamento ha portato (finalmente) significative novità:

- l’art. 39 rubricato «**compiti del responsabile della protezione dei dati**» indica tra tali compiti quello di «*sorvegliare l’osservanza del regolamento (…), la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo*»
- l’art. 47 «**norme vincolanti d’impresa**» par. 2 lett. N) dispone che le norme applicabili ai gruppi d’impresa che trattano dati in più stati dovranno specificare «*l’appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali*».

Lo sviluppo del mercato digitale oggi è questo ?

OPENTECH

CIOApplicationsEurope
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

Esempi di comportamenti sanzionabili

- violazione dell’obbligo di tenuta del registro dei trattamenti;
- mancata valutazione d’impatto - DPIA;
- omessa consultazione preventiva dell’Autorità;
- omessa notifica di Data Breach;
- omessa nomina del DPO;
- omessa adozione di misure di sicurezza adeguate.

Nuovo impianto sanzionatorio

Sanzioni Civili

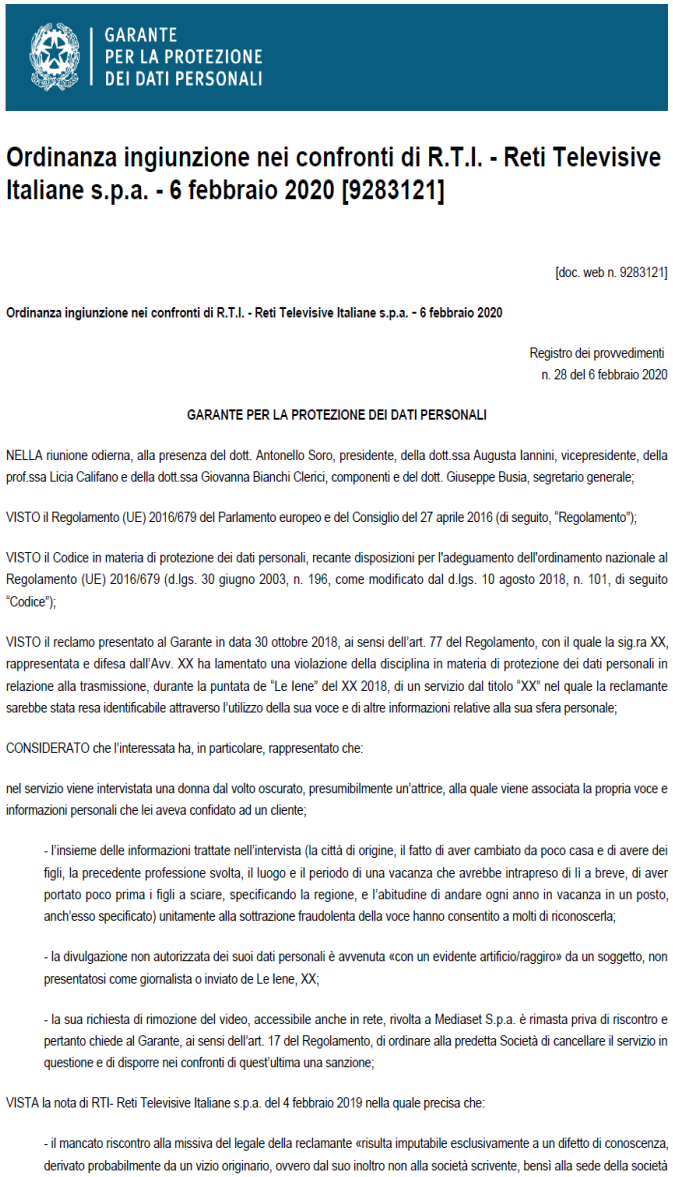
- Risarcimento del danno materiale e immateriale
- Responsabilità solidale

Sanzioni amministrative

- Effettive, proporzionate, dissuasive
- Fino a 10/20 milioni di euro o fino al 2/%-fatturato mondiale totale annuo dell'esercizio precedente

OPENTECH

Recenti provvedimenti del Garante



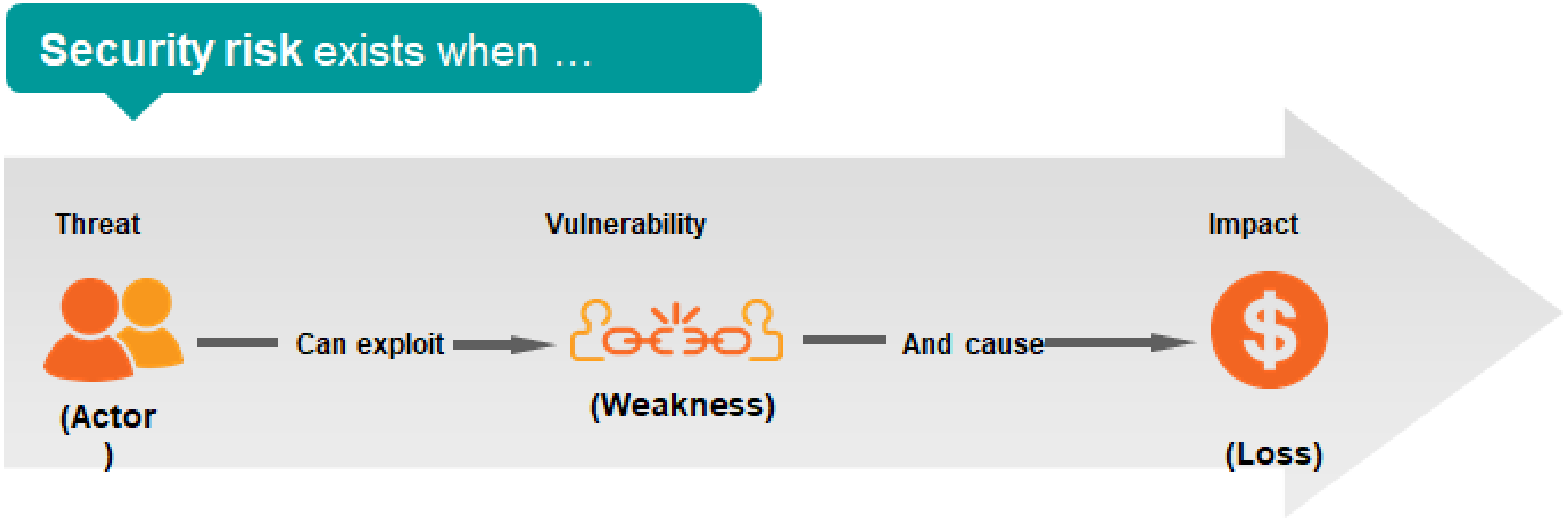
Articolo 32 – Sicurezza del trattamento

1. *Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:*
   a) *la pseudonimizzazione e la cifratura dei dati personali;*
   b) *la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;*
   c) *c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;*
   d) *d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*
2. *Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.*
3. *L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.*
4. *Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.*

OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

Risk Management Approach

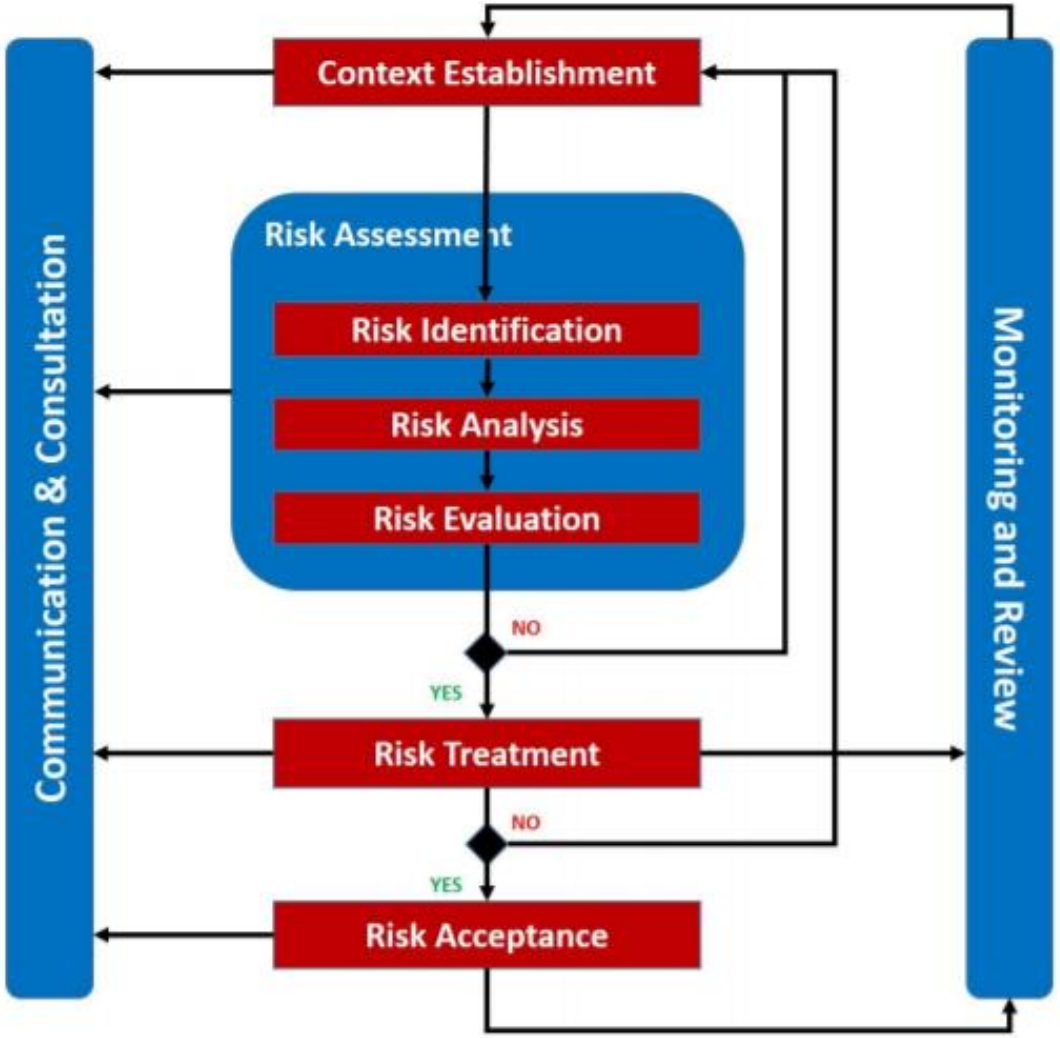


Security Risk Management is the application of control to detect and block the threat, to detect and fix a vulnerability, or to respond to incidents (impacts) when all else fails.

OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

Risk Management Approach



OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

ENISA Methodology for GDPR IT Risk Management

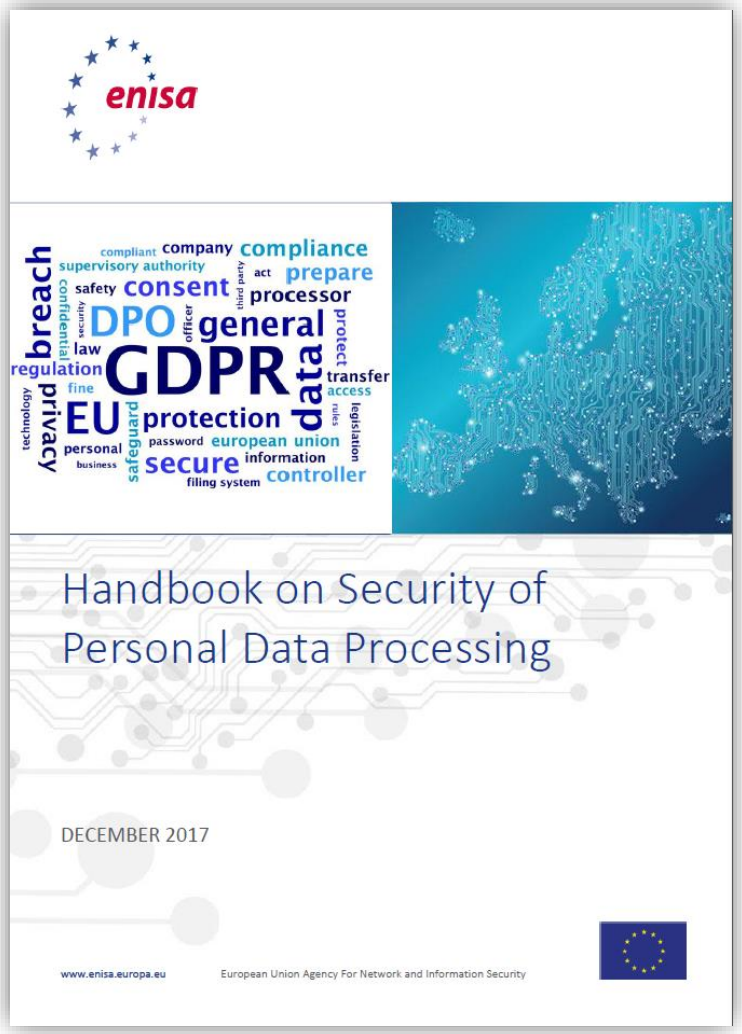
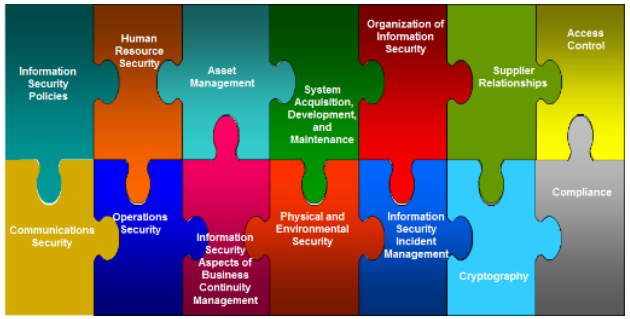


Table of Contents

Mappatura ENISA vs controlli di sicurezza ISO 27002

A. Security policy and procedures for the protection of personal data
B. Roles and responsibilities
C. Access control policy
D. Resource/asset management
E. Change management
F. Data processors
G. Incidents handling / Personal data breaches
H. Business continuity
I. Confidentiality of personnel
J. Training
K. Access control and authentication
L. Logging and monitoring
M. Server/Database security
N. Workstation security
O. Network/Communication security
P. Back-ups
Q. Mobile/Portable devices
R. Application lifecycle security
S. Data deletion/disposal
T. Physical security

5. Information Security Policy
6. Organization of Information Security
7. Human Resource Security
8. Asset Management
9. Access Control
10. Cryptography
11. Physical and Environmental Security
12. Operations Security
13. Communications Security
14. System Acquisition, Development and Maintenance
15. Supplier Relationships
16. Information Security Incident Management
17. Information Security Aspects of Business Continuity Management
18. Compliance



Risk evaluation: Risk = f (Impact, Probability)

I

	QUESTION	EVALUATION
I.1.	Please reflect on the impact that an unauthorized disclosure (loss of confidentiality) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.	☐ Low ☐ Medium ☐ High ☐ Very high
I.2.	Please reflect on the impact that an unauthorized alteration (loss of integrity) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.	☐ Low ☐ Medium ☐ High ☐ Very high
I.3.	Please reflect on the impact that an unauthorized destruction or loss (loss of availability) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.	☐ Low ☐ Medium ☐ High ☐ Very high

P

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

R

IMPACT LEVEL

THREAT OCCURRENCE PROBABILITY	Low	Medium	High / Very High
Low			
Medium			
High			

Legend

Low Risk *Medium Risk* *High Risk*

OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

Impact evaluation (Esempio)

La proposta è, sulla base delle principali best practicies e linee guida di settore, di valutare i possibili impatti di un data breach in funzione:

- *delle tipologie di interessati eventualmente coinvolti*
  - *ogni tipologia ha un peso assegnato,*
  - *la tipologia di interessati più critica è quella presa come riferimento per l'analisi dei rischi (basso=1; medio=2; alto=3)*
- *delle categorie di dati trattati*
  - *ogni categoria ha un peso assegnato,*
  - *la categoria di dati personali trattati più critica è quella presa come riferimento per l'analisi dei rischi (basso=1; medio=2; alto=3)*
- *del volume di dati personali trattati (basso=1; medio=2; alto=3)*

Tipologia di interessati																
Amministratori, coordinatori, Organismi di tipo associativo	Appartenenti UE	Non appartenenti UE	Italiani	Imprenditori privati	Lavoratori o collaboratori	Militari e forze dell'ordine	Minori	Parenti, affini o conviventi	Dipendenti	Disabili	Persone fisiche	Persone giuridiche	Persone in cerca di occupazione	Studenti	Appartenenti ad Associazioni	EX Appartenenti ad Associazioni
2	1	1	1	1	1	1	3	2	1	3	1	0	2	2	2	2

Categorie dati											
Dati anagrafici identificativi	Dati di identità digitale	Domicilio /Residenza	Tipologia di alloggio	Dati di connessione	Dati di localizzazione	Abitudini di consumo	Profilazione	Condanne Penali e reati	Appartenenza sindacale /opinioni	Dati sulla salute	Orientamento Sessuale
8	5	6	6	7	7	8	8	9	9	10	10

Numerosità di record
1: <1000;
2:<10000;
3:> 10000

Calcolo impatto

Impatti	da	a
Basso	1	4
Medio	5	7
Alto	8	9

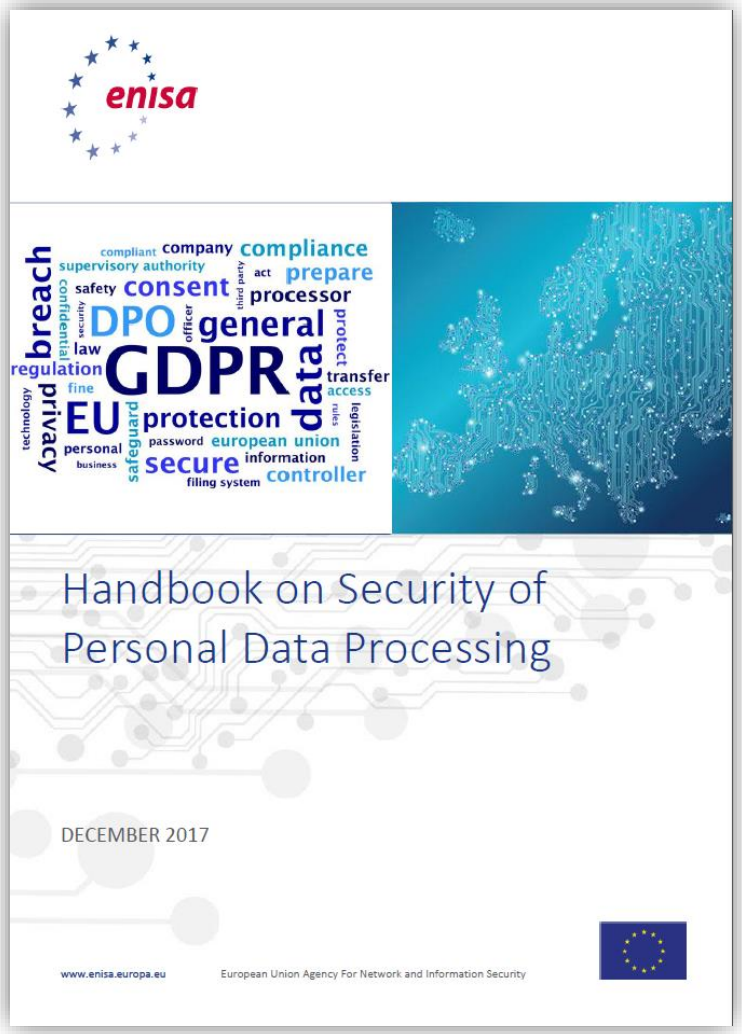
OPENTECH

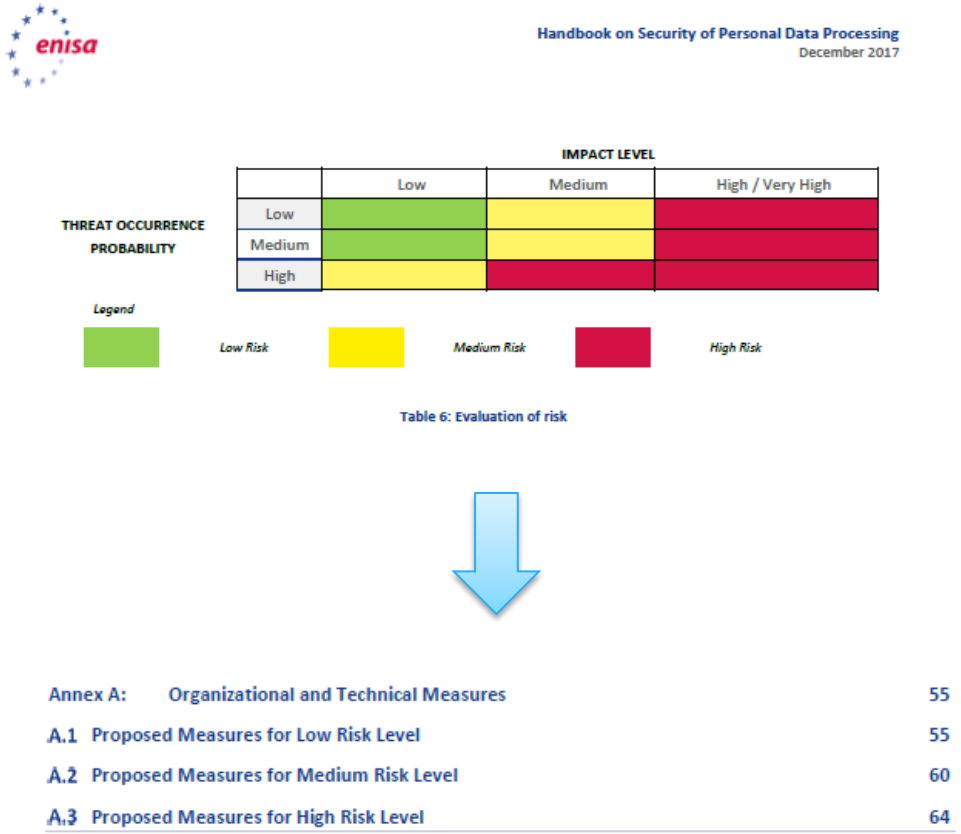
CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

Threat Analysis (esempio)

- NETWORK AND TECHNICAL RESOURCES
  - Numerosità applicativi,
  - Esposizione applicativi
  - Applicativi Standard o personalizzati
- PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA
  - Valutazione dei comportamenti da questionario
- PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA
  - Trasferimenti all'esterno del Gruppo
  - Trasferimenti all'esterno dell'Italia/UE
- BUSINESS SECTOR AND SCALE OF PROCESSING
  - Criticità dei tipologia di dati (più o meno appetibili)

ENISA Methodology for GDPR IT Risk Management

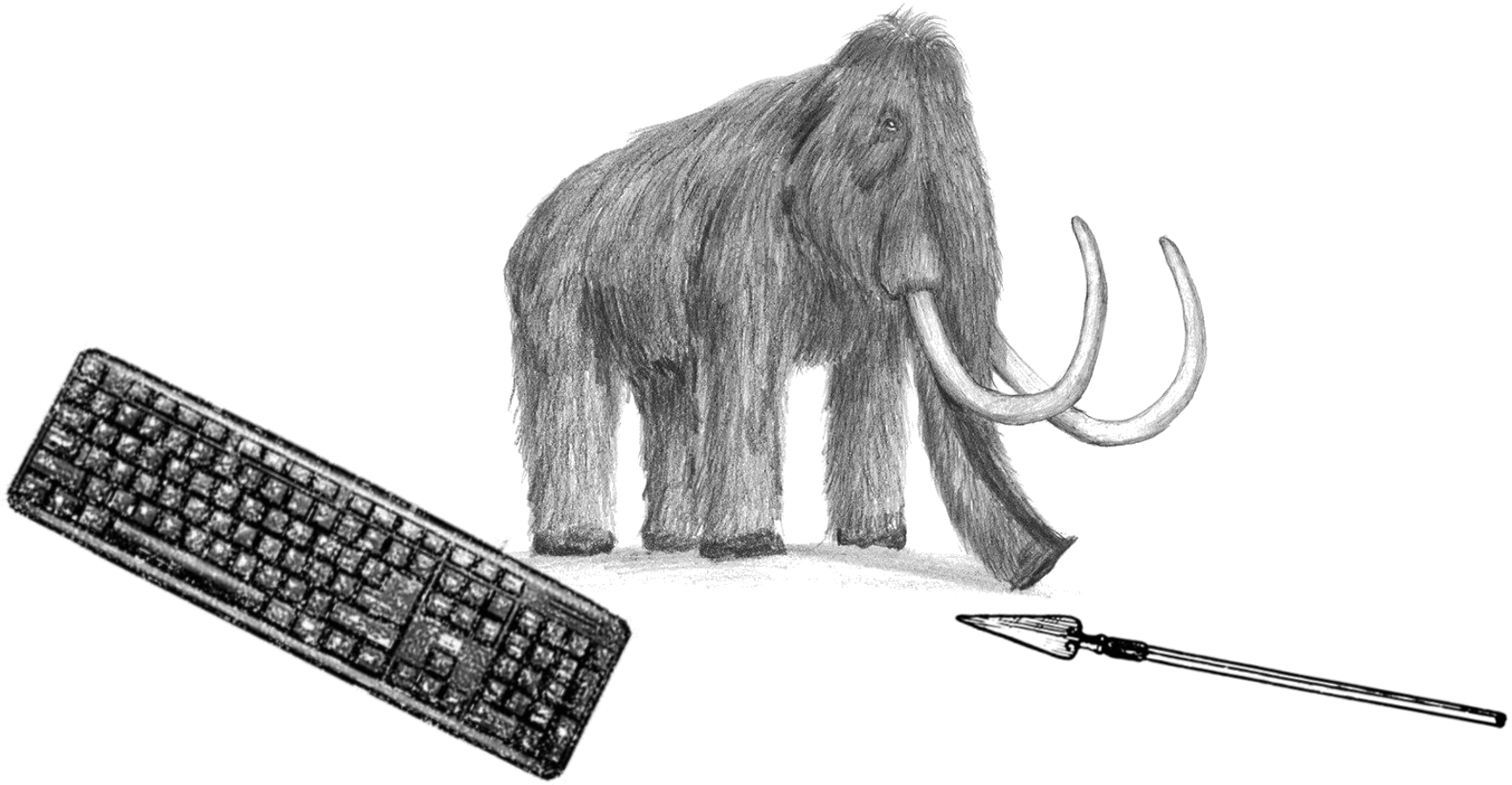




OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

Realizzare strumenti informatici



OPENTECH

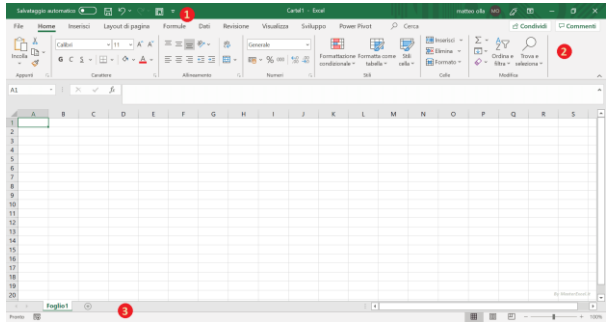
CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

«Strumenti base» per la privacy

WP29

Garante

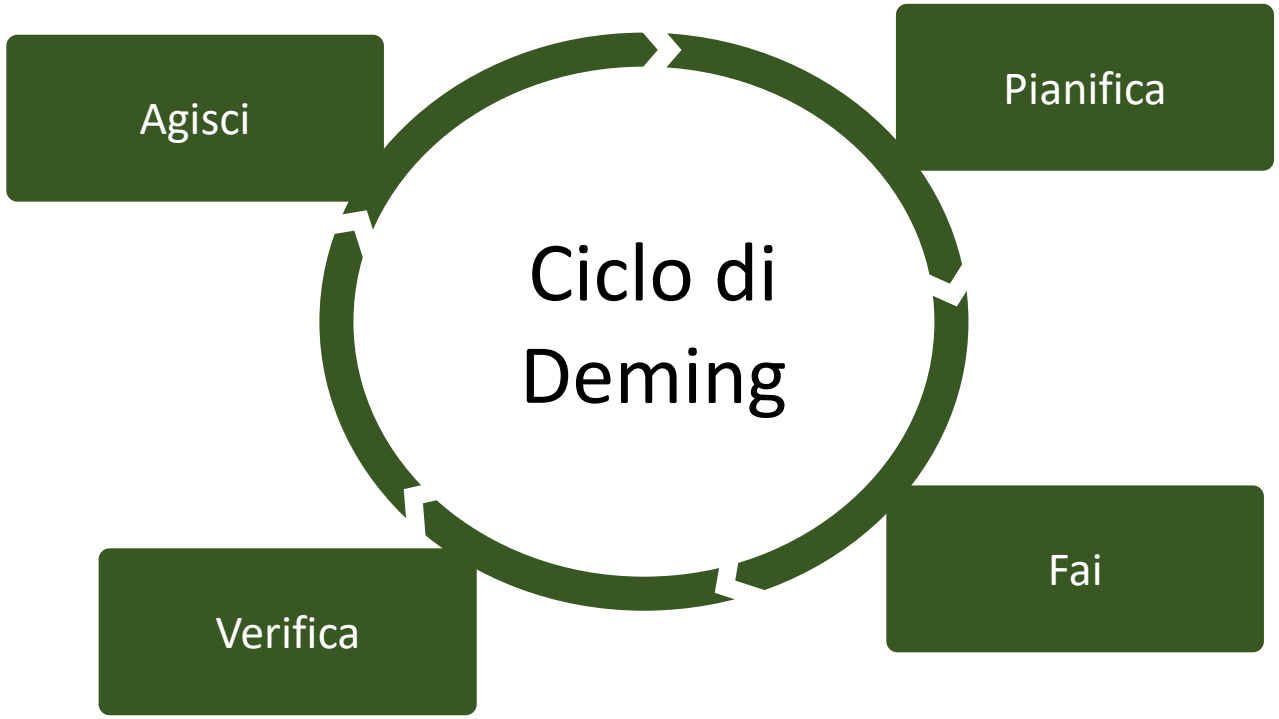
Enisa



OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

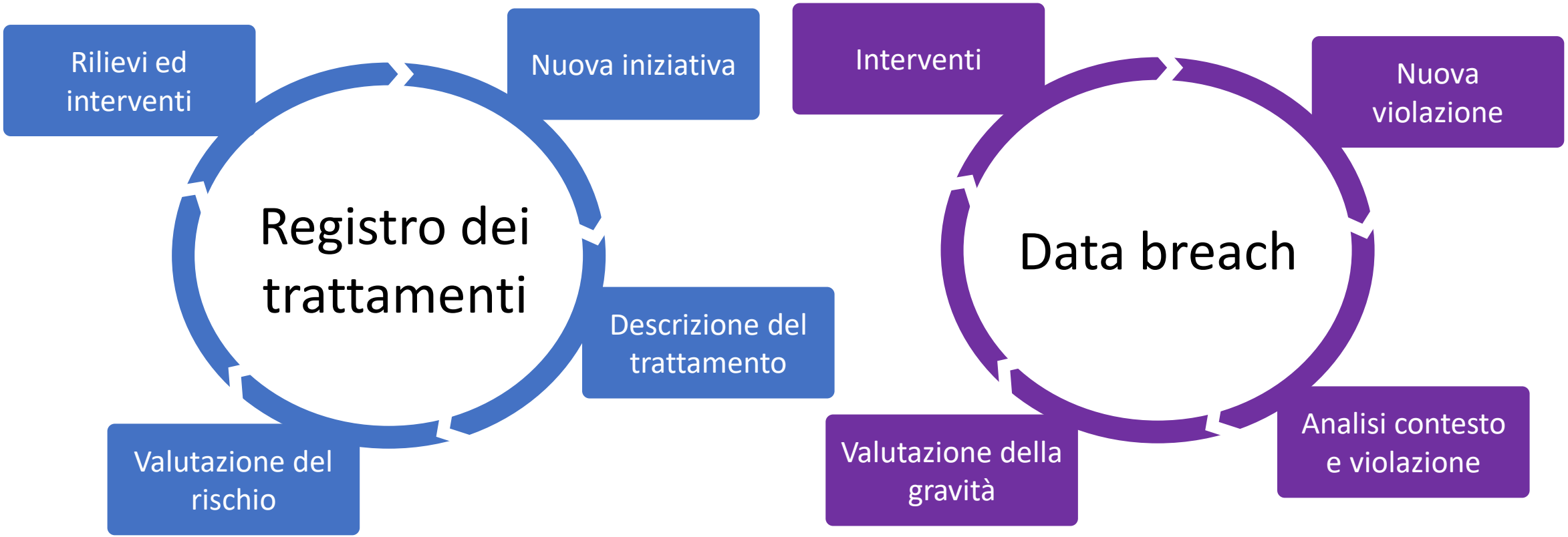
Comprendere (creare) i processi privacy



OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

Comprendere (creare) i processi privacy

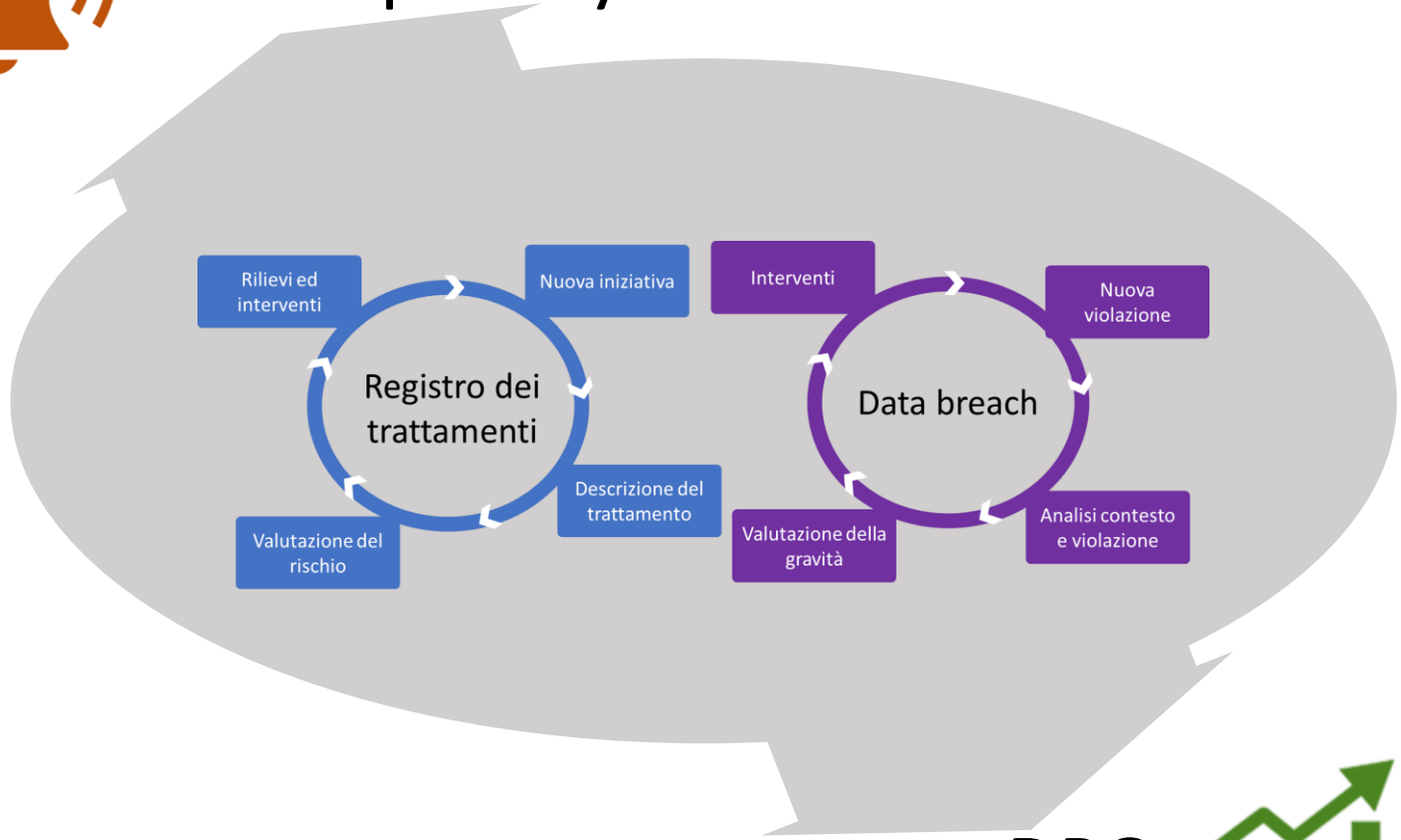


OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

Comprendere (creare) i processi privacy

Ufficio privacy



DPO

OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

Governance integrata in azienda

Compliance

Valutazione del rischio

Processi privacy

Organizzazione

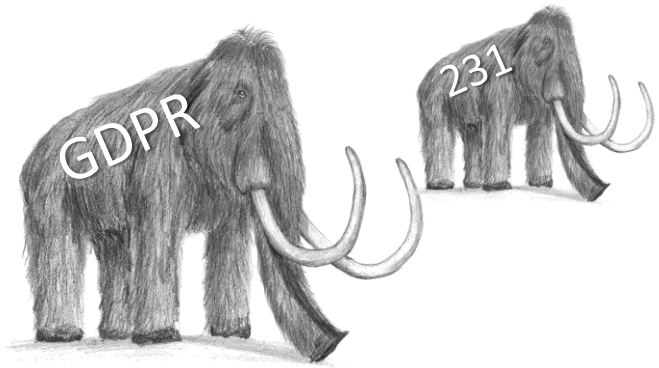
Catalogo asset

Organigramma

OPENTECH

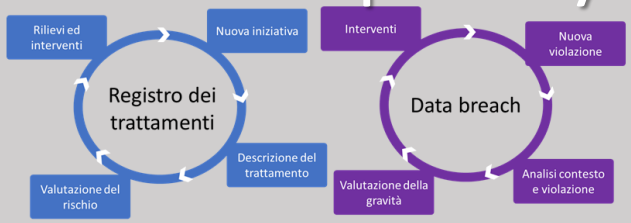
CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

Governance integrata in azienda



Compliance

Processi privacy



Rischio Cyber ed IT

Organizzazione

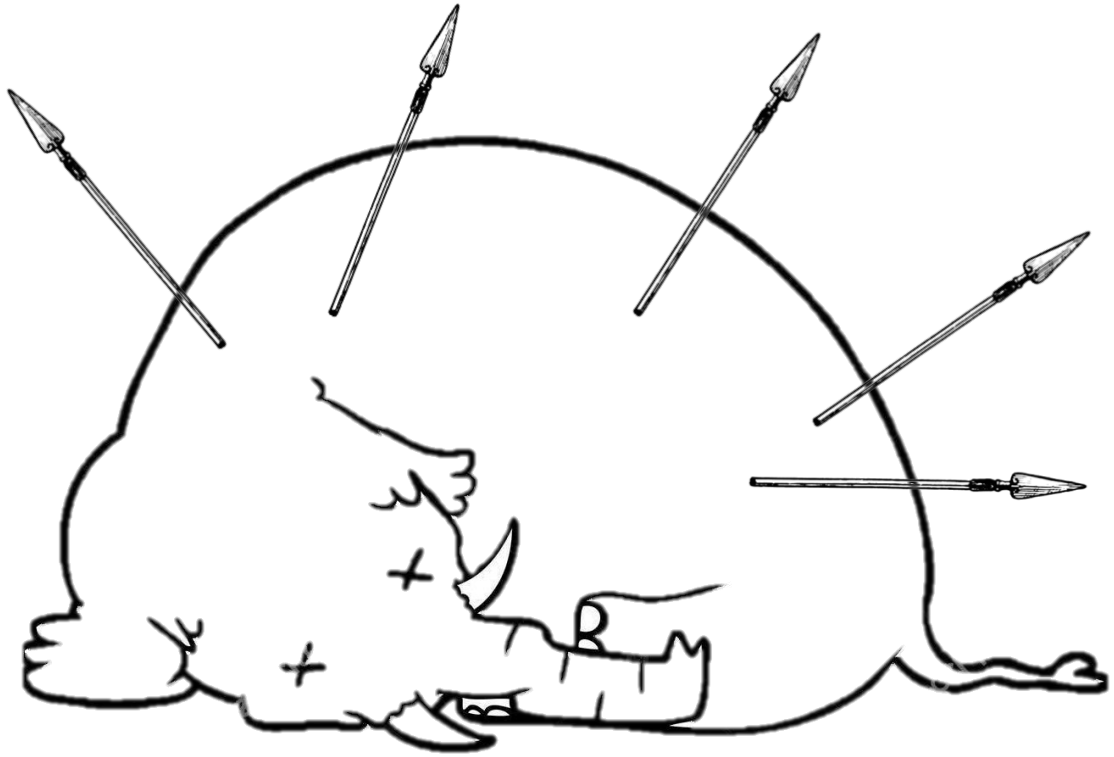
Catalogo asset

Organigramma

OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019

(Nessun animale è stato maltrattato durante questo webinar)



OPENTECH

CIO Applications Europe
Top 10 Risk Management
CONSULTING/SERVICES COMPANIES - 2019